

FOTOFORENSICS AND FORENSICALLY REPORT

Cyber Intel | Fotoforensics & Forensically | 23/09/2023

Executive Summary

This report provides an overview of two prominent image forensics tools: Fotoforensics and Forensically Image Forensics. These tools are designed for analyzing digital images to uncover hidden information, detect image manipulations, and assess the authenticity of visual content.

Index

Executive Summary	1
Index	1
1. Introduction	1
2. Tool Details	2
3. Installation	3
4. Execution	3
5. Scope and Limitations	7
6. Conclusion	7
7. References	7

1.Introduction

Digital images play a significant role in various aspects of modern life, from social media sharing to journalism and law enforcement. However, the ease with which images can be manipulated and altered raises concerns about their authenticity. Fotoforensics and Forensically Image Forensics are tools specifically designed to address these concerns by providing comprehensive image analysis and forensics capabilities.

2.Tool Details

Fotoforensics

Fotoforensics is an online platform that offers a range of tools and techniques for image forensics. Key features of Fotoforensics include:

- **Error Level Analysis (ELA):** ELA highlights areas of an image with unusual levels of compression, often indicating regions that have been manipulated or edited.
- **Metadata Analysis:** Fotoforensics can display the metadata embedded in an image, including details about the camera, location, and editing history.
- **Hidden Pixels:** Fotoforensics shows hidden pixels to discover hidden image content.
- **Strings:** Shows all the string characters in the image.
- **Estimated JPEG Quality:** Identify the last-saved JPEG quality level based on the JPEG quantization tables.
- **ICC+:** Emulates rendering of the image under different colour profiles, applications and operating systems.
- **Training Modules:** Fotoforensics includes a training module with a variety of challenges to help the user understand image manipulation in depth.

Forensically

Key features of Forensically Image Forensics include:

- **Clone Detection:** The tool can identify duplicate or cloned regions within an image, helping users detect instances of image manipulation.
- **Error Level Analysis (ELA):** Similar to Fotoforensics, Forensically offers ELA to identify areas of an image with inconsistent compression levels.
- **Noise Analysis:** Users can assess the noise patterns in an image to determine if it has been tampered with.

- **Magnifier:** The magnifier allows you to see small hidden details in an image. It does this by magnifying the size of the pixels and the contrast within the window.
- **Enhancement:** There are three different enhancements available at the moment. Histogram Equalization, Auto Contrast and Auto Contrast by Channel. Auto Contrast mostly keeps the colors intact, the others can cause color shifts. Histogram Equalization is the most robust option. You can also set this to none.
- **Level Sweep:** This tool allows you to quickly sweep through the histogram of an image. It magnifies the contrast of certain brightness levels. On use of this tool is to make edges that were introduced when copy pasting content more visible.

3. Installation

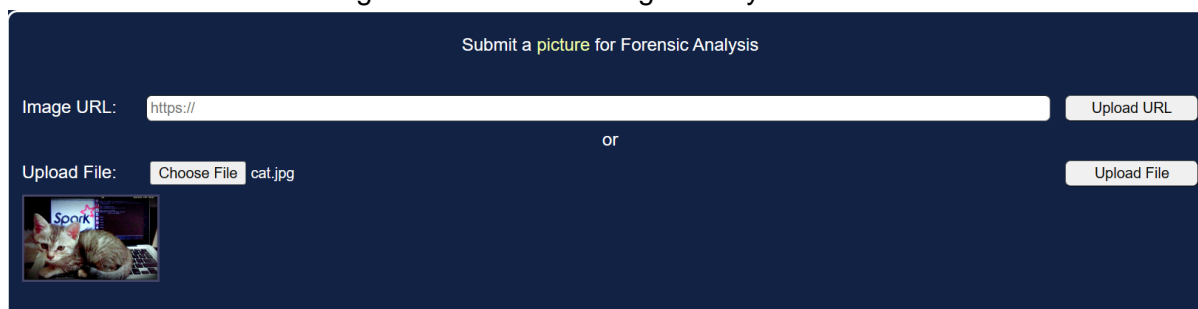
Both FotoForensics and Forensically Image Forensics are web-based tools, and users do not need to install any software or plugins to access their features. Users can visit the respective websites to upload and analyze images.

4. Execution

FotoForensics

Website Link: [FotoForensics](https://www.fotoforensics.com/)

- Upload an image on the website
- You can submit an Image URL or a local image from your hard disk.



The screenshot shows the 'Submit a picture for Forensic Analysis' interface of FotoForensics. It features two main input methods: 'Image URL' with a text field containing 'https://' and an 'Upload URL' button, and 'Upload File' with a 'Choose File' button and a file name 'cat.jpg' next to it, followed by an 'Upload File' button. Below the 'Upload File' section, there is a small thumbnail image of a cat.

- Click on Upload File. After a successful upload, you will be automatically redirected to the analysis page.



Analysis Options

- **Digest:** Shows checksums & file size.
- **Error Level Analysis (ELA):** Compression level consistency. Edges should have similar brightness, surfaces should be similar to other surfaces, and textures should be similar to other textures.
- **Games:** Gamifies image viewing by shuffling it and asking the viewer to piece it back together. May offer a different way to look at the image, which could reveal something interesting.
- **Hidden Pixels:** Shows hidden pixels to discover hidden image content.
- **Strings:** Shows all the string characters in the image.
- **JPEG %:** Identify the last-saved JPEG quality level based on the JPEG quantization tables.
- **ICC+:** Emulates rendering of the image under different colour profiles, applications and operating systems.
- **Metadata:** It is data about the image.
- **Source:** The source image that was uploaded for analysis.
- Further contains rotation, flipping & annotation keys.

Identifying Image Manipulation

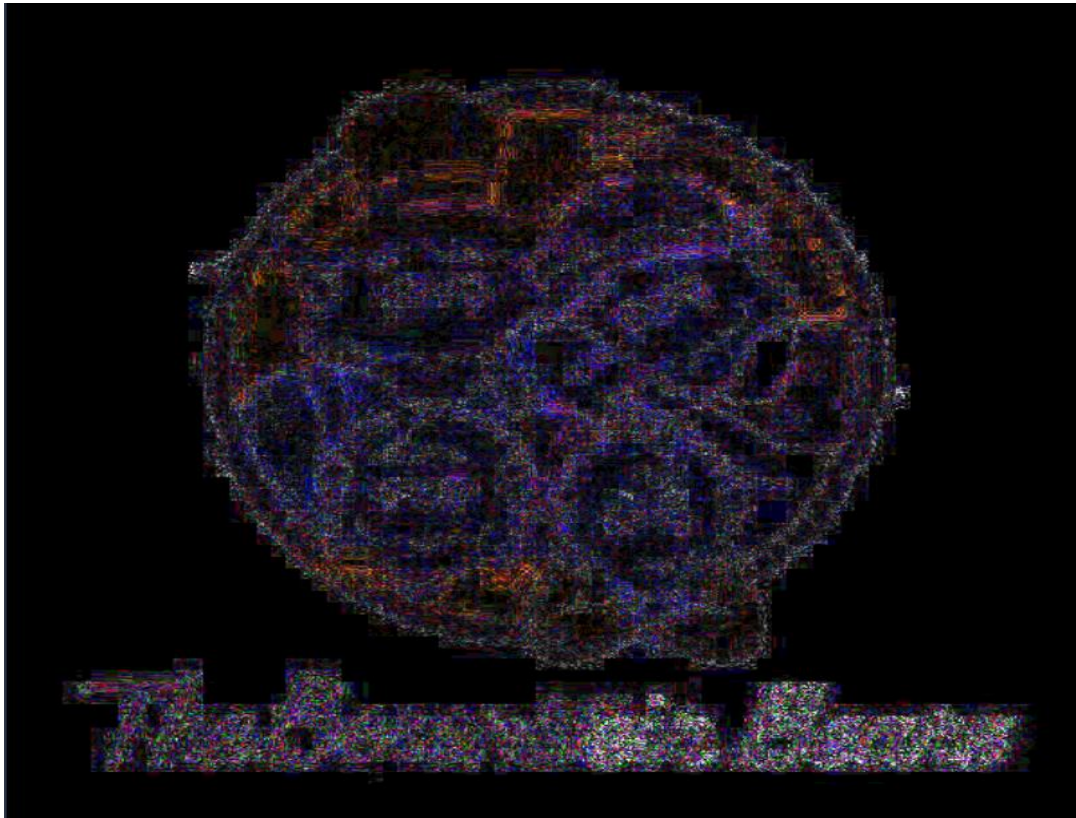
- During **ELA**, check for any differences in colour levels, brightness levels around the edges, textures, colouring around the surfaces. All high-contrast edges should look similar to each other, and all low-contrast edges should look similar. With an original photo, low-contrast edges should be almost as bright as high-contrast edges.
- JPEG image is such that it **degrades its quality over time** due to the cumulative effects of lossy compression each time it is resaved.
- Unaligned JPEGs and transparent PNGs contain pixels that are not displayed. These **hidden pixels** may identify applications.
- Examine the image's **Metadata**, as it contains useful information such as the creation date, the owner's notes, and the camera settings when the photo was taken, etc. Also examine the image's **Strings**, as they may contain ASCII characters that are useful.

Example Usage

"The Berenstain Bears" are a beloved series of children's books and cartoons. At the online forum called Reddit, a user claimed that the characters used to be called the "Berenstein Bears" ("-ein" rather than "-ain"). As proof, he uploaded a digital picture that shows the characters with the "-ein" spelling.



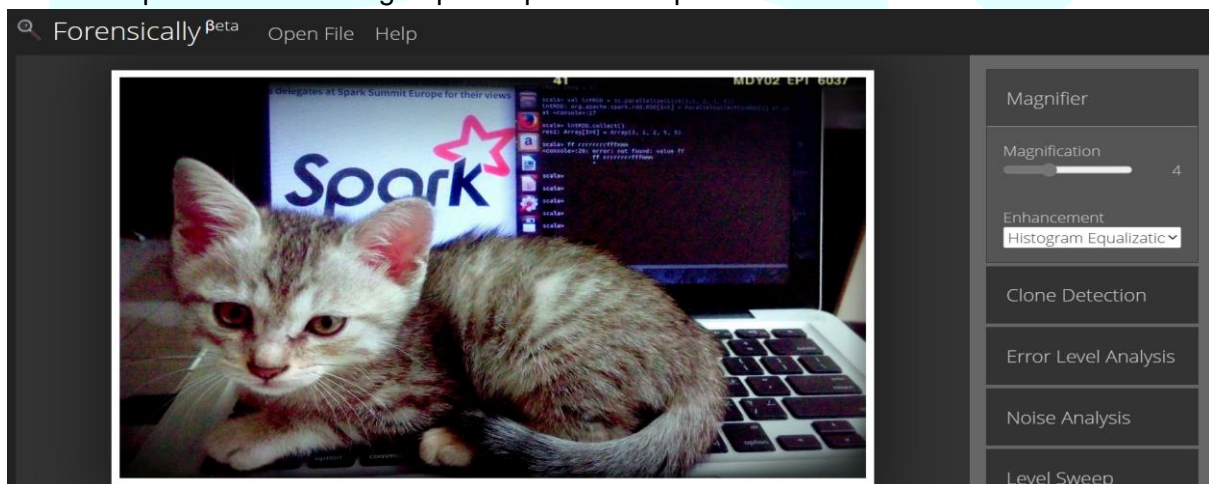
Let's use **ELA** to detect any manipulations.



Error Level Analysis (ELA) shows that the purple lettering at the bottom is inconsistent. The first part of the text, "The Berenst" is at a lower quality than the remaining text, "ein Bears". The spelling was changed from "ain" to "ein". The artist then either rewrote "Bears" or moved it over -- likely to correct the spacing between the words. This shows that the words were digitally altered.

Forensically

Click on Open File & the image opens up with the options.



5.Scope and Limitations

Scope

- Both tools are valuable for identifying image manipulations, which is essential for verifying the authenticity of visual content in fields like journalism and forensics.
- They can assist content creators in detecting unauthorized use of their images and preserving copyright.

Limitations

- The effectiveness of these tools depends on the quality of the input image and the sophistication of the image manipulation. Highly skilled manipulations may evade detection.
- While they can highlight potential issues in an image, additional context and expertise may be required to interpret the results accurately.

6.Conclusion

Fotoforensics and Forensically Image Forensics are powerful tools for conducting image forensics and verifying the authenticity of digital images. They offer valuable features for detecting image manipulations and uncovering hidden information. While they are not foolproof, these tools serve as essential resources for image analysis in various domains.

7.References

[Forensically, free online photo forensics tools - 29a.ch](#)
[FotoForensics - Tutorials](#)
[Photo Forensics Tutorial - YouTube](#)
[How to identify fake & edited photos - YouTube](#)