Raport 10: Analiza zdjęć

Wstęp

To laboratorium ma na celu zaznajomienie się z podstawowymi metodami analizy zdjęć zapisanych cyfrowo oraz metodami badania ich autentyczności.

1. Krótki wstęp

   W ramach tego ćwiczenia poznasz metody badania autentyczności zdjęć. Do badania zdjęć zalicza się miedzy innymi metody: analizę wzrokową zdjęcia, zgodności pliku – metadanych z uwiecznionym obrazem (np. zdjęcie wykonane w ciągu dnia z godziną wykonania 03:00 wskazuje na niezgodność danych i treści zdjęcia), analizę miniatury zdjęcia oraz analizę ELA (Error Level Analysis). Badane będą zdjęcia o popularnym formacie JPEG, na podstawie struktury pliku oraz zawartości EXIF.

   W trzech zadaniach wykonasz analizę przykładowych zdjęć – plików JPEG. W ćwiczeniu zostanie wykorzystane oprogramowanie ExifTool (https://exiftool.org), pozwalające między innymi na podgląd edycję, modyfikację metadanych plików.

   Do analizy ELA wykorzystany zostanie serwis on-line FotoForensics https://fotoforensics.com .

   Pobierz przykładowe 3 zdjęcia znajdujące się w archiwum: zadania.zip i rozpakuj na swoim dysku lokalnym.

3 Zadanie 1 – analiza miniatur

W ramach tego zadania wykonasz analizę zdjęcia w celu rekonstrukcji ukrytych informacji.

Dla podanego zdjęcia uzyskaj dodatkowe informacje poprzez export miniatury z pliku „zad1.jpg”. Zauważ różnice na zdjęciu w pełnej rozdzielczości w stosunku do zdjęcia miniatury.

Do exportu miniatury ze zdjęcia użyj komendy:

exiftool -b -ThumbnailImage image.jpg > thumbnail.jpg

Rejestracja: KR 27G

Zadanie 2 – analiza treści zdjęcia vs metadane

W ramach tego zadania wykonasz analizę zdjęcia w celu zbadania informacji zawartych w metadanych porównując je z zapisanym obrazem.

Kosztując z narzędzia ExifTool uzyskaj dodatkowe informacje na podstawie metadanych z pliku „zad2.jpg”.

Metadane z komendy exiftool:

ExifTool Version Number : 11.88

File Name : zad2.jpg

Directory : .

File Size : 294 kB

File Modification Date/Time : 2021:05:18 22:44:34+00:00

File Access Date/Time : 2022:05:23 13:21:06+00:00

File Inode Change Date/Time : 2022:05:23 13:12:40+00:00

File Permissions : rw-rw-r--

File Type : JPEG

File Type Extension : jpg

MIME Type : image/jpeg

JFIF Version : 1.01

Exif Byte Order : Big-endian (Motorola, MM)

Camera Model Name : Zenith TTL

X Resolution : 72

Y Resolution : 72

Resolution Unit : None

Y Cb Cr Positioning : Centered

Exif Version : 0231

Date/Time Original : 1995:10:23 20:06:34

Components Configuration : Y, Cb, Cr, -

Flashpix Version : 0100

Color Space : Uncalibrated

GPS Version ID : 2.3.0.0

GPS Latitude Ref : North

GPS Longitude Ref : East

Profile CMM Type :

Profile Version : 2.0.0

Profile Class : Display Device Profile

Color Space Data : RGB

Profile Connection Space : XYZ

Profile Date Time : 2009:03:27 21:36:31

Profile File Signature : acsp

Primary Platform : Unknown ()

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 :

Profile ID : 29f83ddeaff255ae7842fae4ca83390d

Profile Description : sRGB IEC61966-2-1 black scaled

Blue Matrix Column : 0.14307 0.06061 0.7141

Blue Tone Reproduction Curve : (Binary data 2060 bytes, use -b option to extract)

Device Model Desc : IEC 61966-2-1 Default RGB Colour Space - sRGB

Green Matrix Column : 0.38515 0.71687 0.09708

Green Tone Reproduction Curve : (Binary data 2060 bytes, use -b option to extract)

Luminance : 0 80 0

Measurement Observer : CIE 1931

Measurement Backing : 0 0 0

Measurement Geometry : Unknown

Measurement Flare : 0%

Measurement Illuminant : D65

Media Black Point : 0.01205 0.0125 0.01031

Red Matrix Column : 0.43607 0.22249 0.01392

Red Tone Reproduction Curve : (Binary data 2060 bytes, use -b option to extract)

Technology : Cathode Ray Tube Display

Viewing Cond Desc : Reference Viewing Condition in IEC 61966-2-1

Media White Point : 0.9642 1 0.82491

Profile Copyright : Copyright International Color Consortium, 2009

Chromatic Adaptation : 1.04791 0.02293 -0.0502 0.0296 0.99046 -0.01707 -0.00925 0.01506 0.75179

Image Width : 1920

Image Height : 1280

Encoding Process : Progressive DCT, Huffman coding

Bits Per Sample : 8

Color Components : 3

Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)

Image Size : 1920x1280

Megapixels : 2.5

GPS Latitude : 52 deg 13' 54.39" N

GPS Longitude : 21 deg 0' 22.17" E

GPS Position : 52 deg 13' 54.39" N, 21 deg 0' 22.17" E

Ocena wiarygodności zdjęcia:

To zdjęcie nie jest wiarygodne, ponieważ występuje kilka niezgodności. Pierwszą z nich są fałszywe współrzędne. Uzyskane w metadanych współrzędne wskazują na Pałac Kultury i Nauki w Warszawie. Po dokładniejszym przyjrzeniu się zdjęciu możemy zauważyć tablicę informacyjną miasta Krakowa, a także restaurację „Ukraiński Smak”, która znajduje się na ulicy Grodzkiej 21 w Krakowie. Na podstawie tych informacji stwierdzam, że dane uległy modyfikacji. Poza tym godzina zrobienia zdjęcia również nie wygląda na autentyczną, ponieważ metadane wskazują na 20:06 23.10.1995r., co nie może być prawdą, ponieważ jesienią o tej godzinie jest już ciemno, a na zdjęciu ewidentnie jest jasno więc musiała to być dużo wcześniejsza pora, a poza tym ubiór ludzi również nie wskazuje na to, aby to był październik, ponieważ wskazuje bardziej na lato, a to również świadczy o tym, że doszło do modyfikacji.

Wykonaj kopię tego zdjęcia oraz zmodyfikuj trzy parametry metadanych: datę wykonania zdjęcia, współrzędne wykonania oraz model aparatu.

Użyj własnych danych, podając aktualna datę oraz wybraną przez siebie lokalizację i model aparatu fotograficznego. Do modyfikacji skorzystaj z poniższych poleceń:

exiftool "-dateTimeOriginal=2021:10:23 20:06:34-05:00" a.jpg

exiftool "-exif:gpslatitude=51 01 51.39" -exif:gpslatituderef=N a.jpg

exiftool "-exif:gpslongitude=19 0 12.07" -exif:gpslongituderef=E a.jpg

```
sansforensics@siftworkstation: ~/Documents/zadania
$ exiftool "-dateTimeOriginal=2022:05:24 00:22:00-05:00" zad22.jpg
    1 image files updated
sansforensics@siftworkstation: ~/Documents/zadania
$ exiftool "-exif:gpslatitude=51 02 50.07" -exif:gpslatituderef=N zad22.jpg
    1 image files updated
sansforensics@siftworkstation: ~/Documents/zadania
$ exiftool "-exif:gpslongitude=23 1 13.04" -exif:gpslongituderef=E zad22.jpg
    1 image files updated
sansforensics@siftworkstation: ~/Documents/zadania
$ exiftool -Model="Sony Vlogo" zad22.jpg
    1 image files updated
sansforensics@siftworkstation: ~/Documents/zadania
```

Metadane po modyfikacji:

```
Y Cb Cr Positioning              : Centered
Exif Version                     : 0231
Date/Time Original               : 2022:05:24 00:22:00
Components Configuration         : Y, Cb, Cr, -
Flashpix Version                 : 0100
```

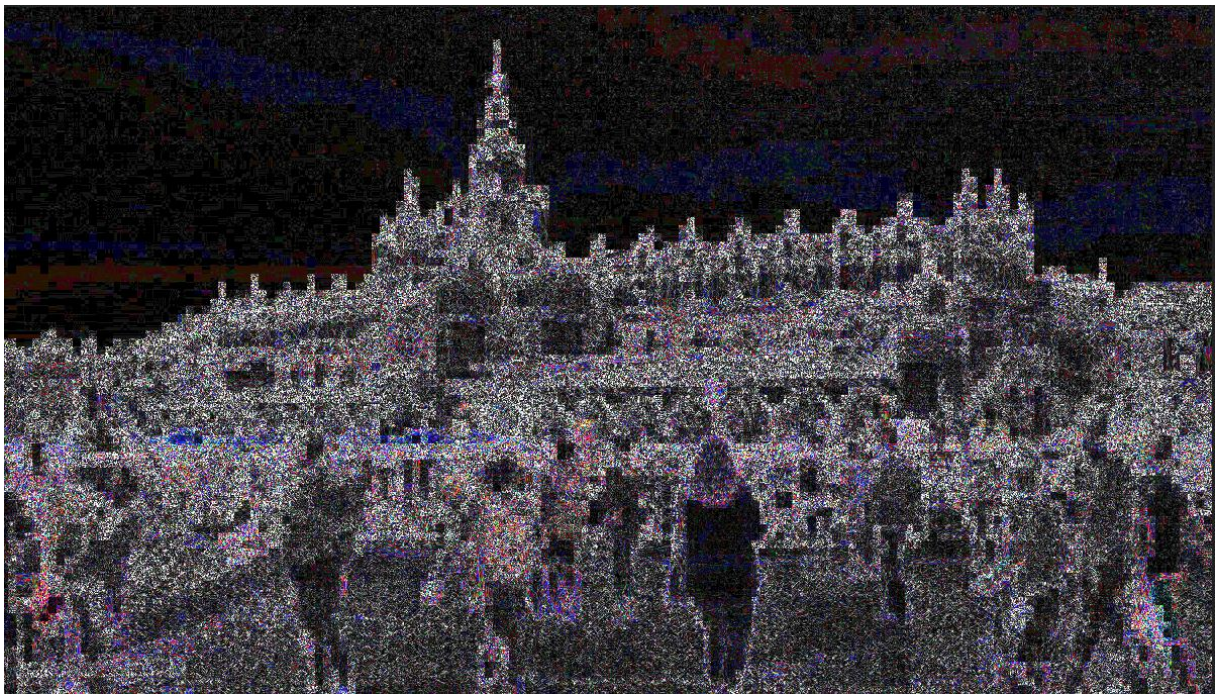
```
JFIF Version                    : 1.01
Exif Byte Order                 : Big-endian (Motorola, MM)
Camera Model Name               : Sony Vlogo
X Resolution                    : 72
Y Resolution                    : 72
```

```
GPS Latitude                    : 51 deg 2' 50.07" N
GPS Longitude                   : 23 deg 1' 13.04" E
GPS Position                    : 51 deg 2' 50.07" N, 23 deg 1' 13.04" E
sansforensics@siftworkstation: ~/Documents/zadania
```

Zadanie 3 – analiza treści zdjęcia vs metadane

Analiza ELA (Error Level Analysis) jest jedną z metod badania autentyczności zdjęć. Analiza ELA pokazuje poziom kompresji (różną jakość) w poszczególnych fragmentach obrazu i na bazie tych różnic można analizować modyfikacje w treści zdjęć. W zadaniu tym dla podanego przykładu „zad3.jpg” wykonaj analizę i wskaż ewentualne miejsce, bądź miejsca modyfikacji zdjęcia. Do analizy ELA wykorzystaj serwis on-line FotoForensics https://fotoforensics.com.

Obraz poddany analizie ELA:



Po analizie można stwierdzić, że zdjęcie zostało zmodyfikowane w zaznaczonym miejscu:

Moim zdaniem, kobieta(rude włosy, czarna bluzka, biała torebka) nie znajdowała się na oryginalnym zdjęciu i zostało ono zmodyfikowane przez dodanie jej na tą fotografię.