DeGigi: A Privacy-by-Design Platform for Image Forensics

Quynh-Chau Long-Vu[1*], Hai-Son Nguyen[1⋆],
Anh-Duy Tran[1], and Duc-Tien Dang-Nguyen[2]

[1] Faculty of Information Technology, University of Science,
Ho Chi Minh City, Vietnam
{lvqchau,nhson17}@apcs.vn
taduy@fit.hcmus.edu.vn
[2] University of Bergen, Bergen, Norway
ductien.dangnguyen@uib.no

Abstract. With the explosion of multimedia has come the rise of advanced image processing and free editing tools, allowing individuals to readily change how an image or video appears in front of other eyes. This act is malicious and may cause disruption in the community; therefore, to resolve these issues, there has been many existing tools that use Digital Image Forensics (DIF) techniques. Even so, based on our MUUP evaluation system, these tools can lack guidance, difficult to utilize and can have privacy issues. Following that, we then investigate existing algorithms from various DIF techniques. Based on the previous points, we then incorporate this knowledge into our DIF web tool - DeDigi. For DeDigi's design, based on our Design Science system, each design iteration will take into account user feedback on how the tool's design is perceived from their perspective. The final outcome of our "privacy-by-design" tool is seven approaches from various categories of the focused field, two interaction functionalities, and a score of 3.92/5 for DeDigi (beta)'s user experience.

Keywords: Digital Image Forensics · Forgery detection tool · Privacy by design · Design Science

1 Introduction

There are more than 3.2 billion images, and 720,000 hours of video are shared online daily [14]; therefore, digital images or video frames are considered a primary means of communication on the World Wide Web. The abundance of digital images creates a disturbing problem for performing forensic on digital photos, and especially in this era, where a digital image may readily be created to convey misinformation and sometimes for malicious purposes. Misinformation, intentionally or unintentionally, could lead to a wide range of consequences that affect individuals' lives, social societies, or even governments on a global

⋆ These authors contributed equally

scale. According to the 2021 Edelman Trust Barometer [2], trust in social media feeds declined by 15% between 2020 and 2021, decreasing from 40% to 35%, indicating the community's loss of trust in social media feeds.

With the current situation of misinformation, and malicious attempts to alter photos or recordings, a solution is required. To address these issues, a sub-field of multimedia security known as Multimedia Forensics aims to detect forgery in images, videos, and audios. Our paper focuses on Digital Image Forensics (DIF), a sub-field of Multimedia Forensics that focuses extensively on digital images.

For the current tools applying DIF techniques, despite their existence, they have not been well-known in the market. These tools were designed for image manipulation checking, a wide-known problem for journalists, fact-checkers, politicians, celebrities, or even the public. Nevertheless, the tools remain known only for a small community of experts who have sufficient knowledge on the topic. Most of the tools, in our consideration, lack guidance. Furthermore, and regrettably, they are difficult to utilize and can be abused. Additionally, the procedures used on these equipment are preferably more suitable for laboratory settings. [12]

Seeing the lack of an easy-to-use DIF tool and the lack of methods from other DIF categories such as Geometric-based or Physics-based methods, we proposed a Digital Image Forensics web tool named **DeDigi**, focusing on detecting forgery using image content (Image Authenticity). The tool's primary focus is on user privacy and improving User Interface (UI) and User Experience (UX), therefore broadening the kind of users who require DIF but lack the essential DIF knowledge. For usability evaluation, the UI/UX development cycle combines real-user feedback and Nielsen's heuristics (1994)[9].

Furthermore, with the development of information security, an increasing number of consumers are becoming hypersensitive to concerns with their data. To address user data privacy, our tool will solely function on the client-side without transmitting or receiving data from the server. In short, it is a **"privacy by design"** image forensic platform.

Our main contributions are:

- Research and evaluate existing DIF tools on the Internet using the MUUP evaluation system created by the authors.
- Generate six user interfaces in three design iterations.
- Study users' UI feedback for the second and the final design iterations.
- Re-evaluate our system using Nielsen's heuristic evaluation.
- Create a DIF tool with user privacy as its main concern - DeDigi.

The content of the paper is organized as follows. In Section 2, we examine several existing DIF tools on the Internet, then apply the MUUP assessment criteria to determine the present state of those DIF tools. In the next three sections, we propose a DIF tool of our own, DeDigi. Section 3 discusses DeDigi's methodologies, Section 4 describes the UI/UX development cycle of DeDigi, and Section 5 describes the project structure or the architecture of DeDigi. Finally, in Section 6, we conclude and present open problems for future work.

2 Analysis of existing tools

2.1 Existing tools

On the market, there are currently over 50 tools [11] available for Image Analysis, each with a unique set of functionalities and capabilities. And they all focus on a common issue for their tool's users: confirming the authenticity of the questioned image. In our considerations, there are four widely used, open-source (except for Forensically), and available programs to address the challenge of Digital Image Forensics; they are *FotoForensics* [13], *Forensically* [15], *Ghiro* [1], and *WeVerify* [16].

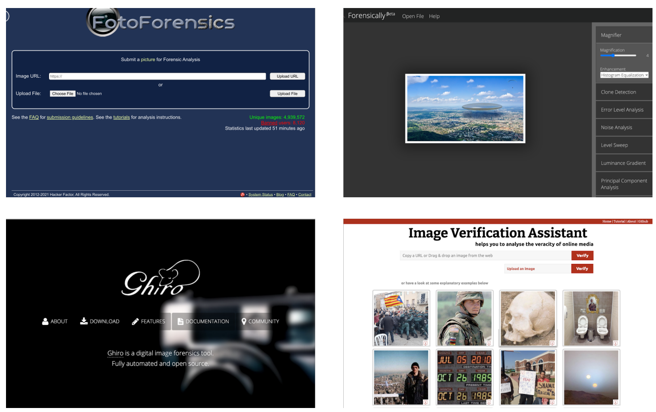

Fig. 1: FotoForensics *(top-left)*, Forensically *(top-right)*, Ghiro *(bottom-left)*, and WeVerify *(bottom-right)*

FotoForensics was re-created in 2012 by Hacker Factor after Mr. Ringwood, the owner of the site errorlevelanalysis.com, a free website service where people could upload photos and web pictures for analysis, took down his site. The Hacker Factor decided that the basic principle of the service is inherited: a free service that introduces photo forensics, which came from Pete Ringwood himself.

Forensically was publicly released on the Internet on August 16th, 2015. Forensically is a wonderful high-end collection of tools for digital image forensics developed individually by Jonas Wagner, one of many hobby projects of his, containing a set of free tools for digital image forensics. The website is still fully operational with lots of users and sometimes new updates.

Ghiro is a fully automated digital image processing for forensics purposes. It is designed to run a large number of images and generates a neatly structured report at the end of the forensics process. Using a user-friendly and fancy browser-based application for displaying. There are two options when using Ghiro: download the tool from the main page and set it up on your own, or go to the URL that Jekil and Burlone host at imageforensic.org and submit your photo there.

WeVerify is a professional platform that hosts a variety of smaller projects. One of them is Image Verification Assistant, developed in previous EU projects under the name Reveal. At WeVerify, the Reveal project is maintained and extended, with more algorithms added to the tool and an updated User Interface (UI) for better User Experience (UX).

2.2 Analytics - the MUUP evaluation measurement

The evaluation measurement consists of four main points, alias as ***MUUP***. They are: **M**ethods, **U**ser Interface (UI), **U**ser Experience (UX), and **P**rivacy. In summary, the current state of existing Digital Image Forensics tools on the Internet, as determined by the MUUP measurement, is demonstrated in Table 3. In Table 3, along with the evaluation of the 4 mentioned tools in Section 2.1, we also provide further evaluation on our own tool - DeDigi. For further notice, readers should consider that the MUUP measurement is developed subjectively and solely based on the authors' standpoint. Therefore, mistakes are inevitable. We welcome any feedback on improving the quality and quantity of the evaluation measurement.

For the analysis of **Methods**, after careful analysis, we have discovered that the two tools which are Forensically and Image Verification Assistant from WeVerify, are applying some of the conventional and popular methods, such as Metadata Extraction and Error Level Analysis. However, even with the current popularity and widespread use of these tools, implementations from categories like **Geometric-based** or **Physics-based** have not been showing up much in the tools.

With the **UI** of the tools, 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. Moreover, there is no distraction created by other methods while using a singular method, along with this is high interactivity over the parameters used in each algorithm. Even so, not many UIs, even Forensically, provide a straightforward description of the algorithms being used; therefore, creating a high probability that the users will **misuse**, **misunderstand**, or **misinterpret** the result.

Further on, besides UI, the tool needs **UX** to provide positive experiences and flow which keep the users in their website. As such, handling error, being proficient in doing tasks, ease of use, are one of the few important aspects in the user experience field. Based on this, each existing tool mentioned 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, straightforward, but is static and is not interactive enough.

With the case of **Privacy**, most tools provide their own privacy policy that users must follow. Additionally, for certain tools, there is a need for delivering the inputted image to the server side for further detection; thus, making users' images vulnerable to attacks during the course to the server. However, for

Forensically, it is a *Client-side only* tool that users can use without an Internet connection.

To sum up, the result of the analysis above which summarizes the strengths and weaknesses of existing DIF tools, is the groundwork for designing and implementing our tool - DeDigi.

3 DeDigi: Methodology

Our web tool for Digital Image Forensics is a browser-based tool and is named DeDigi. DeDigi is short for de-digitalized, meaning reversing the digital actions done on the original digital image. Ultimately, DeDigi is a tool for detecting image tampering using DIF techniques and is implemented with other techniques and functionalities that further enhance the user's engagement and create an actual environment for interacting with DIF methods.

DeDigi consists of seven methods, they are:

- Error Level Analysis (Format-based) [6]
- JPEG-Ghost (Format-based) [5]
- Demosaicing Artifact (Camera-based) [3]
- Geometric and Physics Test (Geometric-based and Physics-based) [10]
- Histogram Test [4]
- Metadata Extraction [7]

Methods such as Error Level Analysis and Metadata Extraction are among the most commonly utilized in existing Internet tools. Others are chosen because they are reliable and simple to implement, but they are rarely found in DIF tools.

Comparing only these methods with the list of other DIF tools described in Section 2; the following table shows the results of the method comparison:

Method	Foto-Forensics	Forensically	Ghiro	WeVerify	DeDigi
ELA	✓	✓	✓	✓	✓
Metadata	✓	✓	✓	✓	✓
JPEG Ghost				✓	✓
Noise Median Inconsistencies		✓		✓	✓
Demosaicing Artifact					✓
Geometric and Physics Test					✓
Histogram Test					✓

Table 1: Method overview of different DIF tools

The method *Geometric and Physics Test* takes advantage of realistic physics properties such as reflection, light, or shadow consistent in the real world. Through some modification procedures, the altered digital image may leave behind artifacts inconsistent with real-world physics.

By drawing lines between objects and checking common properties such as Reflection Vanishing Point, Reflection Line Midpoints [10], or Shadow Consistency from a Direct Light Source, [8] the image's authenticity could be determined.

The *Histogram Test* technique [4] looks at the Histogram of the digital image to discover Double JPEG Compression. After a high-quality JPEG compression is made on the digital image, the process is repeated with a lower JPEG quality; thus, producing a Histogram with up and down bars consecutively next to each other. In contrast to the preceding process, a low-quality JPEG compression on a digital image is performed, followed by a higher-quality compression, resulting in a Histogram with absolute zero appearing between the bars.

4 DeDigi: UI/UX Development Cycle

In this section, we introduce the tool DeDigi and its UI/UX development cycle, we have created six user interface (UI) designs during the design process, and these designs are separated into three iterations. Each is unique in its own way; some designs have gone through the product development phase but have to come to a halt as the requirements for UI/UX change along the way. For the second iteration, a user feedback analysis will be provided based on the third and fourth designs, and this analysis acts as the input for the final iteration. Below are the six user interfaces designed for the tool.

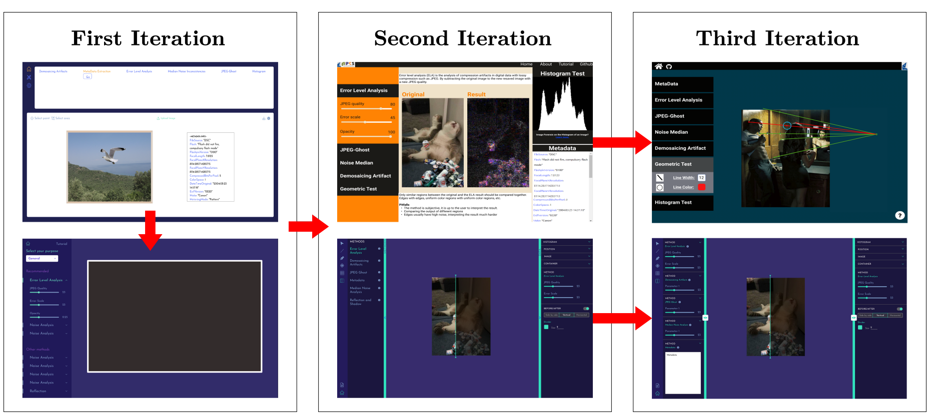

Fig. 2: DeDigi's design iterations

4.1 Design Science

The **Design Science** for our UI/UX Development cycle is by following three main phases in a Design Iteration: **Design**, **User feedback**, and **Evaluation**. Our tool is user-centric, therefore, after a design for the product has been made, a feedback form will be given to the users for their evaluation of the current design. The feedback form will be added with some extra information depending on the targeted reviewers and user interfaces. After getting all the necessary feedbacks, an evaluation on the form results will be made to determine the next step in the upcoming design iteration.

4.2 First Design Iteration

For the first iteration, two designs of similar color schemes are created – with dark purple as the primary color. **The first UI** is a fully functional prototype with hard-coded parameters for a few DIF methods and acts only as a demo product, a prototype. After going deeper into the DIF field and its existing tools on the Internet, we create **the second UI** with a tutorial page to make it easier for users with no background knowledge to understand what our product does. The second design has changed in terms of UI responsiveness and provides a better user experience (UX) than the first one, with adjustable parameters for DIF methods.

4.3 Second Design Iteration

In the second UI development cycle, each author creates a UI of their own – Orange UI and Purple UI. The **Orange UI** is divided into three sections, with adjustable parameters on the left sidebar, static information such as Histogram and Metadata on the right sidebar, and at the center is the image.

The **Purple UI** consists of four sections which are aligned as vertical bars to enhance users' overall usage. The first vertical bar contains icons for tool objects and navigation purposes; the second bar consists of DIF methods; the bar on the right-hand side shows histogram and adjustments tool.

After finishing the two designs, a **User Interview** is conducted with questions based around colors, information, size and spacing, etc., to engage real user involvement since our product is based upon the users, and for the users. After the interview, we come to a conclusion, as shown in Figure 3, where the chart will be displayed using two vertical bars, representing the Orange UI and the Purple UI, and the points are based upon the 5 aspects with points from 0 (lowest) to 5 (highest).

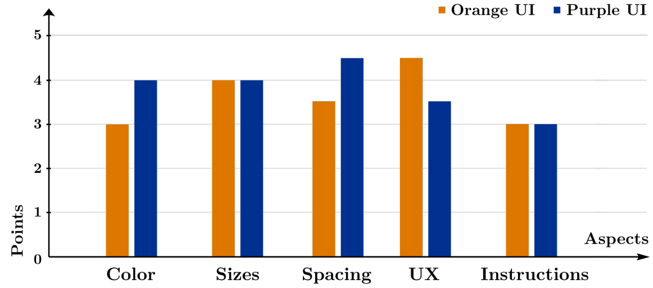

Fig. 3: Design interviews' results based on five aspects

4.4 Final Design Iteration

In the third iteration, each member uses the feedback in the second iteration to alter the previous UIs. The Orange UI - now renamed to **Sherpa Blue UI** has a whole new look to it, whilst the **Purple UI 2.0** remains unchanged and is nearly identical to the original Purple UI.

After careful consideration, we determine that the new Purple UI version – **Purple UI 2.0** – is a preferable choice for creating the DIF tool in this paper. As a result, we make it our final design and begin the product development process, transforming the design into a fully functional product.

4.5 Nielsen's Heuristic Evaluation

To analyze DeDigi's final design in a more uniform manner, a heuristic evaluation with the goal of generic usability testing –Nielsen's heuristic evaluation [9] – is used. For our present tool, we are using the general principles of Nielsen heuristics to define the product's usability. In Nielsen heuristics, we use a set of criteria to assess where our product is at in terms of usability, on a scale of 1 (lowest score) to 5 (highest score), as indicated in Table 2.

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			✓		

Table 2: Tool usability inspection based on Nielsen's heuristic evaluation

5 DeDigi: Project structure

5.1 Use cases

After going through the designing process, we have analyzed the use cases of possible interactions that a user can perform on our tool. The five main use cases are:

- *Upload an image*: User can upload a new image for forensics
- *Change a DIF method's input*: User can use sliders or input boxes to adjust the value passed into the method
- *Run a DIF method*: User can run the method to view the effect of that method on the original image
- *Draw objects*: User can draw lines, circles, paths onto the image and can rotate or resize them
- *View tutorial*: User can view the detailed description of the tool's methods

5.2 ReactJS - Javascript

For client-side rendering, the project uses **ReactJS with JavaScript (JS)** as the programming language. Python can also be used alongside ReactJS instead of JS; however, the support for this duo has not been fully supported. As a result, we choose JS better to incorporate the Document Object Modeling (DOM) handling to make changes to the inputted image in ReactJS. In the project, we are also using **Strategy pattern** to manage the execution of DIF techniques.

5.3 Client-side only

When handling a digital image on a normal DIF tool, DIF techniques will be applied onto the image data, allowing computations to be done on the server-side for better rendering. However, to ensure protection against attack during the path from client-side to server-side and to safeguard the privacy of inputted images, we decide **not to use a server** and will instead execute relevant algorithms on the client-side. Therefore, DeDigi will be a **"privacy by design"** DIF platform.

6 Results and Conclusion

In this section, we first gives a concise overview of the user's feedback for the final product - DeDigi Beta version. Afterwards, we will conclude the process and the extended future work of this project.

6.1 User feedback for DeDigi - Beta version

After completing the final production, we conduct a final interview with the users to get input for the next phase of the product, possibly in the near future. **Occupation and Needs**, **User Interface**, and **User Experience** are the three sections of the feedback form. The original viewpoint of the users for DeDigi (Beta) is displayed accordingly in the mentioned sections as in Figure 4.

- *Occupation*: Out of all 30 reviews, **1/30** is a Chef, **1/30** is a Construction-related job, **1/30** is an ERP Technical Consultant, **2/30** are Photographers, **2/30** are Journalists, **7/30** are Software-related jobs, and **16/30** are Academic-related.
- *Needs*: For user's job that requires DIF, **16.7%** of users answers Yes. For user's needs of DIF, **36.7%** of users answer Yes.
- *User Interface*: Overall score for all aspects in UI section is **3.8/5**.
- *User Experience*: Overall score for all aspects in UX section is **3.92/5**.

6.2 Discussion

During our studies, we have concluded certain limitations of our chosen methods, along with some drawbacks of our web tool - DeDigi. Below we list out a few of the limitations and drawbacks which we deem important and is in need of an update to resolve these three main issues:

- *Methods are not effective in every scenario*: While using certain methods, the result might not be effective because there is a wide range of possible forgeries requiring another set of methods. Moreover, when an image is passed through many social media platforms, a distinct type of compression of that social media will be applied, causing the final image to be re-compressed many times and is harder to detect.

- *Results are difficult to interpret*: For methods resulting in another image being applied with DIF techniques, the result can be hard to interpret if the user does not have prior knowledge of this field. Some of the suggested approaches can be to apply a tampering probability score or a heat map.
- *The web tool lacks functionalities and actions for the user*: The current functionalities of the tool are still hard to use and are not as robust as expected. Due to this, these functionalities can be improved further using Machine Learning approaches to detect certain aspects or hints, assisting the user in their overall experience while at our website.

6.3 Conclusion

In this paper, we evaluate existing tools with the MUUP evaluation system, study different methodologies in DIF, and design User Interfaces for the product. Our main contribution is a tool specific for the purpose of detecting manipulation on digital images – *DeDigi*, focusing on user privacy and their experience while examining a digital image. The tool consists of 7 total methods coming from different categories in Digital Siginal Processing field of Image Authenticity techniques — Format-based, Camera-based, Geometry-based, and Physics-based. Moreover, we have gone through three design iterations based on the Design Science we specified in this paper. And as result, we have organized two user feedback sections for the Second Design Iteration and the Beta version of DeDigi, with the final result from 30 users to be 3.82% for both UI and UX.

For *performance and sustainability*, possible extended work for this project is applying more DIF techniques and adding other drawing functionalities that are yet to be done. At the same time, we will increase the performance of the existing methods in both time complexity and the final result. Moreover, for improving user experience while using the provided methods, a few of our future works are Tampering visibility, Social media files' analysis, Edge detection, Line mapping, Automation for Geometric and Physics Analysis (Machine Learning).

The tool - DeDigi is hosted at https://dedigi.herokuapp.com[⋆⋆⋆].

[⋆⋆⋆] Last updated: Sep 2021

	Methods	**UI**	**UX**	**Privacy**
FotoForensics	Few methods Lack methods from different categories	Outdated UI	Easy to use Lack interactive support	Has Back-end processing
Forensically	Variety of methods	Mordern UI Great UI	Lack instructions on the methods	Client–side only tool
Ghiro	Lack methods from different categories	Simple UI	Easy to use Lack interactive support	Has offline version Web–version: Has Backend processing
WeVerify	Variety of methods Up–to–date methods	Mordern UI	Complex system	Has Back-end processing
DeDigi	Variety of methods	Mordern UI	Easy to use Has instructions	Client–side only tool

Table 3: Summary of the current state of some of the DIF tools on the Internet

Interviewee's occupation	**Undergraduate/ Student**	**Fresh Graduate**	**Software-related**	**Photographer**	**ERP Technical Consultant**	**Journalist**
	11	**5**	**7**	**2**	**1**	**2**
	Construction-related	**Chef**				
	1	**1**				

Occupation and Needs	Yes	No	% of Yes
Does your job requires DIF?	5	25	**16.7**
Do you yourself need DIF?	11	19	**36.7**

Occupation and Needs	**1** Never	**2** Rarely	**3** Sometimes	**4** Often	**5** Always	**Average**
Your interest in detecting forgery in images	4	4	7	12	3	**3.2**

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					

Fig. 4: Feedback results of DeDigi (Beta)

References

1. Burlone, J.: Ghiro as a web service. https://www.imageforensic.org/
2. Daniel J. Edelman Holdings, I.: 2021 Edelman trust barometer
3. Dirik, A.E., Memon, N.: Image tamper detection based on demosaicing artifacts. In: 2009 16th IEEE International Conference on Image Processing (ICIP)
4. Eric Kee, D., James O'Brien, B.: Seminar: Photo Forensics at Dartmouth's Jones Seminars on Science, Technology, and Society
5. Farid, H.: Exposing digital forgeries from jpeg ghosts. IEEE transactions on information forensics and security **4**(1), 154–160 (2009)
6. Gunawan, T., Hanafiah, S., Kartiwi, M., Ismail, N., Za'bah, N., Nordin, A.: Development of Photo Forensics Algorithm by Detecting Photoshop Manipulation using Error Level Analysis pp. 131–137 (07 2017)
7. Kee, E., Johnson, M.K., Farid, H.: Digital image authentication from JPEG headers. IEEE transactions on information forensics and security **6**(3), 1066–1075 (2011)
8. Kee, E., O'Brien, J., Farid, H.: Exposing photo manipulation from shading and shadows. ACM Transactions on Graphics **33** (08 2014)
9. Nielsen, J.: Usability Engineering. Morgan Kaufmann Publishers Inc. (1994)
10. O'Brien, J., Farid, H.: Exposing photo manipulation with inconsistent shadows. ACM Transactions on Graphics - TOG **32**, 1–11 (05 2012)
11. Pallaris, C.: Open source intelligence tools and resources handbook 2020. https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf
12. Piva, A.: An overview on image forensics. International Scholarly Research Notices **2013** (2013)
13. Ringwood, P.: Fotoforensics. http://fotoforensics.com
14. T.J. Thomson, Daniel Angus, Paula Dootson: The Conservation's topic - 3.2 billion images and 720,000 hours of video are shared online daily. https://theconversation.com/3-2-billion-images-and-720-000-hours-of-video-are-shared-online-daily-can-you-sort-real-from-fake-148630
15. Wagner, J.: Forensically: Set of tools for digital image forensics, https://29a.ch/photo-forensics
16. WeVerify: Image verification assistant. https://mever.iti.gr/forensics/ (2020)