Panoramica sui software di Image Forensics esistenti (tratta dalla Tesi di Gianluca Ghuran)

In questo capitolo faremo una breve panoramica sui software esistenti dedicati all'elaborazione di immagini a scopo forense.

2.1 Image Error Level Analyzer

2.1.1 Descrizione e scopo del tool

Questo tool funziona interamente online [10], e si basa sull'analisi del livello di errore (*Error Level Analysis*, ELA).
L'ELA è un metodo veloce e facile di *Image Forensics*, che permette di determinare se un'immagine è stata modificata da qualche programma, come ad esempio *Photoshop*.
Viene applicato risalvando l'immagine da analizzare ad una qualità predefinita, e confrontando il risultato con l'immagine originale. Quando un'immagine jpeg viene risalvata più volte, la sua qualità diminuisce. In questo modo, risalvando l'immagine e confrontandola con l'originale possiamo tentare una stima del numero di volte che è stata salvata.
Se un'immagine non è stata manipolata, allora tutte le sue parti saranno state salvate un numero di volte uguale. Se l'immagine è composta da parti provenienti da sorgenti diverse, essere potrebbero essere state salvate un numero di volte differente, e quindi risulteranno di colori differenti nel test ELA.
Questo permette quindi stabilire eventualmente un ordine cronologico delle modifiche alle varie parti dell'immagine: le parti più chiare sono state editare più recentemente, quelle più opache sono state salvate più volte.
Stando a quanto scrive l'autore, questa implementazione fa uso della *Python Image Library* e di *libjpeg* (v6.2.0-822.2), ed è completa al 95%.

2.1.2 Uso e test

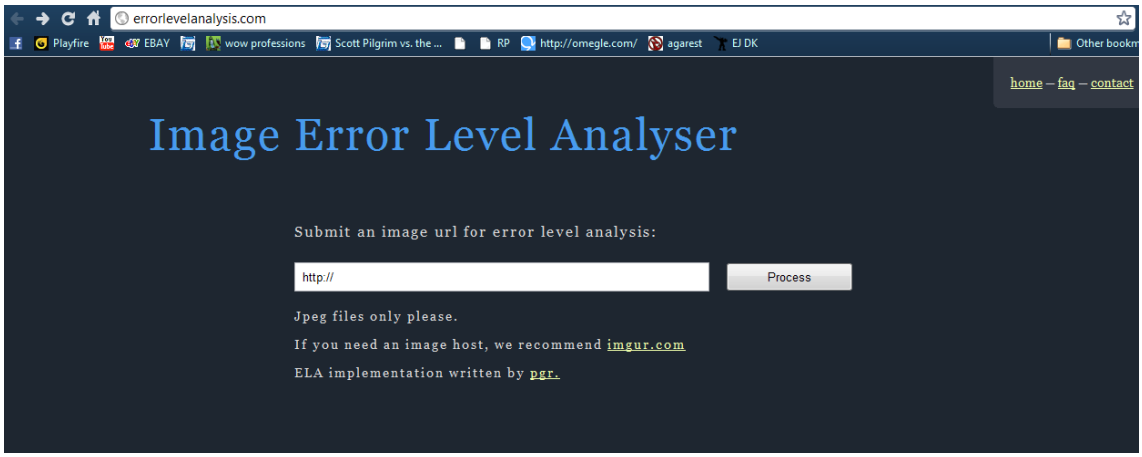

Figura 2.1 : Casella di input dell'Image ELA

Il tool si presenta all'utente come nella figura 2.1. Nella casella di testo va inserita la url dell'immagine (solo in formato jpeg) da analizzare.

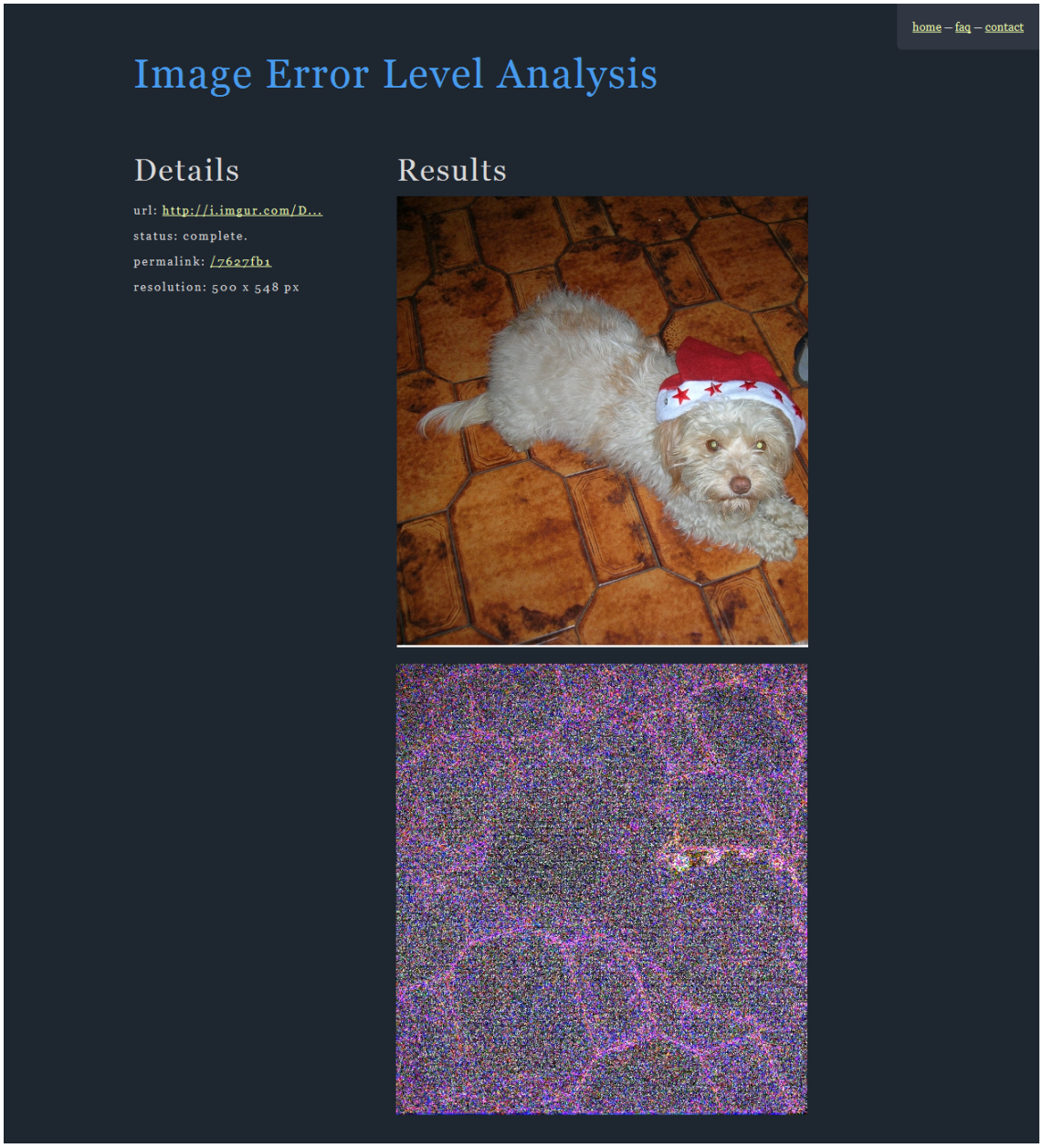

Figura 2.2 : Pagina di risultato

Dopo aver premuto il pulsante "Process" si viene ridirezionati in un altra pagina che mostra in colonna l'immagine originale con il risultato della ELA (figura 2.2).
L'immagine originale (figura 2.3) dopo lo scatto ha subito un'operazione di cropping e in seguito una riscalatura. E' stata quindi nuovamente salvata 2 volte, ma il suo contenuto non ha subito manipolazioni e non sono stati inseriti elementi da altre fonti.
Il risultato dell'analisi (figura 2.4) effettivamente tiene fede alla storia dell'immagine: le uniche parti debolmente più luminose corrispondono ai bordi e alle zone in cui il rosso è più chiaro nel cappello.

2.1.3 Punti deboli

ELA oltre agli errori, mostra con un colore più chiaro anche i contorni e le parti colorate di rosso, a causa del modo in cui i programmi salvano le immagini. In questi casi non

Figura 2.3 : Foto originale sottoposta all'analisi

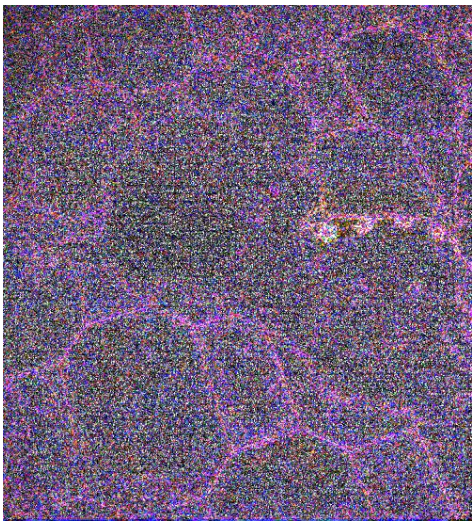

Figura 2.4 : Risultato dell'ELA

fornisce prova di manipolazione.
Inoltre, questo tool funziona solo con immagini jpeg, presumibilmente ad alta qualità (95%) . Quindi non darà risultati attendibili se applicato a immagini di qualità bassa o a cui comunque è stata ri-applicata la compressione jpeg molte volte.
L'analisi può dare un falso negativo nel caso le varie parti dell' immagine siano state salvate lo stesso numero di volte (in questo caso tutte le zone dell'immagine avranno comunque luminosità uniforme).
Infine, come abbiamo detto prima, l'immagine che abbiamo usato per il test è stata sottoposta a riscalatura : questo poichè il tool accetta immagini di dimensioni limitate. Inserendo l'immagine 2.3 prima della riscalatura (dimensioni 1568x1720) il tool restituisce una pagina di errore (figura 2.5). Facendo diverse prove si è visto che vengono accettate immagini larghe fino a 1224 pixel per lato.

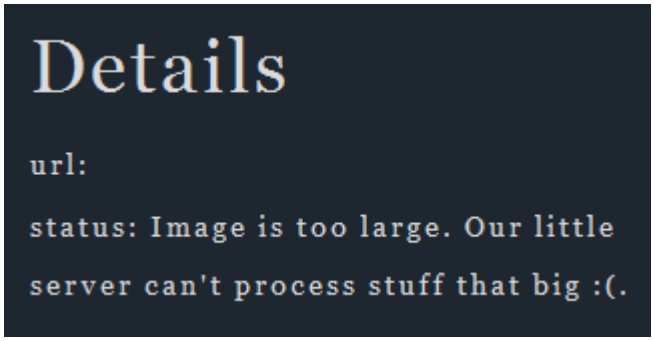

Figura 2.5 : Messaggio di errore mostrato se l'immagine è troppo grande

2.2 Jpeg Snoop

2.2.1 Descrizione e scopo del tool

Jpeg Snoop è un programma open source per Windows, scaricabile da [11]. Esso analizza e decodifica i meta-dati delle immagini jpeg e dei file MotionJPEG avi. Permette anche di identificare la sorgente dell'immagine al fine di provarne l'autenticità.
Tutte le foto digitali contengono una certa mole di metadati (EXIF, IPTC), questi

possono contenere non solo informazioni sulla fotocamera che è stata usata per scattare la foto e sui settaggi usati per lo scatto, ma anche dati riguardanti la qualità e la natura della compressione jpeg usata.
Una delle caratteristiche più interessanti del programma è la presenza di un database interno che permette di confrontare i dati ottenuti dall'immagine con le firme di compressione al suo interno. In questo modo JpegSnoop può tentare di stimare la fotocamera o il software che ha generato l'immagine. Questo è di vitale importanza nel cercare di capire se l'immagine è stata modificata/manomessa in qualche maniera. Se per esempio la firma di compressione trovata è quella di Photoshop, possiamo dedurre che l'immagine quasi sicuramente non è originale.
In aggiunta a questo il programma può estrarre molte altre informazioni, come ad esempio le tabelle di quantizzazione usate (luminanza e crominanza), settaggi di qualità JPEG, tabelle di Huffman, istogrammi RGB e altro ancora.

2.2.2 Utilizzo e test di Jpeg Snoop

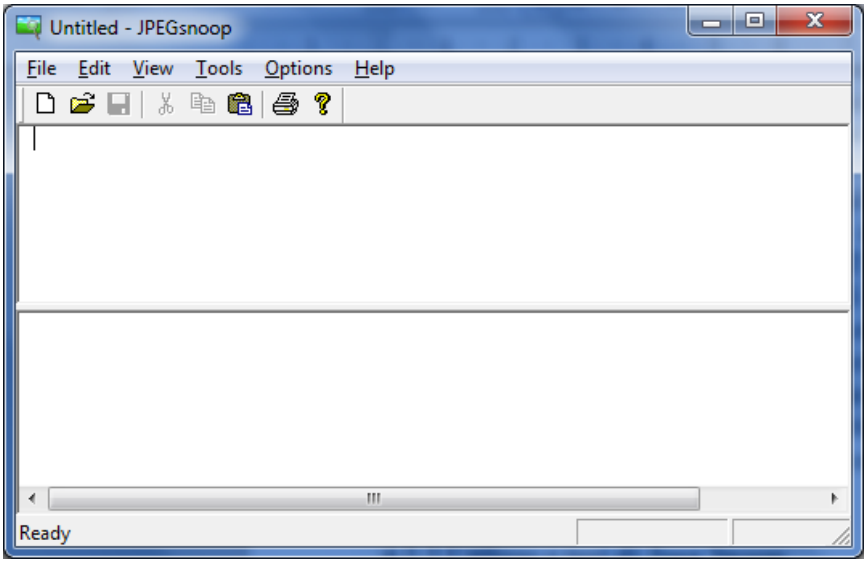

Figura 2.6: Interfaccia di Jpeg Snoop

L'interfaccia di *Jpeg Snoop* si presenta come nella figura 2.6. Nel menù in alto è possibile, dai sotto-menù Tools e Options, modificare alcuni settaggi e opzioni dell'analisi del programma.
La gui è divisa in 2 pannelli centrali : quello in basso contiene un'anteprima dell'immagine aperta ed eventuali grafici elaborati dall'analisi (ad esempio istogrammi), quello in alto stampa l'output di testo del report.
Per selezionare il file da esaminare basta usare la voce del menù File -> Open Image oppure trascinare l'icona del file da aprire sopra la finestra.
Utilizzando la stessa immagine vista nel paragrafo precedente (figura 2.3), e tralasciando le informazioni che non ci interessano (il report è veramente molto lungo), vediamo i marker riguardanti la sorgente stimata (codice 2.1 e 2.2).

```
EXIF IFD0 @ Absolute 0x00000026
    Dir Length = 0x000D
    [ImageDescription                    ] = "          "
    [Make                                ] = "NIKON"
    [Model                               ] = "E4600"
    [Orientation                         ] = Row 0: top, Col 0: left
    [XResolution                         ] = 300/1
    [YResolution                         ] = 300/1
    [ResolutionUnit                      ] = Inch
    [Software                            ] = "E4600v1.1"
    [DateTime                            ] = "0000:00:00 00:00:00"
    [YCbCrPositioning                    ] = Co-sited
    [ExifOffset                          ] = @ 0x08FC
    [XPKeywords                          ] = "lilly"
    Offset to Next IFD = 0x000018B4
```

Codice 2.1 : Informazioni estratte dai metadati exif da Jpeg Snoop. I dati relativi alla sorgente sono evidenziati in grassetto

```
*** Searching Compression Signatures ***

  Signature:           019A5A3F4E1CAB2BEA76F978702613E2
  Signature (Rotated): 01F870A8F8261FC607E1DE4C088B1B47
  File Offset:         0 bytes
  Chroma subsampling:  2x2
  EXIF Make/Model:     OK   [NIKON] [E4600]
  EXIF Makernotes:     OK
  EXIF Software:       OK   [E4600v1.1]

  Searching Compression Signatures: (3327 built-in, 0 user(*) )

          EXIF.Make / Software        EXIF.Model                          Quality           Subsamp Match?
          ------------------------    ----------------------------------  ----------------  --------------
     CAM:[Minolta Co., Ltd.          ] [DiMAGE F100                      ] [               ] No
     CAM:[NIKON                      ] [E3100                            ] [FINE           ] No
     CAM:[NIKON                      ] [E4500                            ] [FINE           ] No
     CAM:[NIKON                      ] [E5000                            ] [FINE           ] No
     CAM:[NIKON                      ] [E5400                            ] [FINE           ] No
     CAM:[NIKON                      ] [E5700                            ] [FINE           ] No
     CAM:[NIKON                      ] [E8700                            ] [FINE           ] No
     CAM:[SAMSUNG TECHWIN            ] [VLUU NV 7, NV 7                  ] [               ] No
     CAM:[SAMSUNG TECHWIN            ] [VLUU NV10, NV10                  ] [               ] No
     CAM:[SEIKO EPSON CORP.          ] [PhotoPC 3000Z                    ] [               ] No
     CAM:[SONY                       ] [CYBERSHOT                        ] [               ] No
     CAM:[SONY                       ] [DSC-H2                           ] [               ] No
     CAM:[SONY                       ] [DSC-H5                           ] [               ] No
     CAM:[SONY                       ] [DSC-H7                           ] [               ] No
     CAM:[SONY                       ] [DSC-H9                           ] [               ] No
     CAM:[SONY                       ] [DSC-L1                           ] [               ] No
     CAM:[SONY                       ] [DSC-R1                           ] [               ] No
     CAM:[SONY                       ] [DSC-V1                           ] [               ] No
     CAM:[SONY                       ] [DSC-V3                           ] [               ] No
     CAM:[SONY                       ] [DSC-W7                           ] [               ] No
     CAM:[SONY                       ] [DSC-W80                          ] [               ] No
     CAM:[SONY                       ] [SONY                             ] [               ] No
     SW :[IJG Library                ]                                     [094            ]

    The following IJG-based editors also match this signature:
     SW :[GIMP                       ]                                     [094            ]
     SW :[IrfanView                  ]                                     [094            ]
     SW :[idImager                   ]                                     [094            ]
     SW :[FastStone Image Viewer     ]                                     [094            ]
     SW :[NeatImage                  ]                                     [094            ]
     SW :[Paint.NET                  ]                                     [094            ]
     SW :[Photomatix                 ]                                     [094            ]
     SW :[XnView                     ]                                     [094            ]

  Based on the analysis of compression characteristics and EXIF metadata:

  ASSESSMENT: Class 4 - Uncertain if processed or original
              While the EXIF fields indicate original, no compression signatures
              in the current database were found matching this make/model

  Appears to be new signature for known camera.
  If the camera/software doesn't appear in list above,
  PLEASE ADD TO DATABASE with [Tools->Add Camera to DB]

Position Marked @ MCU=[  37,   4](0,1) YCC=[ -660, -166,  184]
```

Codice 2.2 : Report del confronto con il database di firme di compressione

L'immagine è una foto scattata con una Nikon E4600, che dopo essere stata acquisita è stata croppata usando Microsoft Paint e ri-salvata in formato jpeg. I metadati exif non

sono stati alterati nel processo, quindi lì viene ancora indicato il modello corretto.
Il matching con le firme del database ci restituisce un risultato più incerto invece : ci vengono indicati alcuni modelli di fotocamere che si avvicinano nel matching, tra cui altri modelli di Nikon ma non quello effettivamente usato. In seguito viene riportato il matching con alcuni software di editing, e tra questi vi è effettivamente Paint .NET.
Se riprendiamo la stessa immagine, la apriamo usando Photoshop CS4 e la ri-salviamo in formato jpeg, una nuova analisi ci darà dei risultati differenti (codice 2.3 e 2.4).
Possiamo vedere come Photoshop lasci le sue tracce nei metadati, sia come abbia una sua firma di compressione ben riconoscibile.

```
  EXIF IFD0 @ Absolute 0x00000026
    Dir Length = 0x000C
    [ImageDescription                    ] = "          "
    [Make                                ] = "NIKON"
    [Model                               ] = "E4600"
    [Orientation                         ] = Row 0: top, Col 0: left
    [XResolution                         ] = 3000000/10000
    [YResolution                         ] = 3000000/10000
    [ResolutionUnit                      ] = Inch
    [Software                            ] = "Adobe Photoshop CS4 Windows"
    [DateTime                            ] = "2011:02:21 19:08:51"
    [YCbCrPositioning                    ] = Co-sited
    [XPKeywords                          ] = "lilly"
    [ExifOffset                          ] = @ 0x0104
    Offset to Next IFD = 0x00000394
```

Codice 2.3 : Metadati exif relativi alla sorgente nell'immagine salvata da. Si può notare che Photoshop viene riconosciuto come software usato

```
 Signature:           01C1158E443D1C90F302FF6BE49DDD87
  Signature (Rotated): 01C1158E443D1C90F302FF6BE49DDD87
  File Offset:         0 bytes
  Chroma subsampling:  1x1
  EXIF Make/Model:     OK   [NIKON] [E4600]
  EXIF Makernotes:     NONE
  EXIF Software:       OK   [Adobe Photoshop CS4 Windows]

  Searching Compression Signatures: (3327 built-in, 0 user(*) )

          EXIF.Make / Software        EXIF.Model
Quality           Subsamp Match?
          -------------------------   ----------------------------------
---------------  --------------
     SW :[Adobe Photoshop          ]
[Save As 12      ]

  NOTE: Photoshop IRB detected
  NOTE: EXIF Software field recognized as from editor
  Based on the analysis of compression characteristics and EXIF metadata:

  ASSESSMENT: Class 1 - Image is processed/edited
```

Codice 2.4 : Risultato del matching con riconoscimento di Photoshop

2.2.3 Punti deboli del tool

Le tipiche problematiche legate alla ballistica di un'immagine (trattate più approfonditamente in [3]).

La manipolazione dei metadati dell'immagine o della firma di compressione può ovviamente falsare i risultati del tool.

2.3 NFI PRNU Compare

2.3.1 Descrizione e scopo del tool

Questa applicazione ha come obiettivo di aiutare a identificare le sorgenti di foto e video, basandosi sul *Photo Response Non-Uniformity* (PRNU) .
PRNU Compare è open-source, ed è stato sviluppato in Java dal Netherland Forensics Institute.

2.3.2 Utilizzo del tool

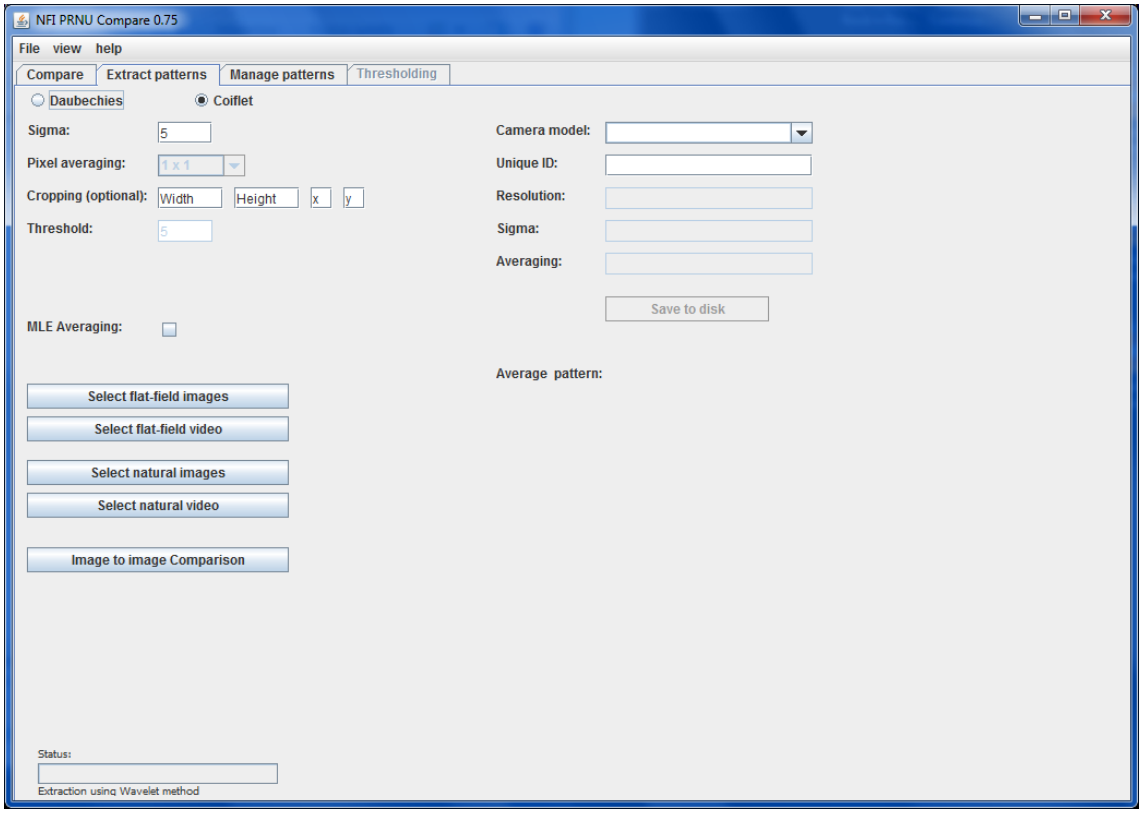

Figura 2.7 : Interfaccia di PRNU Compare , tab di estrazione patterns

L'interfaccia è suddivisa in diversi tab. I due più importanti per l'utilizzo del programma sono "Extract Patterns" (figura 2.7) e "Compare" (figura 2.8).
Nel primo si estraggono i pattern dalle immagini. Con il pulsante "select flat-field images" si ottengono i *pattern* di riferimento da un set di immagini. Il pulsante "Select natural images" permette di estrarre i *pattern* da confrontare. Sono presenti i pulsanti analoghi per estrarre i *pattern* dai video.

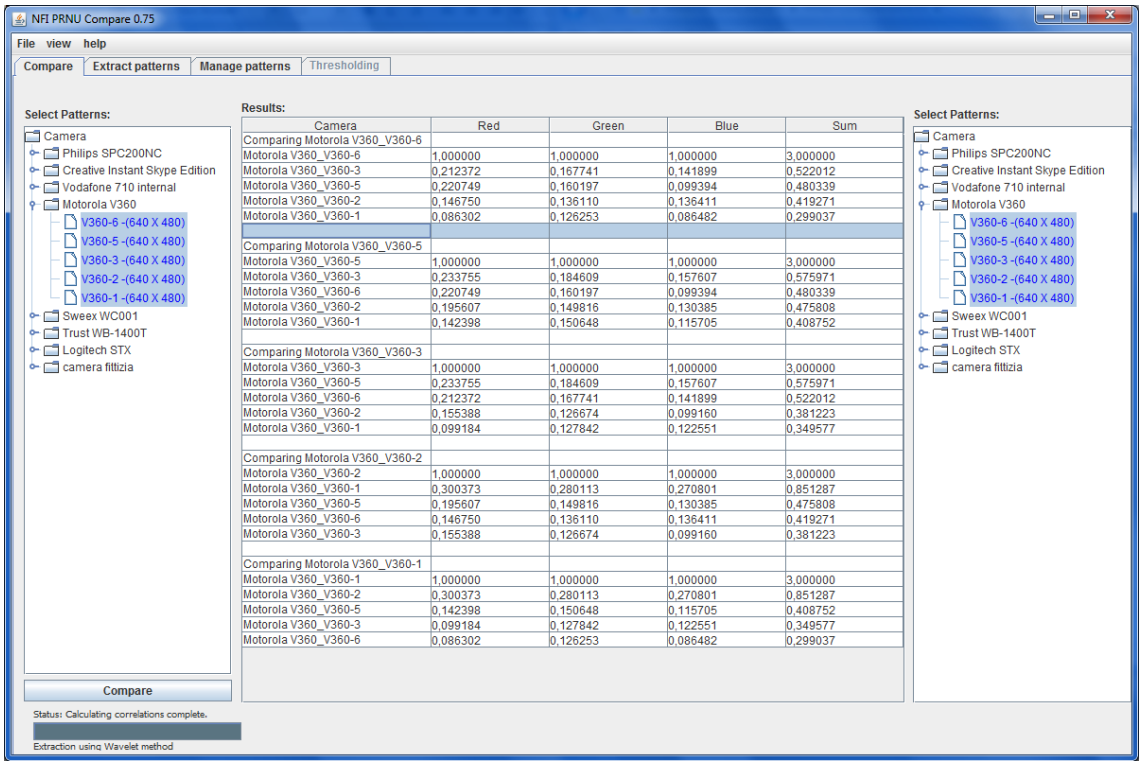

Figura 2.8 : Tab di comparazione dei pattern

Per l'estrazione è possibile scegliere l'algoritmo da utilizzare dal menù delle opzioni. Gli algoritmi presenti sono , in ordine di velocità : *Gaussian*, *Wavelet*, *Non-Local Means*.
Dalle prove effettuate il metodo *Wavelet* risulta già eccessivamente lento.
La comparazione dei pattern avviene nel tab "Compare" (figura 2.8). A destra e a sinistra è presente la liste dei *pattern* estratti, duplicata. I *pattern* selezionati dalla lista a sinistra vengono confrontati con quelli selezionati a destra. Per avviare il confronto si preme il pulsante "Compare".
I risultati vengono mostrati nella tabella centrale, con la correlazione per i canali R,G,B e la somma dei 3 risultati. I risultati con la correlazione più alta (ovvero quelli con la più similitudine) vengono posizionati in cima alla lista.
Infine i risultati della tabella possono essere copiati o esportati in formato csv.

2.3.3 Punti deboli del tool

Ovviamente i risultati del tool vengono falsati nel caso le immagini abbiamo subito manipolazioni del noise pattern.
Una nota negativa và poi all'interfaccia : tende a disorientare l'utente e rende il *worflow* un pò forzato. Personalmente, è stato necessario il file di help per la comprensione.
Un'altra nota negativa riguarda il tempo di esecuzione degli algoritmi : l'unica opzione effettivamente utilizzabile è il *Gaussian*.

2.3.4 PRNU Decompare

Rimanendo in tema di PRNU forging, esiste questo tool open-source (sviluppato sempre in Java) la cui funzione principale è compromettere il *pattern noise* dell'immagine [13] (figura 2.9).
Questa applicazione mette a disposizione 3 funzioni per manomettere il PRNU dell'immagine :

- tramite l'opzione "Destroy" l'immagine subisce in sequenza un filtraggio di *blurring* e uno di *sharpening*, causando una forte variazione del *pattern noise*;
- l'opzione "Remove" rimuove il *pattern* dall'immagine, ma per farlo necessita dell'estrazione del PRNU da un set di immagini di riferimento (una *darkframe picture* e circa 30 *flat-field*);
- l'opzione "Forge" rimuove il *pattern* attuale e ne inserisce un altro. Per fare ciò necessita di 2 set di riferimento (uno per la camera originale da rimuovere e uno per quella del *pattern* da inserire).

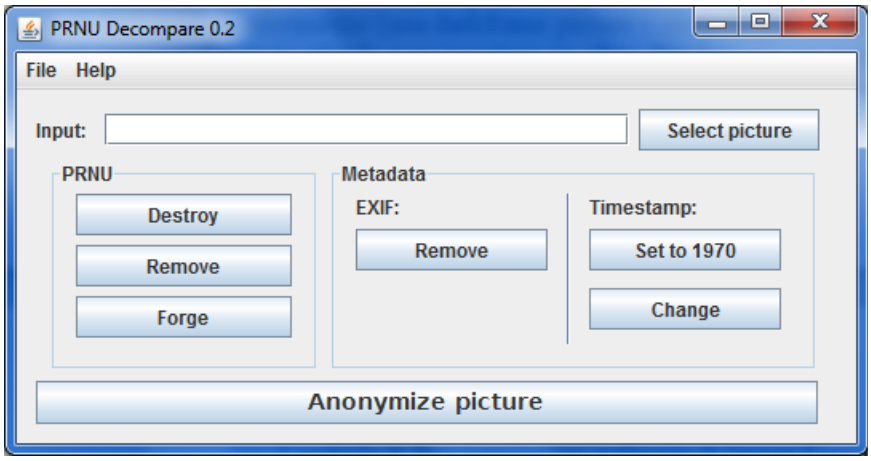

Figura 2.9 : PRNU Decompare

Infine sono presenti anche opzioni relative alla rimozione dei dati EXIF e alla manomissione dei *timestamp*.

2.4 Amped Five

Amped Five ("*Five*" è l'acronimo di "*Forensic Image and Video Enhancement*") è un software proprietario sviluppato da Amped.
Si tratta di un software per l'elaborazione di immagini e filmati per applicazioni forensi, investigative e legate alla pubblica sicurezza. Esso incorpora svariate funzioni in una soluzione unica. L'applicazione principale di Amped Five è il miglioramento di immagini e filmati provenienti dalle scene di un crimine e catturate con i più disparati dispositivi, come macchine fotografiche digitali, sistemi di sorveglianza o telefonini.

2.4.1 Funzionalità

Le caratteristiche generali sono le seguenti:

- Caricamento, salvataggio, elaborazione, analisi di singole immagini, sequenze di immagini o filmati.
- Aggiunta, configurazione e modifica in tempo reale un numero illimitato di filtri, anche durante la riproduzione di un filmato.
- Applicazione automatica di una stessa sequenza di filtri a differenti file.
- Modifica in ogni momento di qualsiasi passo dell'elaborazione e visualizzazione diretta del risultato finale.
- Generazione automatica di report dettagliati.
- Applicazione di filtri solamente ad una zona di interesse dell'immagine (ROI, *Region of Interest*), oppure solamente ai fotogrammi di interesse in una sequenza.

- Interfaccia semplice e comoda.
- Possibilità di scegliere fra tecniche di elaborazione classiche o algoritmi allo stato dell'arte.
- Selezioni e misurazioni sulle immagini con precisione al pixel.

Formati supportati

- Caricamento di immagini da tutti i formati più comuni, come bitmap, jpeg, tiff, targa, jpeg 2000, png.
- Caricamento di filmati da qualsiasi formato standard; li può decodificare sia tramite i codec di sistema che con la libreria interna: nel secondo caso può caricare la maggior parte dei file senza aver nemmeno bisogno del codec installato sul sistema.
- Caricamento di una sequenza di immagini come un filmato.
- Transcodifica un filmato in un altro formato oppure trasformazione in una sequenza di immagini (o viceversa).
- Possibilità di selezionare solamente i fotogrammi di interesse da un filmato (consecutivi o in posizioni arbitrarie).
- Controllo di modifiche verificando l'hash code del file.
- Visualizzazione dei dati Exif delle immagini.

Funzioni di modifica

- Funzioni di editing di base come ritaglio, inversione a specchio, conversione e estrazione di canale, zoom e rotazione.
- Correzione di distorsioni causate da lenti ad ampio angolo o conversione di immagini riprese da una telecamera omnidirezionale in un formato panoramico.
- Correzione della prospettiva per visualizzare la scena da una diversa angolazione.
- Ridimensionamento delle immagini con algoritmi avanzati, che garantiscono una definizione migliore rispetto ai classici algoritmi di interpolazione impiegati da altri software.
- Conversione di filmati interlacciati in progressivi senza perdita di informazioni.
- Miglioramento manuale della luminosità e del contrasto, regolando le curve di intensità o con algoritmi di regolazione automatica.
- Analisi delle immagini con vari filtri di soglia e riconoscimento bordi.
- Misurazione di distanze, altezze e lunghezze da immagini.

Funzionalità di filtraggio

- Miglioramento dei dettagli delle immagini (unsharp masking, rational sharpening).
- Riduzione dell rumore e della grana (filtri, medio, mediano, bilaterale, rational smoothing).
- Applicazione di filtri personalizzati.
- Riduzione degli artefatti da compressione con l'algoritmo di deblocking.
- Rimozione interferenze e sfondi periodici con il filtro di Fourier.
- Correzione della sfocatura dovuta a movimenti troppo veloci o errata messa a fuoco.
- Rimozione del rumore da un filmato con il filtraggio temporale e l'integrazione dei fotogrammi.
- Miglioramento e stabilizzazione filmati mossi.

- Correzione e modifica del punto di vista in diversi fotogrammi con l'allineamento della prospettiva.

2.4.2 Esempi

Nelle figure 2.10, 2.11, 2.12 e 2.13 sono riportati alcuni esempi tratti direttamente dal sito di Amped.

Figura 2.10 : Contrast enhancement di Amped Five

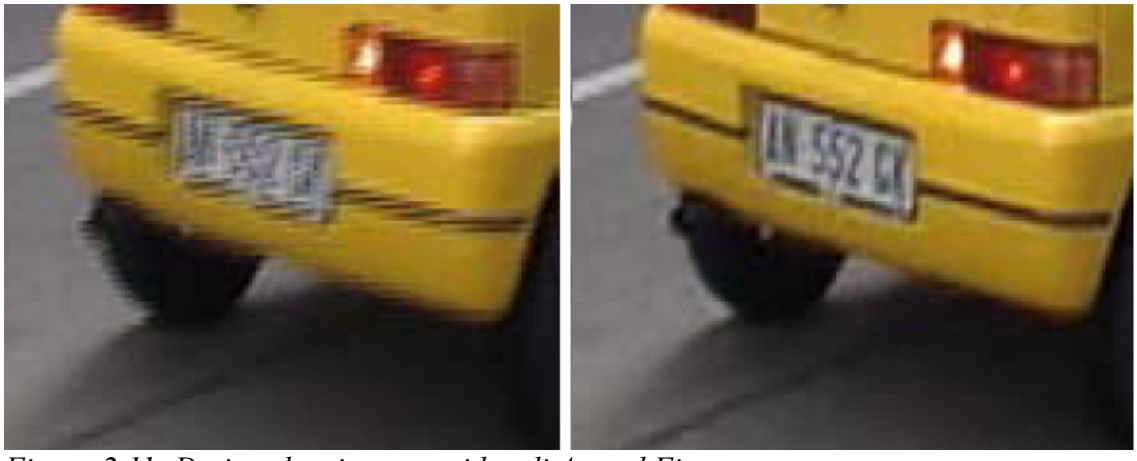

Figura 2.11: De-interlacciamento video di Amped Five

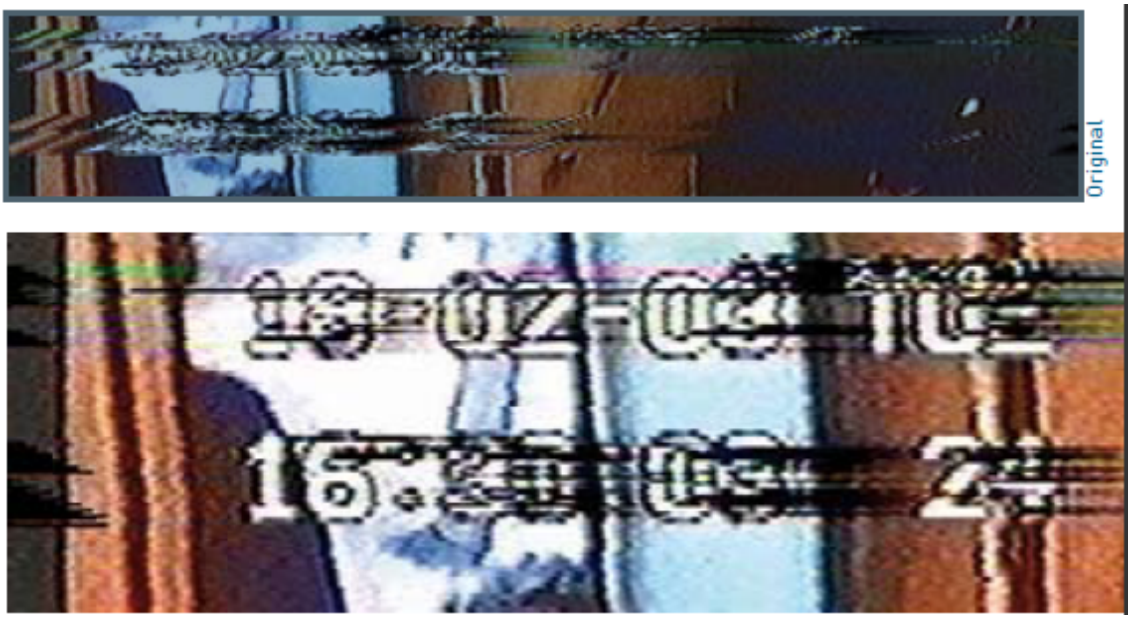

Figura 2.12: Correzione VHS danneggiato di Amped Five

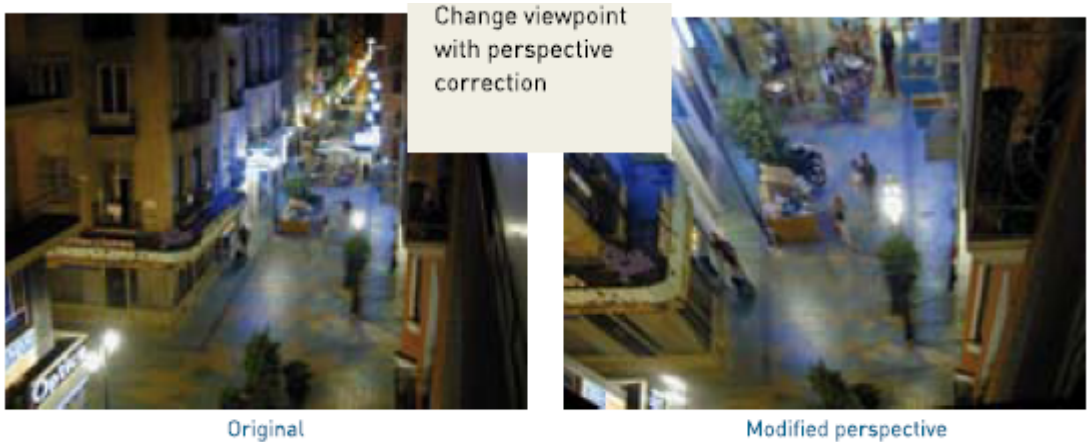

Figura 2.13: Cambio punto di vista con correzione prospettica di Amped Five

2.5 Videntifier Forensic

2.5.1 Scopo e descrizione

Videntifier è un software commerciale sviluppato da Videntifier Technologies. Il suo scopo è fornire alle forze di investigazione uno strumento per la verifica e il riconoscimento automatico dei video.
Una delle attività che maggiormente consumano tempo durante un'investigazione è la revisione del materiale video: quando viene individuato un sospettato di possesso di materiale illegale, si procede al sequestro di tutti i suoi supporti multimediali (hard disk, DVD e supporti di memorizzazione vari), dopodichè gli investigatori devono cercare e visionare manualmente i file video in cerca del materiale illegale. La visione manuale è obbligatoria perchè un semplice check sui metadati o un confronto a campione dei frame del file non ci dà garanzie sul contenuto: un video può venire compresso, croppato, riscalato, ruotato, riflesso o subire altre operazioni simili, in questo caso il contenuto del video non cambia ma strumenti convenzionali come l'*hashing* del file non sarebbero più in grado di riconoscerlo. Videntifier utilizza un approccio diverso per

automatizzare questo procedimento.

2.5.2 Funzionamento

Videntifier basa il suo funzionamento sul concetto di "*visual fingerprints*" (impronte visuali). Queste ultime sono seguenze di numeri codificate dal valore visuale in specifici punti di interesse nei frame del video (figura 2.14). Queste impronte codificano solo i punti e le zone di interesse più robusti relativi a specifiche strutture all'interno dell'immagine. In questo modo la codifica per impronte è robusta contro compressione, cambio di colore, riscalatura e altre operazioni di questo genere.
Videntifier si appoggia ad un database centrale per effettuare il matching dei punti salienti del video. Questo database al momento contiene ha classificato al suo interno un totale di circa 30000 ore di video, ed è in continua crescita con il materiale video più comune e non.
Al momento dell'analisi video, il client invia una query al database con i dati delle impronte calcolate sul video in esame attraverso una connessione criptata. Nel caso in cui un certo numero di frame venga riconosciuto, allora i dati del filmato verranno inviati al client per la classificazione. Se invece il filmato non viene riconosciuto (perchè non presente sul database) allora il client sposterà il file in una directory apposita per l'eventuale controllo manuale.

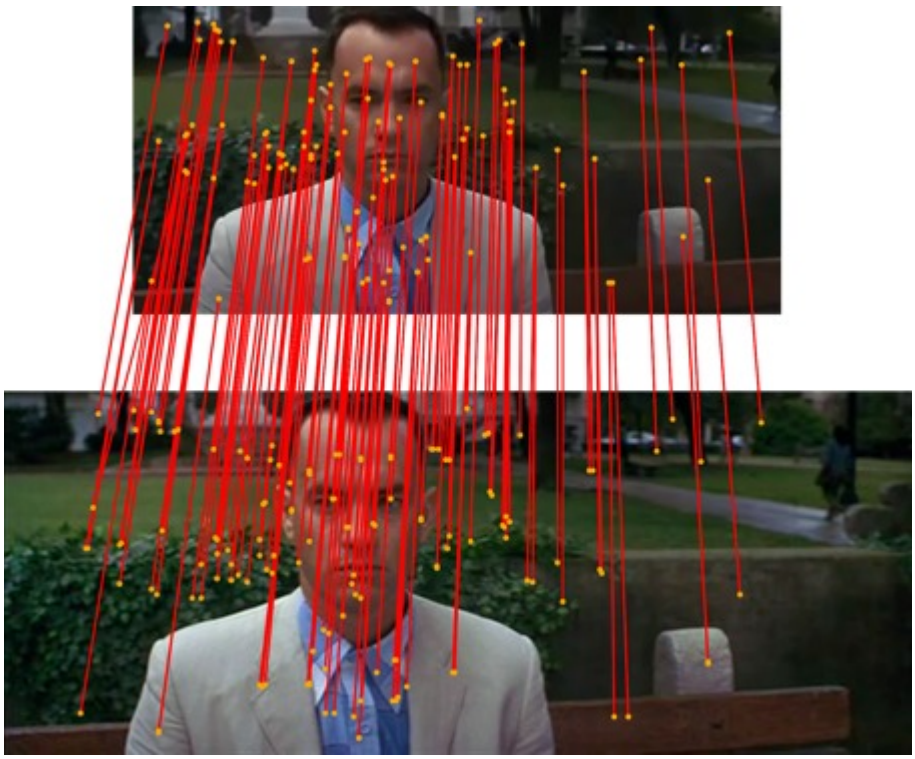

Figura 2.14: Matching delle impronte tra il frame originale di un video e una sua versione riscalata

2.5.3 Licenze e costi

Videntifier viene offerto in 4 diversi modelli di servizio incrementali: Basic, Silver, Gold e Platinum (in ordine di prezzo). Essi differiscono per velocità e robustezza di

analisi, numero di licenze fornite e aggiunte extra come supporto on-site e fornitura di unità di estrazione dedicate per l'analisi dei video.
I prezzi degli abbonamenti annuali per le versioni Basic e Silver sono rispettivamente di 1699 € e 2699 €. I prezzi delle versioni Gold e Platinum non sono riportati sul sito.

2.6 Adroit Photo Forensics

2.6.1 Descrizione e scopo

Adroid Photo Forensics (APF) (figure 2.15, 2.16 e 2.17) è un software forense commerciale sviluppato da Digital Assembly, specializzato nel recupero e nell'analisi di foto digitali.
E' in grado di funzionare su file system diversi come FAT12/16/32, NTFS, HFS, HFS+, può leggere formati come EnCase, RAW e dd ed è noto per implementare gli algoritmi di SmartCarving e GuidedCarving per il recupero di immagini digitali.
APF è pure in grado di leggere i dati EXIF delle immagini e può essere usato per riordinarle in base ai timestamp exif anzichè rispetto a quelli forniti dal file system. E' dotato anche di un visualizzatore di time-line che si basa sia sui dati EXIF che sui timestamp del filesystem.
La sua interfaccia è ottimizzata per la visulizzazione di foto, e include opzioni per l'ordinamento e il raggruppamento delle immagini.

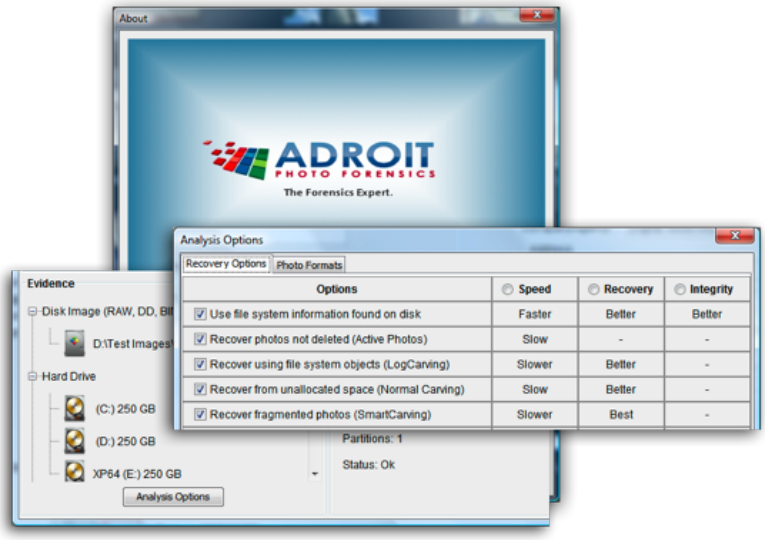

Figura 2.15: Interfaccia di APF per l'analisi dei File System

2.6.2 Licenze e costi

Digital Assembly mette a disposizione 2 versioni di APF: una con attivazione online e una con attivazione via *dongle*. La versione con attivazione online richiede una costante connessione a internet per la verifica della chiave di registrazione e il conseguente utilizzo. La versione con dongle richiede che un piccolo pezzo di hardware sia connesso al computer per l'uso. L'hardware in questione viene inviato via posta al richiedente. Le due versioni costano rispettivamente 499 e 599 dollari.
Inoltre è prevista la possibilità di acquistare un piano di manutenzione annuale per il servizio e il supporto al prezzo di 150$ annui.

Figura 2.16: Opzioni di visualizzazione e raggruppamento delle foto trovate da APF

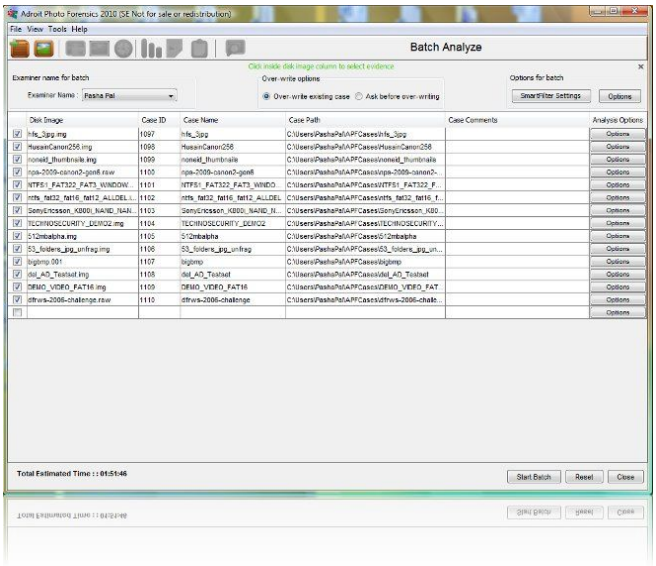

Figura 2.17: Interfaccia di APF per l'analisi in batch

2.7 Adroit Photo Recovery

2.7.1 Descrizione e scopo

Adroit Photo Recovery (APR) è un programma sviluppato da Digital Assembly, specializzato nel recupero di foto. Utilizza l'algoritmo di SmartCarving, già utilizzato da Adroit Photo Forensics, per recuperare le foto tenendo conto della frammentazione del

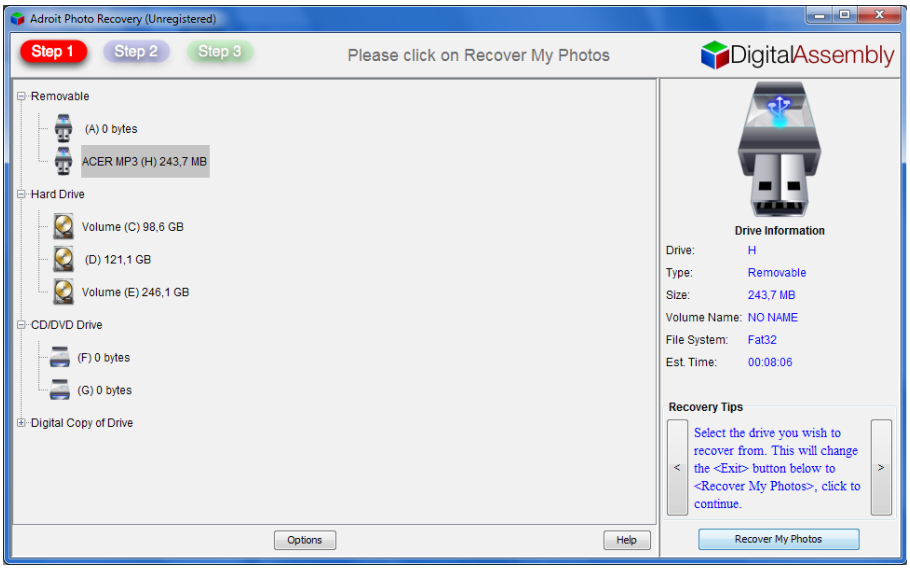

Figura 2.18: Scelta del drive da analizzare con Adroit Photo Recovery

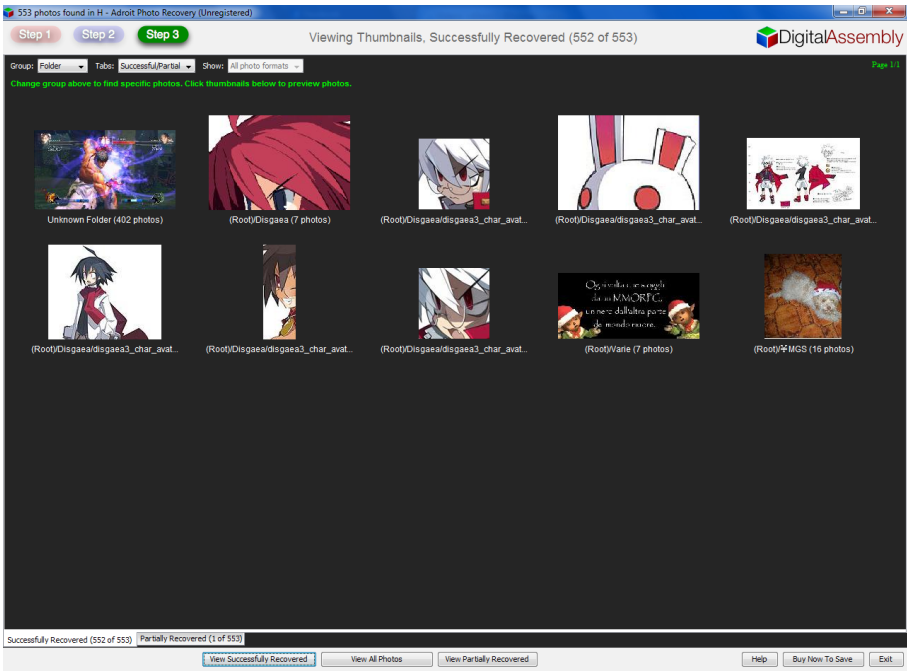

Figura 2.19: Risultati ottenuti da Adroit Photo Recovery

file system. Questo gli permette di ottenere risultati migliori rispetto alla maggior parte dei software di questo tipo.
Malgrado sembri molto simile ad APF, APR possiede molte meno funzionalità implementate.

2.7.2 Funzionamento e punti deboli

A livello di inferfaccia il programma è incredibilmente semplice e intuitivo, e il recupero viene
suddiviso in 3 fasi : nella prima si seleziona il supporto su cui effettuare l'analisi (figura 2.18), nella seconda fase il software di occupa di analizzare la periferica selezionate e applicare il *carving*, e infine nella terza fase vengono mostrati i risultati ed è possibile salvare le immagini trovate. Il software permette di ordinare i risultati trovati secondo

diversi criteri (directory, data, tipo, ecc.), ma sopratutto divide i risultati in 3 categorie principali : *Recovered* (immagini trovate e ricostruite con successo), *Not Deleted* (immagini che effettivamente non sono mai state cancellate) e *Partially Recovered* (immagini di cui non sono stati trovati tutti i frammenti, spesso non sono neanche visualizzabili).
Il programma è stato provato con alcune periferiche di memorizzazione usb, sul quale sono state copiate e poi cancellate alcune directory contenenti immagini. Il programma ha mostrato risultati molto buoni nel recupero di immagini jpeg e png, mentre invece non è riuscito a recuperare nessun file Bitmap e gif (tutti Partially Recovered).
Infine il programma ha degli ovvi limiti nei casi in cui i frammenti delle immagini vengano completamente eliminati (formattazione completa oppure disco totalmente riempito da altri file).

2.7.3 Licenze e costi

Sul sito di Adroit Photo Recovery è possibile scaricare la versione demo del programma, sulla quale sono state effettuate le prove. Nella demo l'unica funzionalità bloccata è quella del salvataggio delle immagini recuperate, per il resto è possibile osservare il funzionamento completo del software e i risultati che ottiene.
La licenza del programma (che permette di sbloccare la funzione di salvataggio finale) costa 20$.

2.8 Image Forensics Search System

2.8.1 Scopo e descrizione

Image Forensics Search System (IFSS) è un programma open source, sviluppato in Java, che permette, data un'immagine "target", di cercare immagini che la contengono oppure immagini simili a essa.
La motivazione principale dietro lo sviluppo di questo software è assistere le forze dell'ordine e altre organizzazioni simili quando esse hanno bisogno di scoprire se una particolare immagine (che loro già possiedono) si trova all'interno di una grossa raccolta di immagini. Per esempio pratico può essere la polizia in possesso di una foto che mostra attività illegali di un qualche tipo, e vuole verificare se tale immagine si trova all'interno di un hard disk sequestrato.
IFSS permette agli utenti di fare 3 tipi di ricerche:

- ricerca di immagini simili a quella target all'interno di una directory;
- ricerca dell'immagine target all'interno di una seconda immagine scelta ("Image within image" singola);
- ricerca dell'immagine target all'interno di tutte le immagini di una directory ("Image within image" multipla).

Per ognuna delle ricerche il tool mette a disposizione vari parametri, che influiscono sull'algoritmo di ricerca in vario modo (ad esempio dando priorità a certi aspetti come la ricerca di certe tonalità di colore o l'utilizzo dei soli bordi per la comparazione).

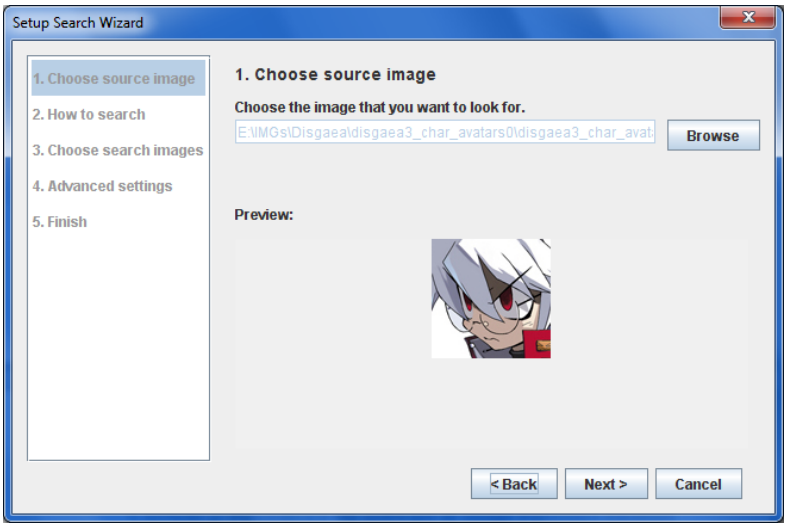

Figura 2.20: Scelta immagine di target per IFSS

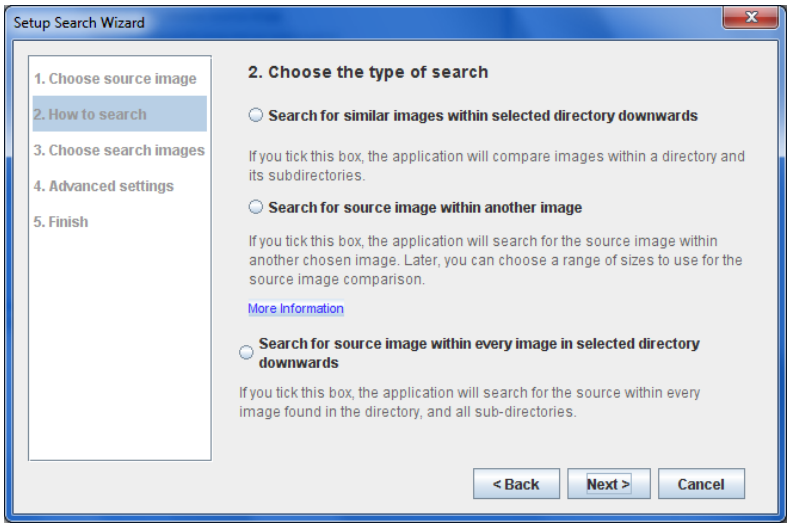

Figura 2.21: Scelta tipo di ricerca di IFSS

2.8.2 Funzionamento del programma

Il programma nella sua interfaccia presenta sequenzialmente diversi pannelli che danno varie opzioni per l'elaborazione all'utente. Per prima cosa viene chiesto di indicare l'immagine target e il tipo di ricerca (figure 2.20 e 2.21), in seguito vengono richiesti parametri specifici relativi alla ricerca selezionata (immagini/directory di confronto, soglie e criteri vari).
Durante l'elaborazione viene mostrata la schermata di caricamento e alla fine vengono presentati i risultati.
Al termine l'utente può iniziare una nuova ricerca tramite l'apposito pulsante. Tutte le ricerche vengono conservate nei vari tab richiudibili della finestra principale.

2.8.3 Punti deboli

L'unico vero punto debole individuato è la lentezza notevole nell'elaborazione, in particolar modo nelle ricerche del tipo "image within image". Ciò non ha reso possibili test esaustivi.

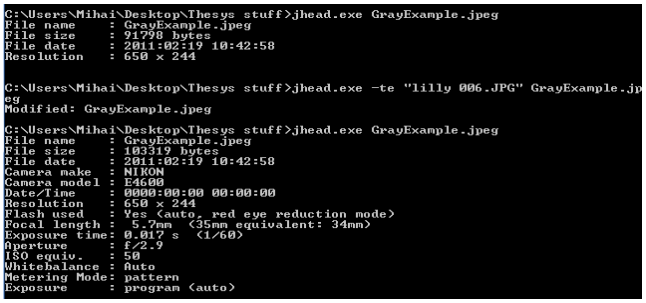

Figura 2.22: Esecuzione di jhead nel prompt di Windows

Inoltre, durante l'elaborazione alcuni elementi dell'interfaccia smettono di rispondere a dovere: ciò fa pensare ad una certa instabilità nell'applicazione.
Infine, bisogna considerare il dispendio di CPU: il tool è stato fatto girare su un processore Intel Core 2 Duo da 3 Ghz, e durante tutta l'elaborazione ha usato in media il 90% del tempo di CPU. Malgrado ciò i tempi di esecuzione sono stati notevoli: questo fa pensare che il tool sia proibitivo nel suo utilizzo su macchine poco prestanti.

2.9 Exif Jpeg header manipolation tool

2.9.1 Descrizione e scopo

Questo tool è un programma gratuito che serve a manipolare gli header dei file exif. I file exif non sono altro che file jpeg con un header modificato per contenere metadati relativi ai settaggi della camera e l'immagine di anteprima (thumbnail). Praticamente tutti i file immagine creati dalle fotocamere moderne sono file exif.
La specifica exif utilizza anche altri formati oltre jpeg, ma jpeg è cmq il più diffuso.
Pur non essendo stato sviluppato a scopo forense (l'autore è solo un appassionato di fotografia), il tool può aiutare nella balistica della fotocamera (malgrado la visualizzazione exif sia implementata in diversi altri programmi), e sopratutto può diventare uno strumento di anti-forense grazie alle funzioni di manipolazione dell'exif.

2.9.2 Funzionamento e punti deboli

Il programma non è dotato di interfaccia grafica e funziona interamente da shell (figura 2.22). Nel suo utilizzo di base prende in parametro solo un'immagine jpeg, e visualizza il contenuto dei suoi metadati exif. Inserendo altri parametri è possibile accedere a tutta una serie di funzioni per la manipolazione dell'header exif. Una lista completa dei parametri e delle opzioni è presente sul sito del programma [19].
Note dolenti sul programma:

- malgrado la specifica exif sia supportata anche in altri formati, il programma funziona solo con file jpeg (indipendentemente dalla reale presenza di metadati exif nell'immagine);
- Jhead richiama dei programmi esterni per alcune sue funzioni, come la rotazione dell'immagine;
- la modifica dei dati dell'header exif è piuttosto limitata, per la maggior parte si limita a modificare solo campi a lunghezza fissa pre-esistenti;
- Sono presenti dei bug relativi alla rotazione dell'immagine e ad informazioni errate in foto scattate con diversi modelli di fotocamere Canon.

Bibliografia

[1] Sebastiano Battiato, Giuseppe Messina, Rosetta Rizzo - Image Forensics : Contraffazione Digitale e Identificazione della Camera di Acquisizione: Status e Prospettive - Chapter in IISFA Memberbook 2009 DIGITAL FORENSICS - Eds. G. Costabile, A. Attanasio - Experta, Italy 2009;

[2] Sebastiano Battiato, Giovanni Maria Farinella, Giuseppe Messina, Giovanni Puglisi - Digital Video Forensics : status e prospettive - Chapter in IISFA Memberbook 2010 DIGITAL FORENSICS - Eds. G. Costabile, A. Attanasio - Experta, Italy 2010

[3] Judith A. Redi, Wiem Taktak, Jean-Luc Dugelay - Digital image forensics: a booklet for beginners - Multimedia Tools and Applications - Springer Netherlands 2010

[4] Martino Jerian - Forensic Image Processing FAQ – Overview - http://martinojerian.com/forensic-image-processing-faq/overview

[5] Creating plug-in modules for Windows - Adobe Photoshop SDK Guide

[6] How to Write a Photoshop Plug-In, Part 1 - http://www.mactech.com/articles/mactech/Vol.15/15.04/PhotoshopPlug-InsPart1/index.html

[7] How to Write a Photoshop Plug-In, Part 2 - http://www.mactech.com/articles/mactech/Vol.15/15.05/PhotoshopPlug-InsPart2/index.html

[8] The Adobe PICA API Reference

[9] Cross-Application Plug-in Development Resource Guide

[10] Image Error Level Analyser - http://errorlevelanalysis.com/

[11] JPEGsnoop – JPEG file decoding utility - http://www.impulseadventure.com/photo/jpeg-snoop.html

[12] NFI PRNU Compare 0.75: A graphic comparison tool to help you with your work - http://www.softpedia.com/get/Multimedia/Graphic/Graphic-Others/NFI-PRNU-Compare.shtml

[13] PRNU Decompare - http://sourceforge.net/projects/prnudecompare/

[14] Amped Five - http://ampedsoftware.com/it/five

[15] Videntifier Forensic – Automatic Video Identification - http://eu.videntifier.com/

[16] Androit Photo Forensics - http://www.forensicswiki.org/wiki/Adroit_Photo_Forensics

[17] Adroit Photo Recovery - http://photo-recovery.info/

[18] Image Forensic Search System - http://www.cse.ust.hk/image_forensics/

[19] Exif Jpeg header manipolation tool - http://www.sentex.net/~mwandel/jhead/

[20] Exchangeable image file format - http://it.wikipedia.org/wiki/Exchangeable_image_file_format