Detection and Tracking of Forged Digital Images from Social Media

Kumarshankar Raychaudhuri
LNJN National Institute of Criminology and Forensic Science
(Ministry of Home Affairs), Govt. of India

Presented at:
Open-Source Digital Forensics Conference (OSDFCon-2020)
Overview of Digital Image
Fake Images in Social Media
Detection and Tracking
Clone Detection using Forensically
Detection and Tracking
JPEGSnoop for Image Tracking
Challenges and Limitations
Digital image is composed of picture elements, known as **pixels**, each with a finite set of numeric representation, that can be handled and stored by a digital computer.

The digital image consists of a fixed number of rows and columns of pixels.

Web browsers can display standard internet image formats such as **JPEG**, **GIF** and **PNG**.
Images can be cloned or forged using image processing applications.

Regions in the image can be manipulated by playing with colors or copying objects from other images.

The fake images cannot be detected with the naked eye.

Social Media strips-off metadata from uploaded images, which makes tracking of the image difficult.
**Fake:** Terror-linked social media accounts shared a photo of a mother and her child who died in the rubble, supposedly during Turkey's anti-terror operation in northern Syria.

**Real:** The image was actually taken in another part of Syria in 2016.
The real difficulty in the investigation is to detect the cloned regions and track the source of the image.

Tracking the image source is a challenge in the absence of EXIF Metadata.

Open-source tools Forensically and JPEGSnoop prove to be useful to a great extent.

These tools analyze and detect cloned regions in the image.
Clone Detection using Forensically

- Magnification
- Cloned Detection
- Error-level Analysis
- Noise Analysis
- JPEG Analysis
- Structural and String Analysis
Controlling the zoom level

Auto-contrast and Auto-contrast by Channel.
Detection and Tracking - Cloned Detection

- Minimal similarity.
- Minimal details.
- Minimal cluster size.
- Block size
- Maximal Image size
Detection and Tracking- Error Level Analysis

- It is used to spot the artifacts that have been implanted on an image by compressing it multiple times.
- The parameters used are: JPEG Quality, Opacity and Error Scale.
- It is used to identify unwanted noise in the image.
- The parameters used are: **Noise Amplitude** and **Opacity**.
It contains 8x8 tables, called **Quantization tables**, which specify the way an image has been compressed.

Each cell in the table represents pixels intensities ranging from **0 to 255**.

In order to compress the image, the pixel intensities are modified by the software application in the range of **-128 to 127**, and new quantization table is calculated.

The value of the standard quantization table is **95**, which is automatically created when image is not processed.

Adobe Photoshop uses quantization table of the value **85** (Photoshop Quality).
JPEG images also contain the “Comment” section, which might contain useful information such as the source of the image file, or any software application used for writing the image etc.
Detection and Tracking - Structural Analysis

- Structural Analysis of a JPEG image refers to the analysis of the order of different sections (markers) of the image.

- The markers **SOI (Start of Image)** and **EOI (End of Image)**, indicate the beginning and start of the image file.

- Multiple SOI and EOI markers indicate presence of hidden image.

- Application Segment markers include: **APP0**, **APP1** and **APP13**.

- **APP0** contains the JPEG version, screen and printing resolution.

- **APP1** contains information on imaging parameters like date/time, focal length, aperture etc.

- **APP13** indicates that image has been processed using Adobe Photoshop.
Presence of marker **SOS** *(Start-of-Scan)* will indicate that the image has been compressed.
Strings are the pieces of data contained in the JPEG image, which can provide much useful information in the absence of EXIF metadata.

While analyzing images from Facebook, a string of the order of “FBMD01000a9…”, indicates that the image might have been uploaded using a web interface.
**JPEGSnoop for Image Tracking**

- **JPEGSnoop** is a JPEG image examination tool, which is used for extracting embedded information from JPEG images.

- It is used to identify "**Original Transmission Reference**", which refers to a number or an identifier embedded in the image, provided by the creator or image provider and is used for transmission and tracking purposes.
Based on the compression signature of the cloned image, it generates a list of devices/software, which could have been possibly used for taking the image or creating the image.

This information can be used for tracking which device and model might have been used to click the picture, especially when the EXIF metadata from the image file is missing.
Magnification using “Auto-Contrast by Channel” splatters the colors of the image.

GPS data might not be available if image is clicked using smartphone with GPS disabled.

Social media platforms strip-off the metadata, which makes tracking difficult. Structural, JPEG and string analysis may be done.

JPEG Analysis can identify quantization tables only if image is processed and edited using Adobe Photoshop.
Thank You and Questions!

Kumarshankar Raychaudhuri
(ksrc089@gmail.com)