NORDIS – NORdic observatory for digital media and information DISorders

Report on Image Verification Tools

Date: 28-02-2023

Version 1.0

Action No:	2020-EU-IA-0189
Project Acronym:	NORDIS
Project title:	NORdic observatory for digital media and information DISorders
Start date of the project:	01/09/2021
Duration of the project:	24
Project website address:	https://datalab.au.dk/nordis
Authors of the deliverable	Duc-Tien Dang-Nguyen, University of Bergen Laurence Dierickx, University of Bergen Carl-Gustav Lindén, University of Bergen Andreas L. Opdahl, University of Bergen

Executive summary

These deliverables aim at developing and improving fact-checker tools through the creation of tailor-made algorithms in multimedia forensics. The goal is to address specific problems in fact-checking and improve existing technologies, with a view to creating stand-alone prototypes that can be integrated into existing platforms. One such tool that has been developed is FotoVerifier, a platform that supports multiple image verification algorithms and takes into account human-in-the-loop and digital media literacy.

NORDIS

Table of contents

NORDIS

1. Introduction

The Nordic Observatory for Digital Media and Information Disorder (NORDIS) is a consortium of researchers and fact-checkers from Denmark, Norway, Sweden, and Finland. We are one of the regional hubs of the European Digital Media Observatory (EDMO), a project that supports the independent community working to combat disinformation. EDMO serves as an observatory for fact-checkers, academics, and other relevant stakeholders. It encourages them to collaborate, actively connect with media organisations and media literacy experts, and provide support to policymakers. This helps to coordinate actions in the fight against disinformation.

NORDIS is funded by a grant from the European Commission and led by Aarhus University's DATALAB. Our specific aim is to develop theories, practices, and models that can help counteract digital information disorders – the spreading of misinformation, disinformation, and other forms of harmful information online – and empower citizens in the Nordic welfare states to resist such information by enabling them to enhance their media literacy. We also work closely with the fact-checking community to develop verification tools.

In this report of Task 4.3, two deliverables "**Tailor-made algorithms for fact-checkers**" and **"Stand-alone prototypes for fact-checkers"** are presented. The aim of these deliverables is to develop and improve fact-checker tools through the creation of tailor-made algorithms in multimedia forensics. We have developed FotoVerifier, a platform that supports multiple image verification algorithms and takes into account human-in-the-loop and digital media literacy. FotoVerifier is developed based on the insights from our previous deliverable (T4.2). In T4.2, concrete characteristics and uses for new tools were identified, such as shared databases of checks, tools for monitoring political debates, and the adaptation of tools to Nordic languages. We also found that the development and design of new fact-checking tools require the consideration of the journalistic context, ethical principles, and human values. Transparency of the fact-checking process and the need for a human-in-the-loop approach are also important. Combining the findings with our expertise in media forensics, FotoVerifier has been developed.

NORDIS

2. Summary of User Fact-checkers Needs

In our previous reports (T4.1 and T4.2), we identified 134 fact-checking tools and services[1], which use a broad spectrum of technologies and methods to find, verify, and classify facts. While the approaches of these tools vary, they all aim to provide accurate and trustworthy information to their users. It is important to note that these tools are not magic wands and do not define the fact-checker. Trusting the tools and the results they provide requires explicability, which can be achieved through transparency and clear communication.

Furthermore, the reliability of fact-checking tools depends on a shared-expertise between the human and the tool. The accuracy of the results also depends on considering the context of the information being checked. Facts are context-dependent, and failing to take the context into account can lead to inaccuracies. Additionally, automation can help improve the speed and efficiency of fact-checking, but it also requires high-quality training datasets and accurate results to be effective.

Our research also revealed that there are four main types of fact-checking tools that are needed: (i) tools for monitoring social networks, particularly TikTok, Telegram, and YouTube, which are considered the most difficult to monitor; (ii) tools for monitoring political debates broadcast in the audio-visual media; (iii) tools for collecting and detecting claims on social networks and audio-visual news media, which can provide links to fact-checks already published; and (iv) tools for verifying information in the context of YouTube and video fact-checks.

In addition to these four main types of tools, our interviewees also expressed four other peripheral needs. These include the accessibility of the tool on mobile devices, the clear presentation of the results to improve their readability, the provision of resources for archiving problematic content published on the web, already published fact-checks, or links to trustworthy websites, and the need for developing resources or providing tools more adapted to the Nordic specificities and languages.

Considering these practical implications, it's important to keep humans in the loop and respect the ethical principles and values of journalism. While fact-checking tools can be helpful, they cannot replace the judgement and expertise of human fact-checkers. Moreover, the tools should provide acceptable levels of explicability, allowing users to understand how they arrived at their conclusions. It's also crucial to consider the context of the fact, the news organisation, and the national context and language when fact-checking. Finally, it's important to consider the level of expertise needed to master the tools and ensure that they are used effectively.

[1] Until May 2022.

3. Summary of State-of-the-Art Image Verification Tools and Services

Until May 2022, we have found over 50 tools (our analysis of the fact-checking tools can be found here: Fact-checking tools database) available for Image Analysis, each with a different set of functionalities and capabilities. In our considerations, there are four widely used by the fact-checkers to address the challenges of Image Verification: *FotoForensics* (Ringwood, 2012), *Forensically* (Wagner, 2015), *Ghiro* (Tanasi & Buoncristiano, 2015), and *InVid-WeVerify* (Marinova et al., 2020).

Fundamentally, all of the analysed tools and services are providing conventional and popular methods, such as Metadata Extraction, Error Level Analysis, or Format-based Analysis. However, we found that implementations from categories like Geometric-based or Physics-based have not been showing up much in the tools. Learning from real daily routines of fact-checkers, we have known that analysis that explores physical artefacts or geometrical constraints are very important in image verification, especially to figure out when and where the photo/video has been taken (Khan et al., 2023). This suggests that there is room for innovation and development in this area.

With regards to the User Interface (UI), most tools share a standard interface due to the simple requirement from the user, which is to confirm the authenticity of the questioned image. Forensically provides an elegant design, including a significant area for the image and a list of methods. However, not many UIs, even Forensically, provide a straightforward description of the algorithms being used, which may create a high probability that the users will misuse, misunderstand, or misinterpret the result.

Furthermore, the tool needs to provide positive User Experience (UX) to keep the users engaged. Handling errors, being proficient in doing tasks, and ease of use are some of the few important aspects in the user experience field. Each existing tool has its own strengths and weaknesses in many different dimensions of UX. For example, FotoForensics shows a direct result to the users; it is fast and straightforward, but is static and not interactive enough.

Regarding Privacy, most tools provide their own privacy policy that users must follow. However, for some tools, there is a need for delivering the inputted image to the server side for further detection, which may make users' images vulnerable to attacks during the course to the server. Forensically is a Client-side only tool that users can use without an Internet connection, making it more secure in terms of privacy.

The details of the analysis can be found at (Tran et al., 2022).

4. FotoVerifier - A Platform for Image Verification

4.1. Goals and Objectives

At the core of our efforts is a focus on **developing tailor-made algorithms** and **stand-alone prototypes** that **provide fact-checkers with powerful and easy-to-use image verification tools**. Our goal is to enable fact-checkers to remain in the loop while seamlessly integrating with other platforms, all while respecting the ethical principles and values of journalism.

Building upon the previous analysis of user needs and the evaluation of state-of-the-art image verification tools and services (Sections 2 and 3), we have extended our core needs into the following specific objectives:

O1. The tools should support common image analysis tasks of fact-checkers, including identifying the source of an image and debunking imagery forgery.

O2. The tools should be developed as stand-alone prototypes to enable users to test them as proof of concepts. This approach will allow us to quickly iterate and refine our tools based on user feedback.

O3. The tools should be easily integrated into other existing platforms, such as Truly Media. This approach will allow us to seamlessly integrate with other tools and workflows, reducing the need for users to switch between different platforms.

O4. The tools should be easy to use and have comprehensive tutorials and guidelines. We understand that ease of use is critical to the adoption and success of our tools. As such, we aim to provide users with a seamless and intuitive experience, coupled with comprehensive tutorials and guidelines to ensure users can quickly become proficient in their use.

Given that, we developed **FotoVerifier**, *an online platform that provides fact-checkers with powerful and easy-to-use image verification tools*. All of our sources are published as open source and can be accessed on Github.

4.2. *The Components of FotoVerifier*

At this stage, FotoVerifier has been developed as a set of stand-alone open-source prototypes and serves as proof of concepts for our objectives. We have designed FotoVerifier to include several components, each of which aims to enhance digital image forensics in its own unique way.

FotoVerifier is being hosted at fotoverifier.eu as an online platform, and all its sources are available as open source on GitHub at https://github.com/fotoverifier/.

FotoVerifier platform consists of four components:

DeDigi

DeDigi is an online platform developed specifically for digital image forensics (DIF), offering a total of 5 common DIF methods: Error Level Analysis (Krawtez, 2007), JPEG-Ghost (Farid, 2009), Shadow and Reflection Consistency Test (Geometric-based and Physics-based) (Kee et al., 2013), Histogram Test (Kee et al., 2011), and Metadata Extraction (Kee et al., 2011). Further details of these methods can be found at (Piva, 2013). What sets DeDigi apart from other tools, e.g., the ones in Section 3, is that it includes both Geometric-based and Physics-based verification in its methods. This diversity helps extract and exploit various types of information in images to detect forgeries.

DeDigi is designed with privacy from the beginning, as it is a client-side only tool, meaning users do not need to upload their image and can use it without connecting to any server. Furthermore, DeDigi is written entirely in JavaScript, which allows it to be integrated into almost any platform. In addition, it takes into account user experience (UX) and user interface (UI) design to ensure a seamless and intuitive user experience. It also provides comprehensive guidelines to assist users in utilising the tool effectively.

Website: https://dedigi.fotoverifier.eu/

FotoVerifier

FotoVerifier is developed mainly based on DeDigi and is designed to serve as a comprehensive training system for users to learn how to verify images. It includes all five DIF methods and is also written in Javascript, which allows for easy integration with almost any platform, making it a versatile tool for professionals across different industries.

As there is always room for improvement, we implemented some machine learning experiments to enhance the detection methods (especially on Error Level Analysis and JPEG-Ghost). While this has the potential to improve the speed and ease of use for users, it is important to note that the experiment is still ongoing, and its impact on transparency and accuracy is yet to be fully determined.

Despite the ongoing experiment, FotoVerifier's tutorials and training exercises are designed to help users use the tool more efficiently and avoid any mistakes or misuse. The tutorials provide an acceptable level of explicability, enabling users to understand how the system arrived at its conclusions, and to increase their understanding of the DIF methods.

Website: https://www.fotoverifier.eu/upload

CLI

CLI (command-line interface) is a collection of Python scripts that offer a command-line interface for accessing the functionality of FotoVerifier. It is a versatile tool that can be used to perform various image analysis tasks, including detecting digital image manipulation and analysing image metadata. Thanks to popularity in machine learning of Python, CLI can be easily enhanced and updated to keep up with the latest developments.

With CLI, users can also easily integrate image analysis into their existing workflows or applications. For example, the CLI can be integrated with natural language processing (NLP) models to provide even more powerful fact-checking capabilities.

Overall, the CLI of FotoVerifier offers a powerful and flexible tool for digital image forensics that is easy to use, easy to enhance, and easy to integrate with other platforms and models. Its popularity and versatility make it a valuable addition to any developer or user's toolkit.

Website: https://github.com/fotoverifier/fotoverifier/tree/main/cli/cli

NameSleuth

NameSleuth is our new experiment, inspired by the increasing need for a verification tool that can specifically cater to social media platforms. With NameSleuth, we showcase the versatility of FotoVerifier, which allows us to seamlessly integrate new tools and features as per the changing requirements.

NameSleuth is an online tool that analyses social media platform traces from uploaded images. By examining the name of an image, NameSleuth offers fact-checkers additional insights into when and on which social media platform an image was uploaded (Dang-Nguyen et al., 2023). This functionality is critical for identifying and verifying the origin of images on social media, which can then be used to debunk misinformation and disinformation.

Website: https://namesleuth.fotoverifier.eu/

We would like to emphasise that FotoVerifier is continuously being developed and is currently at a very early stage. Developing a robust image verification tool requires collaboration between researchers and practitioners from multiple disciplinary areas. The field of media forensics is complex and challenging, and advancements in this field require constant innovation and adaptation. As such, we value and welcome feedback from users and stakeholders, which helps us to improve the platform and tailor it to the evolving needs of fact-checkers. We are committed to providing a user-friendly and effective tool that can assist fact-checkers in their vital work of verifying the authenticity of visual information.

5. Formative Evaluation

As mentioned, FotoVerifier is currently at a very early stage, and we welcome feedback from users and stakeholders, which helps us to improve the platform and tailor it to the evolving needs of fact-checkers. In this section, we report our formative evaluations on DeDigi (and its further development as FotoVerifier).

DeDigi and FotoVerifier are designed following Design Science. Our UI/UX Development cycle is by following three main phases in Nielsen's design iteration (Nielsen, 1992): Design, User feedback, and Evaluation. Our tool is user-centric, therefore, after a design for the product has been made, a feedback form is given to the users for their evaluation. The feedback form added with some extra information depending on the targeted reviewers and user interfaces. After getting all the necessary feedback, an evaluation on the form results were made to determine the next step in the upcoming design iteration. An example of the first three iterations is illustrated in Figure 1.

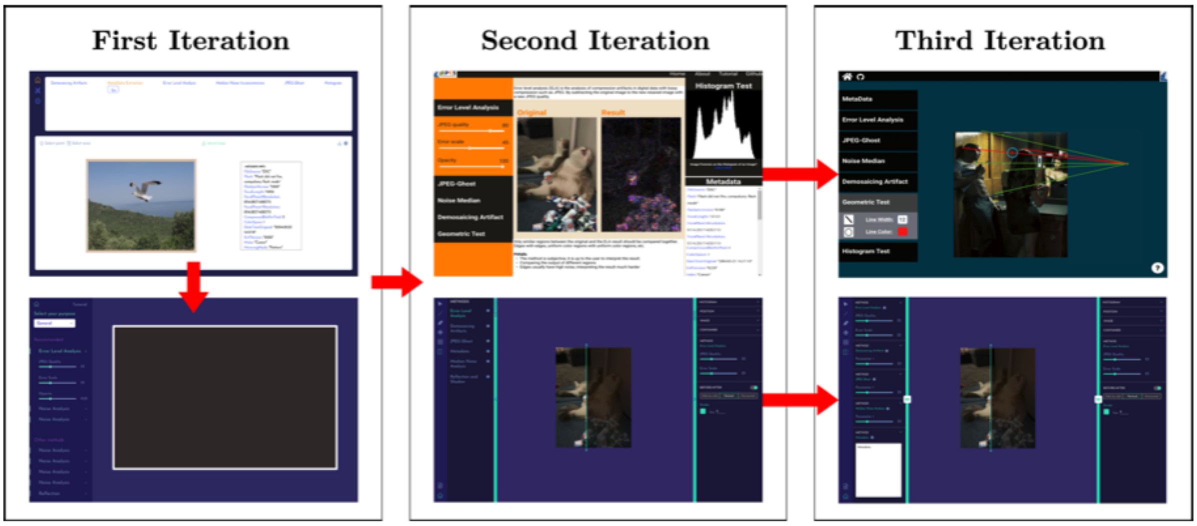


Figure 1. DeDigi's first three design iterations

In order to evaluate DeDigi in a consistent manner, we conducted a heuristic evaluation using Nielsen's heuristic evaluation framework (Nielsen, 1992). We applied the general principles of Nielsen's heuristics to assess the usability of our tool, and utilised a set of criteria to rate its performance on a scale of 1 to 5 (with 1 being the lowest score and 5 being the highest score), as shown in Table 1.

Table 1. Tool usability inspection based on Nielsen's heuristic evaluation for DeDigi.

No.	Principle	1	2	3	4	5
1	Visibility of system status			✓		
2	Match between the system and the real world				✓	
3	User control and freedom				✓	
4	Consistency					✓
5	Error prevention		✓			
6	Recognition rather than recall				✓	
7	Flexibility and efficiency of use			✓		
8	Aesthetic and minimalism in design					✓
9	Recognition, diagnosis, and recovery from errors		✓			
10	Help and Documentation			✓		

Additionally, we conducted final interviews with 30 users to gather input for future iterations of the product. The feedback form covered three sections: Occupation and Needs, User Interface, and User Experience. Overall, the UI section received an average score of 3.8 out of 5, while the UX section received an average score of 3.92 out of 5. Figure 2 summarises the users' original feedback on DeDigi's UI and UX, with further details available at (Tran et al, 2022).

User Interface	1 Very Poor	2 Poor	3 Average	4 Good	5 Very Good	Average
How do you feel about the UI in general?	0	3	5	15	7	**3.9**
Is the layout resonable?	0	0	7	14	9	**4.1**
Is the color scheme appropriate?	2	2	12	10	4	**3.4**
Other feedback **selected few*	- Icon on the left side should show fullname when hover mouse - Personally, I think a brighter theme would be more suitable - Relatively ok, user interface should have more specific description					

User Experience	1 Very Poor	2 Poor	3 Average	4 Good	5 Very Good	Average
From the UI, can you grasph how to use the tool?	3	0	6	12	9	**3.8**
What is your overall experience with the tool?	0	0	7	16	7	**4**
Are the methods easy to use?	0	0	9	11	10	**4**
Are the methods' results easy to interpret?	0	3	7	10	10	**3.9**
Is the tutorial page easy to understand?	0	3	5	15	7	**3.9**
Other feedback **selected few*	- Relatively ok, should have many version for diverse languages and more options - I still have not figured out what DeDigi is for, but the user interface is much better than I expected					

Figure 2. Feedback results of DeDigi

We received valuable feedback from the test users, which can be summarised as follows:

- The effectiveness of certain methods may be limited due to the wide range of possible forgeries, which require additional methods for detection.
- Images that have been passed through multiple social media platforms may be harder to detect due to recompression.
- For some methods that result in an altered image, interpretation may be difficult without prior knowledge of the field. Suggested solutions include providing a tampering probability score or a heat map.
- The current functionalities of the tool are difficult to use and not as robust as expected. Machine learning approaches can be used to improve these functionalities and provide a better user experience on our website.

As a summary, the formative evaluations conducted on DeDigi and its further development as FotoVerifier have been crucial in ensuring that the platform is user-centric and meets the evolving needs of fact-checkers. The UI/UX development cycle, following Nielsen's design iteration, has allowed for user feedback to be incorporated in each phase, resulting in a more effective and efficient tool. The heuristic evaluation using Nielsen's framework and final interviews with users have provided valuable insights into the usability and user experience of the tool, highlighting areas for improvement such as the need for additional methods for detecting forgeries, and the use of machine learning to improve the current functionalities. Overall, the feedback received from users has been instrumental in shaping the development of FotoVerifier, and we will continue to welcome feedback to ensure that the platform remains effective and user-friendly.

6. Conclusion and Way Forward

Objectives Assessment

Two deliverables “Tailor-made algorithms for fact-checkers” and “Stand-alone prototypes for fact-checkers” are presented as a single platform: FotoVerifier, which was developed to address the needs of user fact-checkers in image verification tools. It was developed based on an analysis of user needs, state-of-the-art image verification tools and services, and the requirement that the tools be easy to integrate into other platforms. FotoVerifier supports multiple image verification algorithms and considers both human-in-the-loop and digital media literacy.

We argue that the FotoVerifier fulfilled all four objectives described in Section 4:

O1. The tools should support common image analysis tasks of fact-checkers, including identifying the source of an image and debunking imagery forgery.

All four tools, DeDigi, FotoVerifier, NameSleuth, and CLI, have been designed to support common image analysis tasks of fact-checkers: DeDigi and FotoVerifier allow users to check the authenticity of images, while NameSleuth enables users to identify the original source, in particular - a post on common social media platform, of an image. CLI provides methods in detecting digital image manipulation and analysing image metadata.

O2. The tools should be developed as stand-alone prototypes to enable users to test them as proof of concepts.

All four tools have been developed as stand-alone prototypes. Furthermore, DeDigi and FotoVerifier were developed following a UI/UX development cycle, which allows us to tailor the tools to the evolving needs of fact-checkers.

O3. The tools should be easily integrated into other existing platforms, such as Truly Media.

All four tools have been designed to be easily integrated into other existing platforms: DeDigi and FotoVerifier can be integrated with Truly Media - a web based service - to provide a seamless experience for users as they are written in Javascript. CLI can also be integrated with other platforms via APIs, while NameSleuth can be used as a standalone tool to identify the original source of an image.

O4. *The tools should be easy to use and have comprehensive tutorials and guidelines.*

DeDigi and FotoVerifier have comprehensive tutorials and guidelines to ensure users can quickly become proficient in their use. CLI and NameSleuth, on the other hand, do not provide tutorials. However, they have been designed to be user-friendly and intuitive, with easy-to-use interfaces that require minimal training. In addition, we are committed to providing user support to ensure that users can use the tools effectively.

Overall, FotoVerifier contributes to the development and improvement of fact-checker tools by providing tailor-made algorithms, considering human-in-the-loop and digital media literacy, and being easy to integrate into other platforms. FotoVerifier is continuously being developed, with feedback and collaboration from experts in various fields.

Vision

Looking towards the future, our vision is to continue developing and improving our tools to provide fact-checkers with even more advanced and effective solutions for combating the spread of misinformation and disinformation.

Continued improvement and development of the tools: As the field of fact-checking and image analysis evolves, it will be important to continue to refine and improve the tools to keep up with changing needs and technological advancements. This could involve incorporating new methods for detecting forgery or expanding the scope of the tools to include analysis of other types of media.

Integration with additional platforms: While some of the tools are already integrated with Truly Media, there may be other platforms that could benefit from their capabilities. Expanding the integration options for the tools could make them more widely accessible and useful for a broader range of users.

Development of additional tools: While the current tools cover many common image analysis tasks, there may be other areas that could benefit from the development of new tools. For example, tools that can analyse video content or audio recordings could be useful in detecting deepfakes and cheapfakes (Examples of these problems can be found in (Khan et al, 2023)) or other forms of media manipulation.

Improving digital literacy: Another important future direction is to focus on improving digital literacy among users, particularly in the area of visual verification. We aim to provide comprehensive training and educational resources to help users develop the skills and knowledge necessary to effectively identify and debunk image forgeries. This can include online courses, workshops, and tutorials, as well as partnerships with educational institutions and media organisations to promote digital literacy and responsible journalism.

References

• Alessandro Tanasi and Marco Buoncristiano (2015). “Ghiro”. https://www.getghiro.org/

• Ringwood P. (2012). FotoForensics. http://fotoforensics.com.

• Wagner J. (2015). Forensically: Set of tools for Digital Image Forensics. https://29a.ch/photo-forensics.

• Marinova, Z., Spangenberg, J., Teyssou, D., Papadopoulos, S., Sarris, N., Alaphilippe, A., & Bontcheva, K. (2020, July). Weverify: Wider and enhanced verification for you project overview and tools. In 2020 IEEE International Conference on Multimedia & Expo Workshops (ICMEW) (pp. 1-4). https://mever.iti.gr/forensics/.

• Tran, C. H., Tran, Q. T., Long-Vu, Q. C., Nguyen, H. S., Tran, A. D., & Dang-Nguyen, D. T. (2022, June). DeDigi: A Privacy-by-Design Platform for Image Forensics. In Proceedings of the 3rd ACM Workshop on Intelligent Cross-Data Analysis and Retrieval (pp. 58-62).

• Dang-Nguyen, D. T., Sjøen V., Le D. H., Dao T. P., Tran A. D. & Tran M. T. (2023, January). Practical Analyses of How Common Social Media Platforms and Photo Storage Services Handle Uploaded Images. In Proceedings of the 29th International Conference on Multimedia Modeling.

• Farid, H. (2009). Exposing digital forgeries from JPEG ghosts. IEEE transactions on information forensics and security, 4(1), 154-160.

• Krawtez, N. (2007). A Picture’s Worth: Digital Image Analysis and Forensics. Black Hat Briefings, 131.

• Kee, E., Johnson, M. K., & Farid, H. (2011). Digital image authentication from JPEG headers. IEEE transactions on information forensics and security, 6(3), 1066-1075.

• Kee, E., O'Brien, J. F., & Farid, H. (2013). Exposing photo manipulation with inconsistent shadows. ACM Transactions on Graphics (ToG), 32(3), 1-12.

• Nielsen, J. (1992). The usability engineering life cycle. Computer, 25(3), 12-22.

• Piva, A. (2013). An overview on image forensics. International Scholarly Research Notices, 2013.

• Khan, S. A., Sheikhi, G., Opdahl, A. L., Rabbi, F., Stoppel, S., Trattner, C., & Dang-Nguyen, D. T. (2023). Visual User-Generated Content Verification in Journalism: An Overview. IEEE Access.

Appendix A. User Manual

1. DeDigi

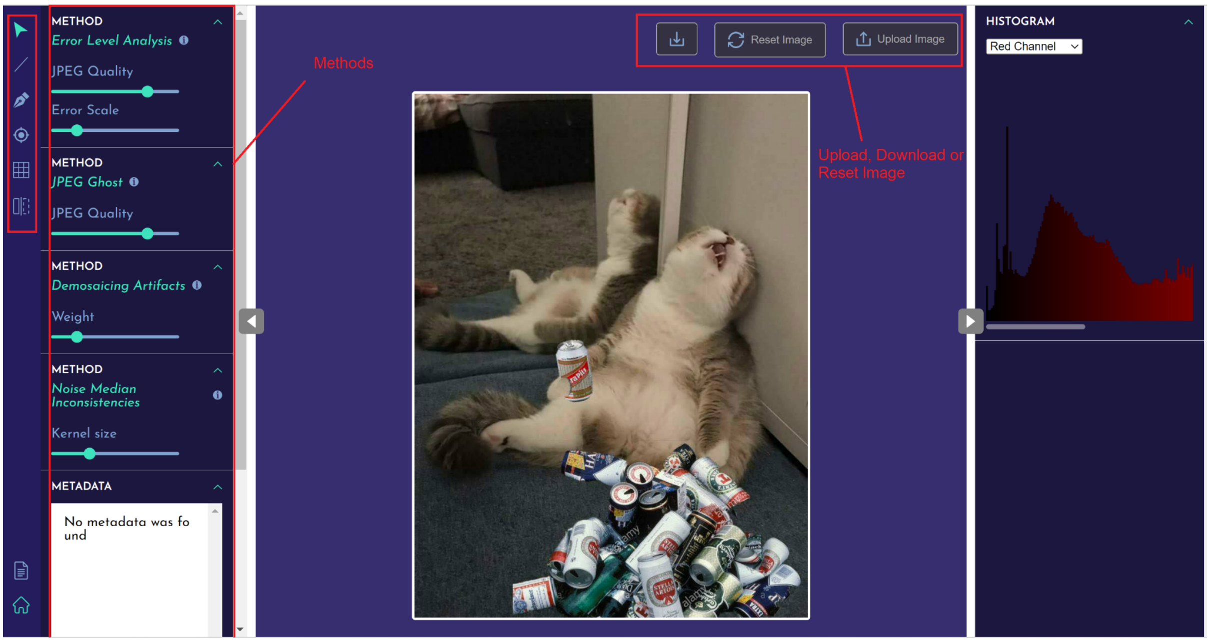
DeDigi is short for de-digitised, with the meaning being reversing the digital actions done on the original digital image.

The term de-digitised, if separated, will consist of "de" and "digitised". "de" means remove/reduce/opposite in English, and "digitised" can be viewed objectively as the tampering/editing actions onto a digital image - as in digitising further after that image has been captured on the digital camera.

DeDigi is a tool for detecting image tampering using Digital Image Forensics techniques, along with the techniques are some other functionalities which further enhance the user's engagement. With the goal of creating an actual environment for interacting with different DIF methods, DeDigi was created.

a. Basic Functions

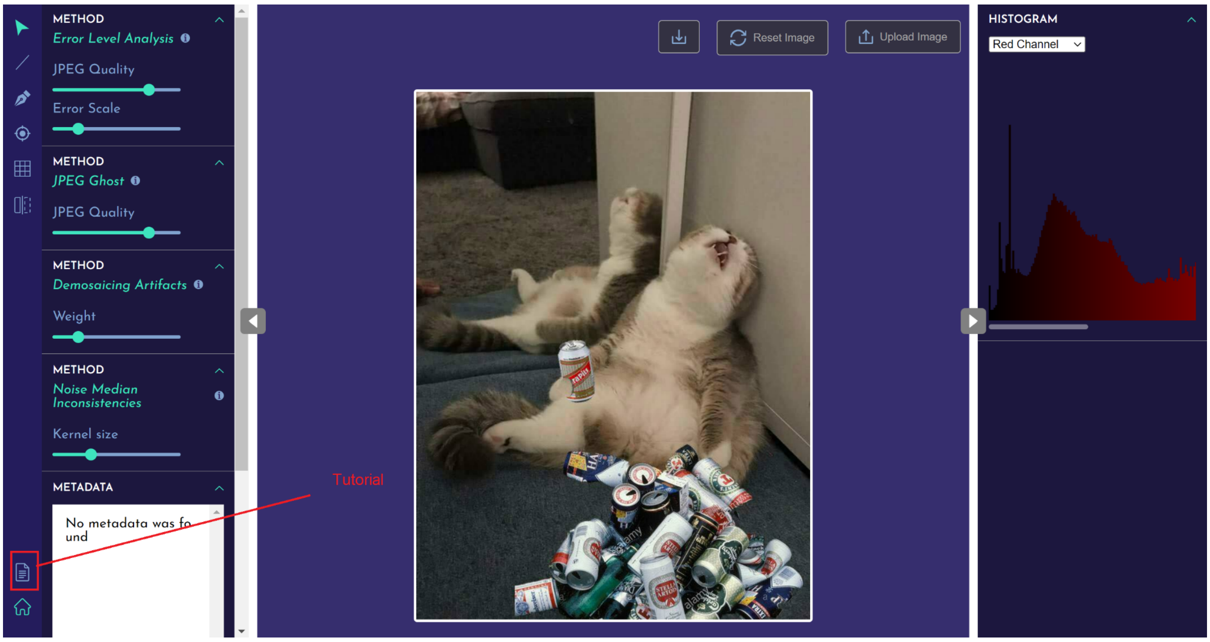
The user can upload, download and reset an image for analysis.



The tools and methods are on the left side of the website.

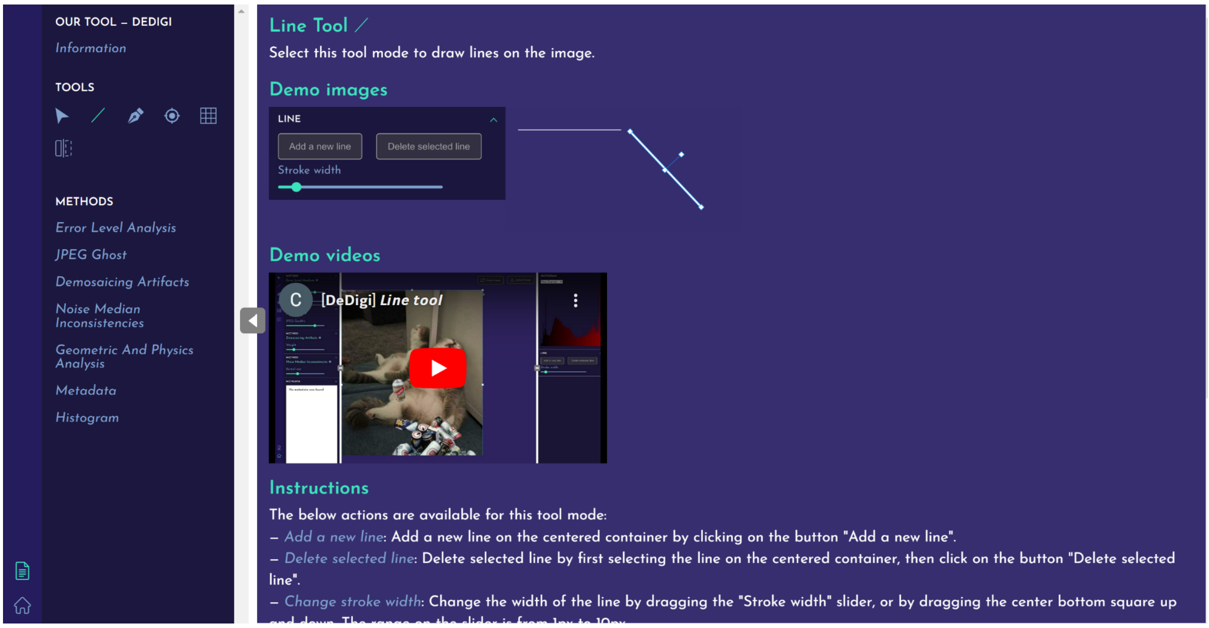
b. Tutorial

The user can check the tutorial of Dedigi via the Tutorial Page: https://dedigi.fotoverifier.eu/tutorial

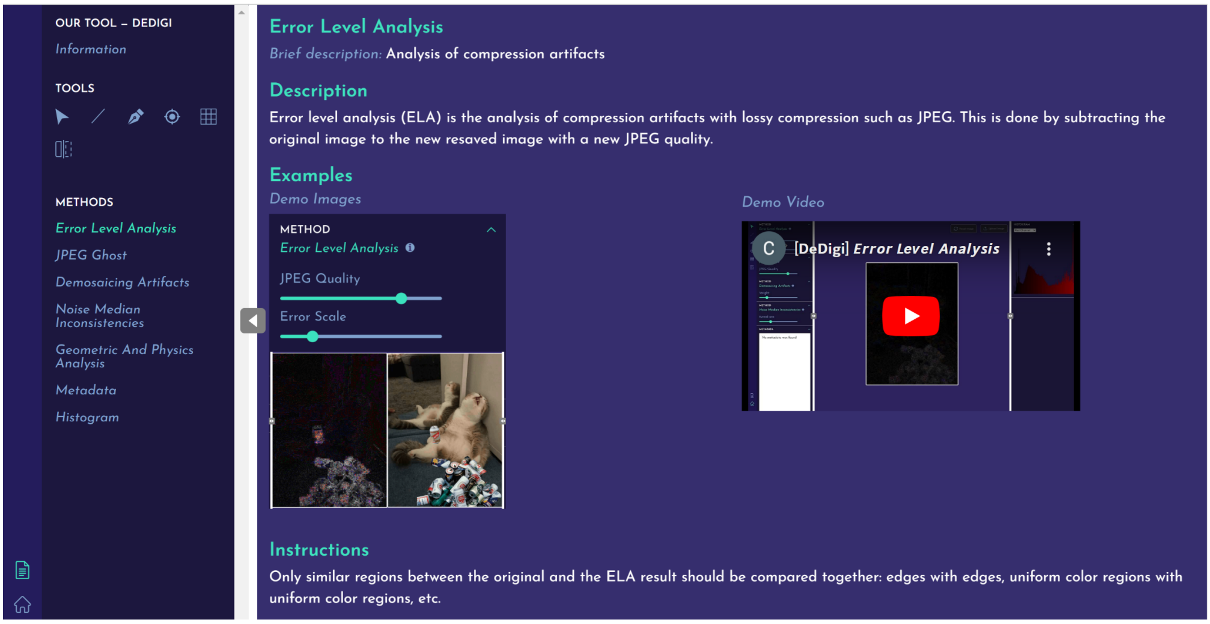


In the Tutorial Page, the user can explore the usage of each tool and image forensics method implemented in the Dedigi platform.

For example, the usage of Line Tool:



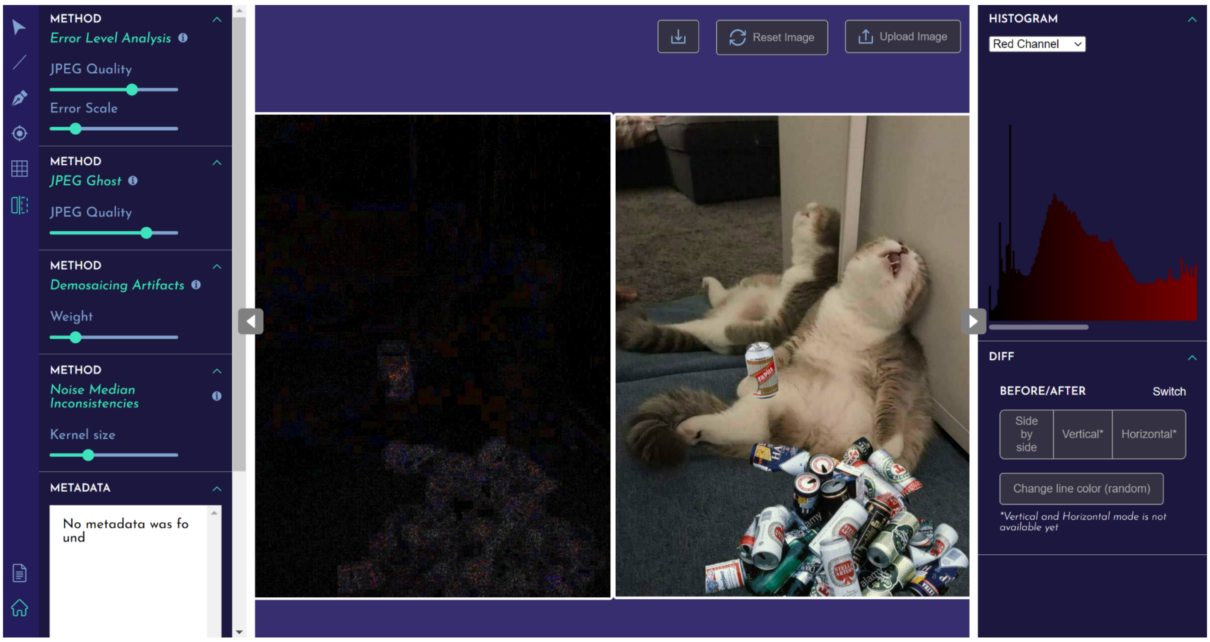
For example, the usage of Error Level Analysis:



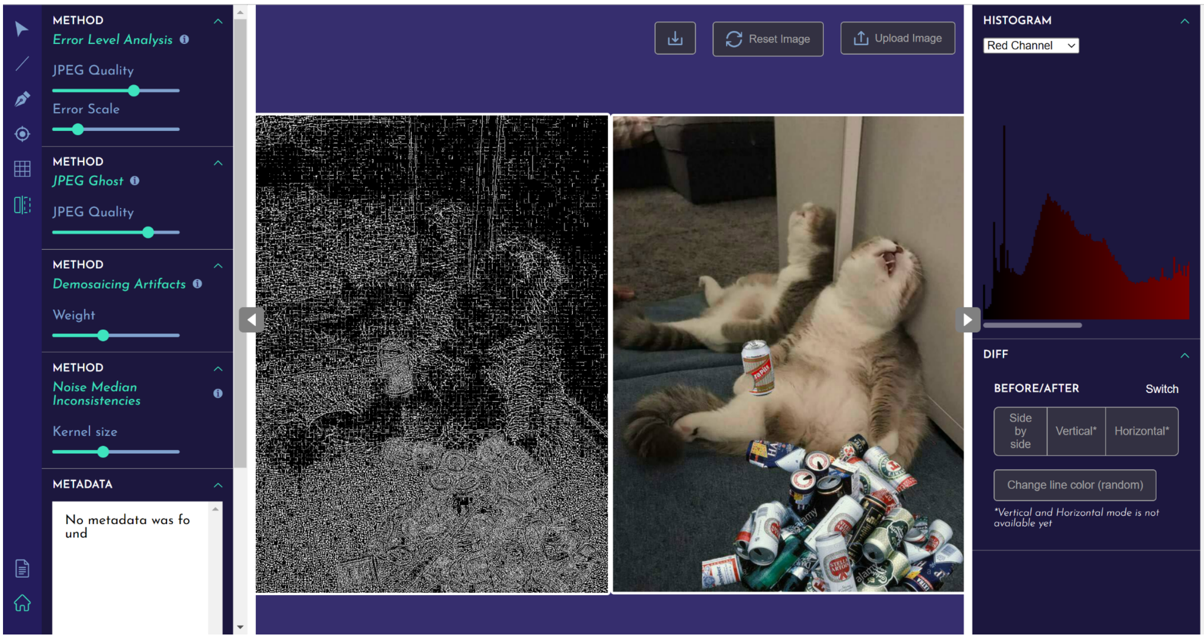
c. Analysis

The image forensics methods implemented in this platform include Error Level Analysis, JPEG Ghost, Demosaicing Artefacts, Noise Median Inconsistencies, Geometric And Physics Analysis, Metadata, and Histogram.

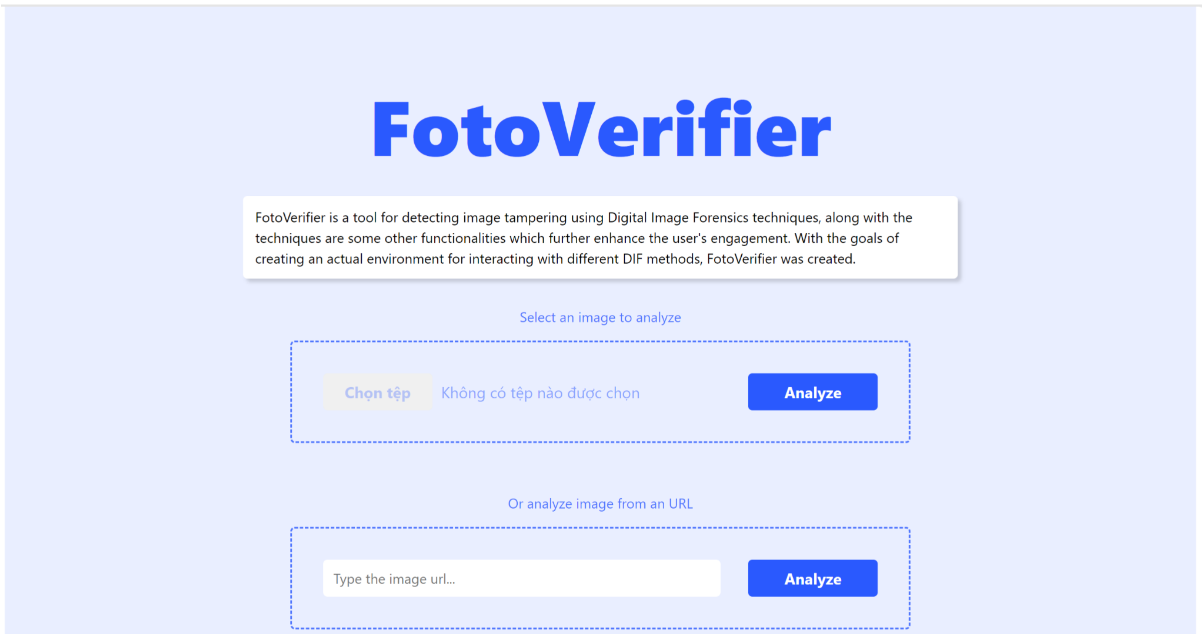
The user can upload an arbitrary image to the Dedigi platform and perform the image forensics method, for example, Error Level Analysis.



The user can customise the slider on the left panel to get a better view of the analysis. Based on the output, the user can make their own decisions.

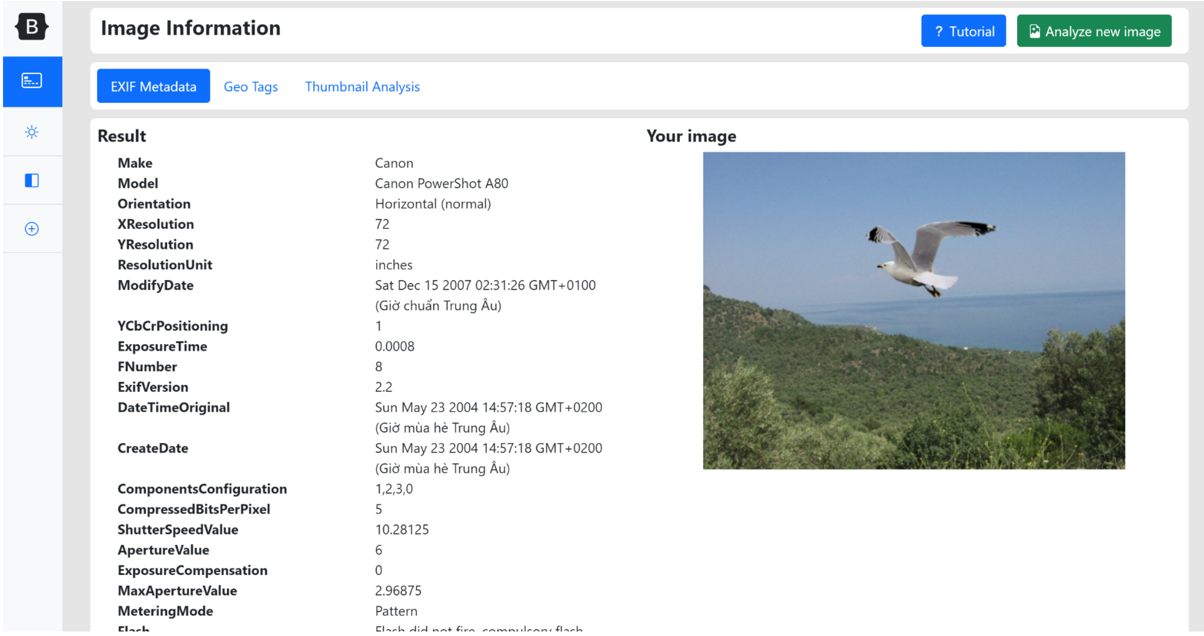


2. FotoVerifier



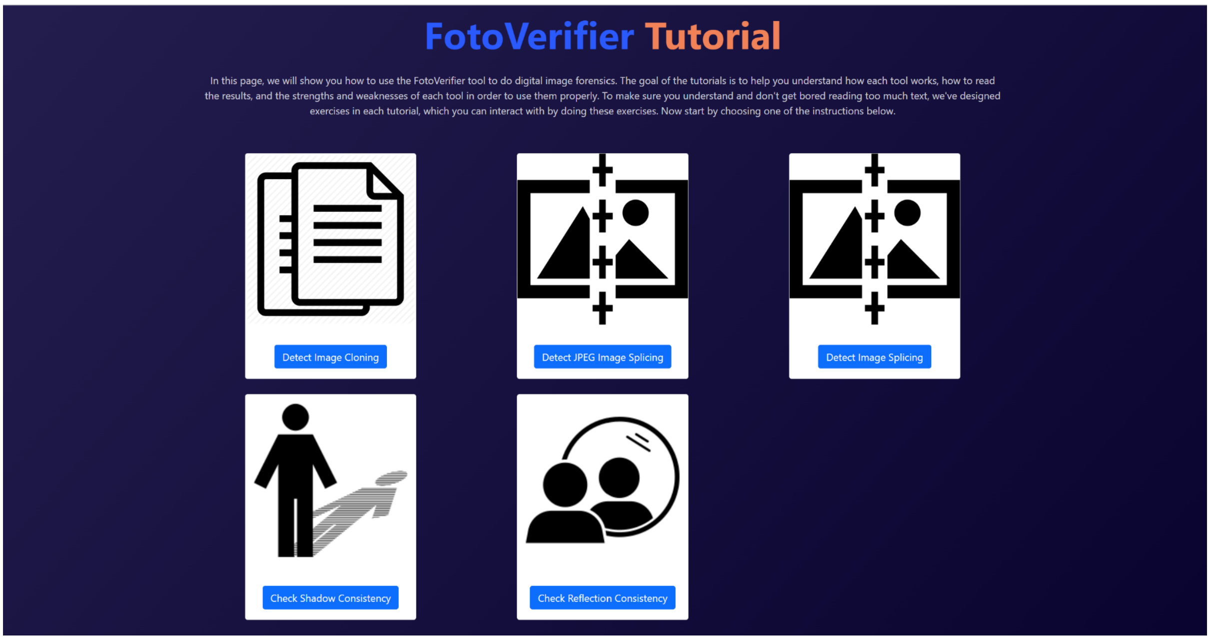
a. Analysis

The user can upload an image and perform simple analysis techniques.

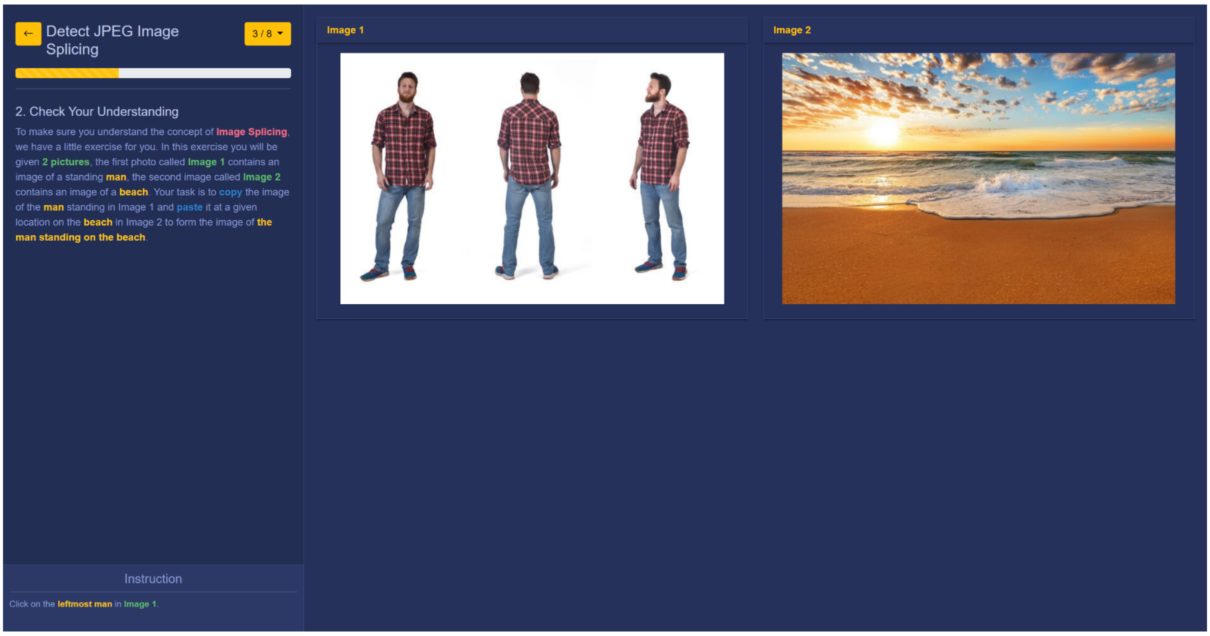


b. Tutorial

The primary function of this platform is the Tutorial section. In the Tutorial, user are trained to have the foundation background of image forensics. There are five series of tutorials implemented including Detect Image Cloning, Detect JPEG Image Splicing, Detect Image Splicing, Check Shadow Consistency, and Check Reflection Consistency.

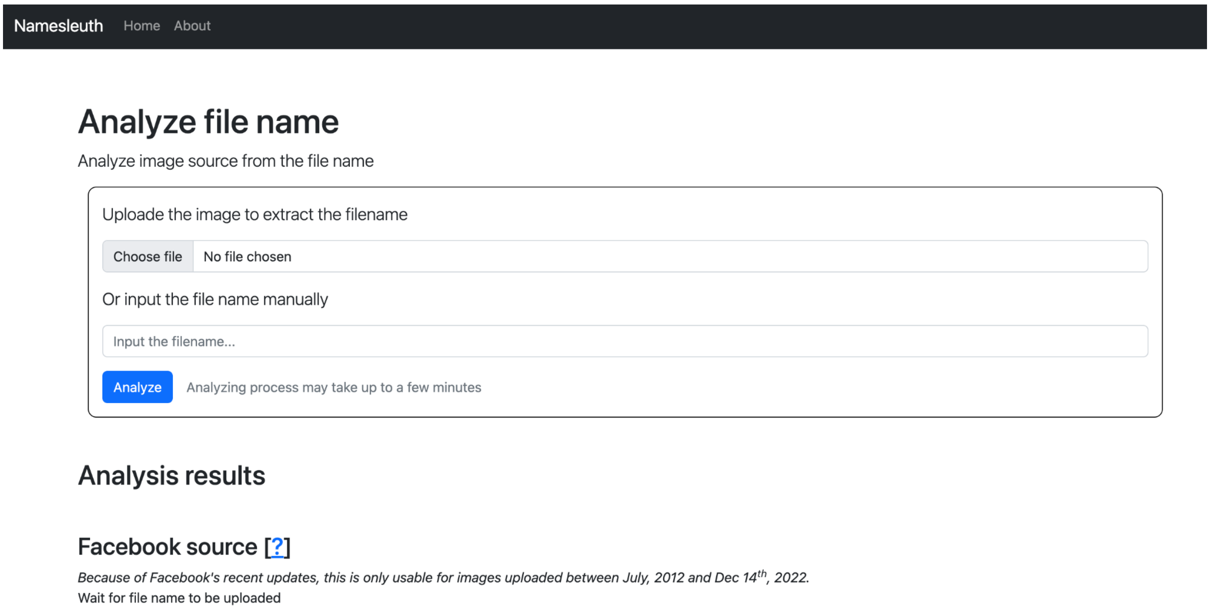


In each tutorial, the user is guided to every small step of the analysis. The instructions are on the left side and the interaction section is on the main page.



3. *NameSleuth*

With the NameSleuth tool, the user can upload an arbitrary image downloaded from social platforms (like Facebook, Flickr, or Reddit) to perform analysis and get the original post.



4. CLI Tool

This tool provides warnings and displays unusual information about the image, highlighting potentially manipulated regions to the users. Based on this information, users can make informed decisions.

Usage:

```
python foreimg.py [options] [-q QUALITY] [-s BLOCKSIZE] input
```

Positional arguments:

```
  Input                  name of the image file
options:
  -h, --help             show this help message and exit
  -e, --exif             exposing digital forgeries by EXIF metadata
  -gm, --jpegghostm      exposing digital forgeries by JPEG Ghost
                         (Multiple)
  -g, --jpegghost        exposing digital forgeries by JPEG Ghost
  -n1, --noise1          exposing digital forgeries by using noise
                         inconsistencies
  -n2, --noise2          exposing digital forgeries by using
                         Median-filter noise residue inconsistencies
  -el, --ela             exposing digital forgeries by using
                         Error Level Analysis
  -cf, --cfa             Image tamper detection based on
                         demosaicing artefacts
  -q QUALITY, --quality QUALITY           resaved image quality
  -s BLOCKSIZE, --blocksize BLOCKSIZE     block size kernel mask
```

A detailed instructions can be found on the Github website.

Appendix B. Implementation Instructions

DeDigi and FotoVerifier

Pre-installation requirements

- Operating system: Ubuntu 18.04
- NodeJS 16.16.0 LTS
- Docker 20.10.16

Instructions to deployDeDigi/FotoVerifier at localhost

- Step 1. Install Vue
  - Run command `npm install vue@latest`
- Step 2. Install the frontend server
  - Go to `DEDIGI/SOURCE/frontend/dedigi` folder
  - Run command `npm install`
  - Then run the `command npm run serve` to start the frontend server
  - When the frontend server starts up, it will get the frontend access address on the console window
- Step 3. Install the backend server
  - Go to folder `DEDIGI/SOURCE/backend`
  - Run the command `docker build -t dedigi_api .` to build docker containers
  - After building docker container, run command `docker run -dp 8888:8888 dedigi_api` to start dynamic backend server
- Step 4. Visit the website at the address shown in the console of the frontend server

CLI Tool

Pre-installation requirements

- Python 3
- PIP
- Python Libraries: Exifread, Opencv-python, Progressbar2, Numpy, Scipy, Pillow, PyWavelets, Matplotlib

Or, Simply run command to install the packets:

```
./install_packet.sh
```

NameSleuth

Pre-installation requirements

- Python 3
- PIP

Instructions to deploy NameSleuth at localhost

- On Linux/MacOS:
  - ./dev.sh
- On Windows:
  - ./dev.ps1
- Using Docker:
  - ./run.sh
  - The **NameSleuth** is hosted at port: 3002