

THE UNIVERSITY OF DODOMA



COLLEGE OF INFORMATICS AND VIRTUAL EDUCATION

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (CSE)

FINAL YEAR PROGRESS REPORT

ACADEMIC YEAR: 2023/2024

TITLE: DIGITAL IMAGE FORENSICS TOOL

GROUP MEMBERS

STUDENT'S NAME	REGISTRATION NUMBER	PROGAMME
1. AZARIA KILASI	T/UDOM/2020/10744	BSc CSDFE
2. COSAM LUBANGO	T/UDOM/2020/09417	BSc CSDFE
3. CATHERINE JOHN	T/UDOM/2020/05907	BSc CSDFE
4. VAILET MTEI	T/UDOM/2020/05929	BSc CSDFE
5. BISEKO BAGETH	T/UDOM/2020/05923	BSc CSDFE

NAME OF SUPERVISOR

SIGNATURE

Mr Isaac Mahenge

.....

Table of Contents

Table of Contents	ii
List of Table of figures.....	iv
List of abbreviations.....	v
CHAPTER ONE	1
1.1 Project Overview	1
1.2 Problem statement.....	1
1.2 Objectives	1
1.4 Project significance	2
1.5 Project scope	2
CHAPTER TWO	3
2.1 Introduction.....	3
2.2 Definitions of Key Terms	3
2.4 Related (Similar) Work.....	5
2.5 Innovation/Research Gap.....	5
CHAPTER THREE.....	7
METHODOLOGY.....	7
3.1 Introduction	7
3.1 Research Approach	7
3.1 Research Method.....	7
3.2 Study Area / Location	7
3.3 Data Collection / Requirements Gathering	7
3.7 System Requirements.....	8
3.7.1 Hardware Requirements.....	8
3.7.2 Software Tools Requirements	9
CHAPTER FOUR.....	10

PROJECT ACTIVITIES AND MILESTONES	10
(WORK DONE).....	10
4.1 Objective One: Requirement gathering.....	10
4.1.1 System requirements	13
4.2 Objective Two: To design DIFT	14
References	20

List of Table of figures

Figure 1: Image editing	11
Figure 2: Challenges of existing tools.....	11
Figure 3: Suggestions.....	12
Figure 4: Expected Features.....	12
Figure 5: Common image attacks	13
Figure 6: Context diagram	14
Figure 7: DFD Level 1	15
Figure 8: DIFT Architecture	16
Figure 9: Use case	17
Figure 10: Activity diagram.....	18
Figure 11: Sequence diagram.....	19

List of abbreviations

UDOM

University of Dodoma

CIVE

College of informatics and Virtual Education

FYP

Final Year Project

DIFT

Digital Image Forensic Tool

CHAPTER ONE

INTRODUCTION

1.1 Project Overview

Digital image forensic tool (DIFT) is windows desktop application that is used to perform carving, verifying the authenticity and integrity of digital images, especially in the context of detecting and localizing forgery. This tool will be designed with a friendly user-interface to examine images for signs of copy-move and splicing forgeries, as well as providing a comprehensive report of the forensic analysis.

1.2 Problem statement

In the digital age, the widespread use of digital images has led to an increase in the manipulation and tampering of visual content for deceptive or to make a false propaganda. Also intentional or unintentional deletion of images leads to loss of important evidence. As a result, there is a growing need for advanced digital image forensic tools that can perform image carving, analyze and authenticate digital images. Despite of having several tools that perform image carving and image forgery detection, most of the existing tools have limitations such as lack of friendly user interface, inadequate of single tool that performing both image carving and forgery detection, weak or no reporting capabilities, requires skilled expertise for studying and navigating through the results to identify the forgery. These limitations poses challenges for digital forensic experts and non-expert users in ensuring the integrity of visual information.

1.2 Objectives

1.3.1 Main objective.

To develop a Graphical User Interface (GUI) digital image forensic tool capable perform image carving and verify the authenticity of image.

1.3.2 Specific objective.

- i. To gather requirements.
- ii. To design DIFT
- iii. To develop a DIFT
- iv. Testing a tool

1.4 Project significance

The development of DIFT holds significant implications for various sectors. It contributes to maintaining the credibility of visual information in journalism, safeguarding the integrity of digital forensics investigations, and combating the spread of misinformation on social media platforms. Additionally, the tool can be instrumental in protecting individuals from the harmful consequences of image manipulation, ensuring the trustworthiness of visual content in the digital age.

1.5 Project scope

The scope of this project encompasses the development of DIFT with a focus on addressing common forgery techniques which are copy move and splicing forgery. The tool will be designed to recover deleted images in jpg formats, as well as analyzing digital images and provide assessments of their authenticity.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

Digital image forensics has gained significant attention due to the widespread use of digital images in various domains such as social media, journalism, and law enforcement. . Owing to their widespread use, digital images are the most commonly tampered digital media, misrepresenting their meaning with malevolent purpose (Sivita Walia, 2018). The detection and authentication of digital images have become crucial to ensure the reliability and trustworthiness of visual information.

This literature review aims to provide an overview of the state-of-the-art digital image forensics tools, focusing on their methodologies, strengths, limitations, and potential future directions.

2.2 Definitions of Key Terms

File carving is a technique used to recover or re-construct files (or file fragments) based on their structure and/or contents. File carving does not depend on any information provided by the operating system or its file system (Ziad A.Al-Sharif, 2015).

Digital or computer forensics is defined as the practice of identifying, preserving, extracting, analyzing and presenting legally sound evidence from digital media such as computer hard drives (Nadeem Alherbawi, 2013)

Image splicing is the process of modifying an image by pasting a cropped part of another image and pasting it into the first image. This is a very common form of forgery and is often followed by some form of image augmentation such as blurring or smoothing to hide the manipulation (Aditya Pandey, 2022).

Copy move forgery on the other hand is when an image is tempered by copying and pasting a small region from an image into the same image (Aditya Pandey, 2022).

2.3 Theoretical Literature/Framework (of the problem that system or artefact is trying to solve) Digital Image Forensics Tool (DIFT) is designed to address the existing challenges of user interface limitations in current tools. This tool specifically focuses on data carving and image detection functionalities, aiming to be a multitasking solution.

This theoretical literature introduces an innovative Digital Image Forensics Tool that tackles the prevailing challenges associated with user interface limitations found in current tools. The tool's primary focus lies in enhancing data carving and image detection functionalities. By combining these two critical processes seamlessly, the proposed tool aims to provide a multitasking solution that offers an intuitive and user-friendly interface.

One of the key features of this tool is its ability to streamline both data carving and image detection, eliminating the need for users to switch between different software or tools. This integration significantly simplifies the forensic analysis process, saving time and effort for investigators.

Moreover, the tool goes beyond mere functionality by generating comprehensive and well-explained reports. These reports provide detailed insights and analysis, augmenting the forensic analysis process. Investigators can rely on the tool's clear and concise documentation to present their findings effectively and support their conclusions.

By addressing the limitations of existing tools, this Digital Image Forensics Tool represents a substantial advancement in the field. Its multitasking capabilities, user-friendly interface, and comprehensive reporting system make it a valuable asset for forensic investigators, enabling them to conduct thorough and efficient analyses of digital images.

2.4 Related (Similar) Work

Image Carving.

1. From the literature, "**Seam Carving for Content-Aware Image Resizing**" (Shamir, 2007): This work introduced seam carving, a technique for content-aware image resizing. Understanding this foundational concept is crucial for developing image carving tools, as it forms the basis for preserving important content during manipulation.
2. From the literature, "**A Comparative Study of Image Retargeting Algorithms**" (Gutierrez): The paper provides a comparative analysis of various image retargeting algorithms, including seam carving. Insights from this work are valuable for making informed decisions in the development of image carving tools.

Image Forgery Detection.

3. From the literature, "**Digital Image Forensics: A booklet for Beginners**" (Memon, 2006): This foundational resource covers various aspects of digital image forensics, offering insights into forgery detection techniques. It serves as a starting point for understanding the principles of detecting image manipulations.
4. From the literature, "**A Survey of Copy-Move Forgery Detection Techniques**" (Bianchi, 2013): The survey provides an overview of copy-move forgery detection techniques, a common form of image tampering. This work is essential for gaining insights into traditional forgery detection methods.
5. From the literature, "**Image Forgery Detection: A Survey**" (Singh, 2016): This comprehensive survey explores various image forgery detection methods, including those based on image processing, machine learning, and deep learning. It offers a broader perspective on the state of the art in forgery detection.

2.5 Innovation/Research Gap

- **Develop a tool with user friendly graphical user interface.**
Graphical user interface will simplify the usability of the tool and make it usable even to non-expert users.
- **Develop a multitask tool which involves both image forgery detection and image carving in a single tool.**

This will simplify the forensic investigation through eliminating the need of using multiple tools to perform image carving and image forgery detection in the same instance of forensic investigation

- **Introduce semantic forgery localization to provide a high-level understanding of manipulated regions.**

Instead of just highlighting manipulated pixels, incorporate a semantic segmentation model that can identify and label objects or regions within the image. This provides a more intuitive visualization for non-experts, allowing them to grasp the impact of the forgery on the content.

- **Implement real-time analysis capabilities and immediate report generation.**

Enable users to receive instant feedback on forgery detection and image carving. The tool can provide a preliminary report during the analysis process, allowing investigators to make informed decisions promptly. This feature enhances the efficiency of the forensic workflow.

CHAPTER THREE

METHODOLOGY

3.1 Introduction

In creating a digital image forensic tool, we need a clear plan, or methodology. This section introduces the steps we'll follow to ensure the tool works well in detecting fake images and extracting information from them. The plan takes into account the ever-changing nature of digital forensics, and we aim to follow a step-by-step process, from generating ideas to designing, building, and testing the tool. This part is crucial to establish the guidelines for developing an effective digital image forensic tool that meets the high standards of the field.

3.1 Research Approach

The research will adopt mixed research approach because it allows for a comprehensive understanding of the carving module's overall performance and user satisfaction.

3.1 Research Method

The research is going to use V-Model (Verification and Validation Model) because it Ensures that testing activities are integrated into the development process from the beginning, this is beneficial for ensuring the accuracy and reliability of forgery detection and carving algorithms.

3.2 Study Area / Location

This project will be conducted at University of Dodoma, College of Informatics because it have large community of ICT Users like ICT students, faculty, and ICT experts which enables easy access to potential users and stakeholders, facilitating engagement and feedback collection. Also the area serves as an ideal environment for understanding diverse user needs, technological challenges, and real-world scenarios relevant to digital image forensics.

3.3 Data Collection / Requirements Gathering

3.3.1 Data Collection Techniques/Methods

Data will be collected using Questionnaires, and exploring documentations of already existing tools and resources for identifying their strength and weaknesses.

3.3.2 Data Collection Tools

Data will be collected Requirements will be gathered using Google Forms note taking tools (notebook and google Docs) and search engines.

3.4 System/Requirements/Data Analysis

The application will be analyzed using Activity Diagram and Sequence diagram

3.5 System/Model Design/Architecture

3.5.1 Logical Design/Architecture

- i. Pre-processing: The input image is pre-processed to enhance its quality and remove any noise or artifacts that may interfere with the detection process.
- ii. Feature extraction: The pre-processed image is then analyzed to extract relevant features that can be used to identify the presence of forgery. This step may involve using techniques such as Z-score feature, error level analysis, or saliency algorithm.
- iii. Classification: The extracted features are then used to classify the image as either authentic or forged. This step may involve using machine learning algorithms such as VGG-16 convolutional neural network or end-to-end attention network.
- iv. Localization: If the image is classified as forged, the application should be able to localize the area of forgery. This step may involve using techniques such as Z-score feature or forgery trace generation network.
- v. Output: The application should provide a clear output that indicates whether the image is authentic or forged and the location of the forged area if applicable.

3.5.2 Physical Design/Architecture

This will involve the use of a stand-alone approach. An application will be installed in designated computer for its use case.

3.6 System Implementation

3.6.1 Coding

The proposed project will be implemented using Python for simplicity, scalability, performance, extensive libraries, and it has great community support.

3.6.2 Testing/Evaluation

The proposed project will be tested using a benchmarks of datasets

3.7 System Requirements

The project will employ hardware components and software resources to meet application requirements. The following will be the system requirements for the successful deployment of the project.

3.7.1 Hardware Requirements

- Intel Processor - 2.7GHz
- Memory - 8 GB
- Disk Space - 500 GB.
- Monitor

3.7.2 Software Tools Requirements

- Integrated Development Environment (IDE) - Visual studio code
- Python 3.11

CHAPTER FOUR

PROJECT ACTIVITIES AND MILESTONES

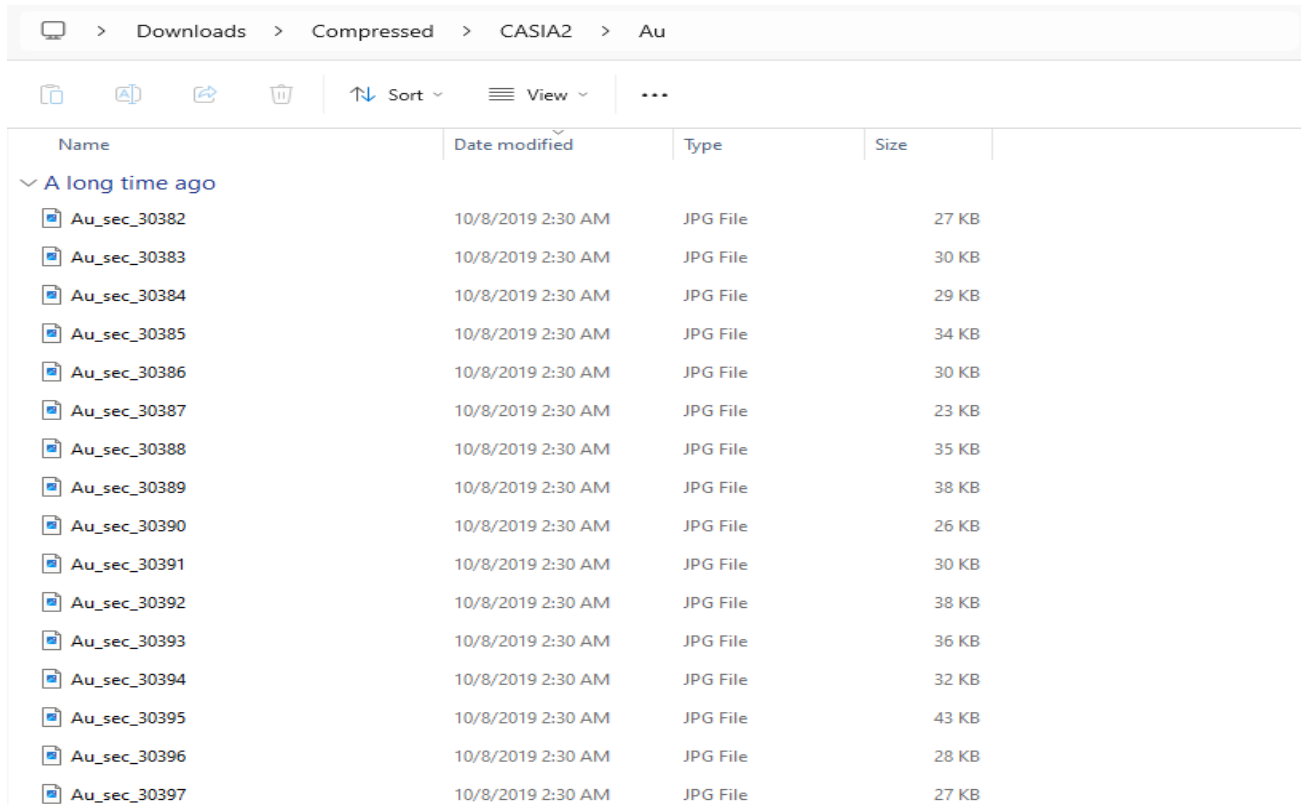
(WORK DONE)

4.1 Objective One: Requirement gathering.

S/N	Activities	Output	Progress Status
1	Review relevant literature on image manipulation detection	Identification of Research Gap	100%
2	To prepare data collection tools	Questionnaire	100%
3	Collecting datasets of digital image forgeries from kaggle	Datasets acquisition	80%
4	To identify functional and non-functional requirements	System Requirements Specifications and User requirements	100%

Descriptions (Illustrations) of the Outputs achieved in Objective One

Dataset was collected from Kaggle CASIA1 and CASIA2 which included the following features: copy move forgery images and splicing forgery images. The total number of images are 17,000.



Name	Date modified	Type	Size
▼ A long time ago			
Au_sec_30382	10/8/2019 2:30 AM	JPG File	27 KB
Au_sec_30383	10/8/2019 2:30 AM	JPG File	30 KB
Au_sec_30384	10/8/2019 2:30 AM	JPG File	29 KB
Au_sec_30385	10/8/2019 2:30 AM	JPG File	34 KB
Au_sec_30386	10/8/2019 2:30 AM	JPG File	30 KB
Au_sec_30387	10/8/2019 2:30 AM	JPG File	23 KB
Au_sec_30388	10/8/2019 2:30 AM	JPG File	35 KB
Au_sec_30389	10/8/2019 2:30 AM	JPG File	38 KB
Au_sec_30390	10/8/2019 2:30 AM	JPG File	26 KB
Au_sec_30391	10/8/2019 2:30 AM	JPG File	30 KB
Au_sec_30392	10/8/2019 2:30 AM	JPG File	38 KB
Au_sec_30393	10/8/2019 2:30 AM	JPG File	36 KB
Au_sec_30394	10/8/2019 2:30 AM	JPG File	32 KB
Au_sec_30395	10/8/2019 2:30 AM	JPG File	43 KB
Au_sec_30396	10/8/2019 2:30 AM	JPG File	28 KB
Au_sec_30397	10/8/2019 2:30 AM	JPG File	27 KB

Figure 1: Datasets Casia2

Data collection methods

Data Collection Tool used: Questionnaire

Ways of Collection: Google Forms (<https://forms.gle/cTTvpSFR9WYRcY979>)

Total Response: 43 Respondents

Responses

About 97.7% of respondent out of 43 who participated in our research argued that, in one way or another have used image editing software.

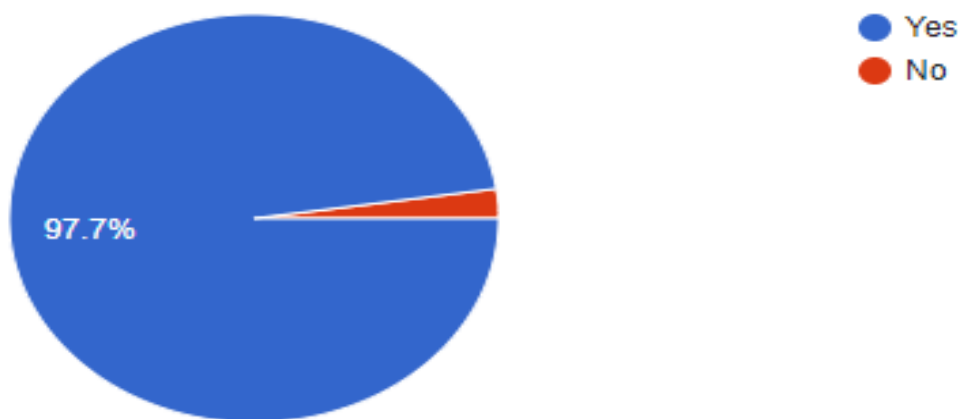


Figure 2: Image editing

Most users find it hard to use CLI tools (72%), furthermore, 65% says most of tools requires expertise to identify area of forgery.

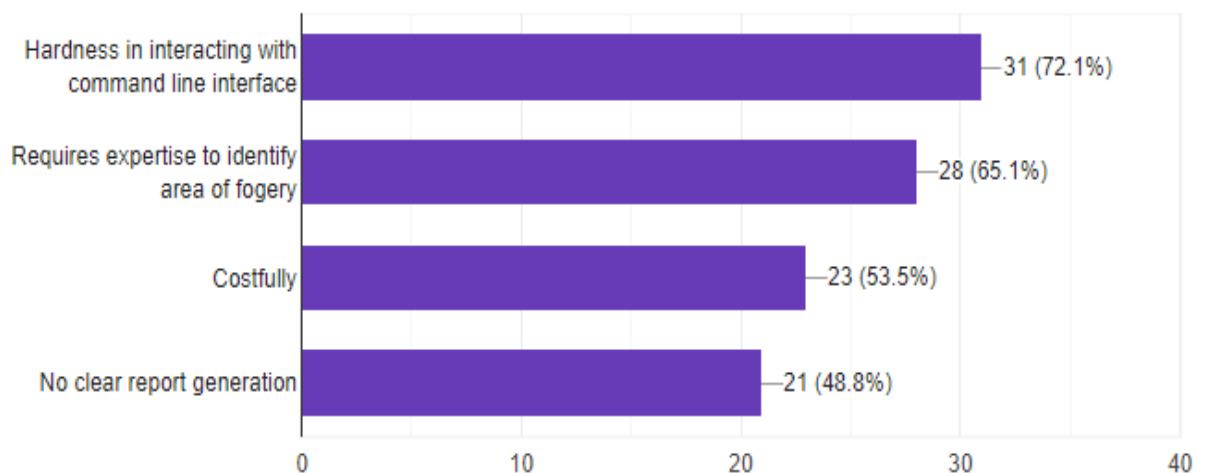


Figure 3: Challenges of existing tools

Most of users provides suggestions on functionality that can be included in the tool based on the challenges that exists in other tools such as report generation (79%).

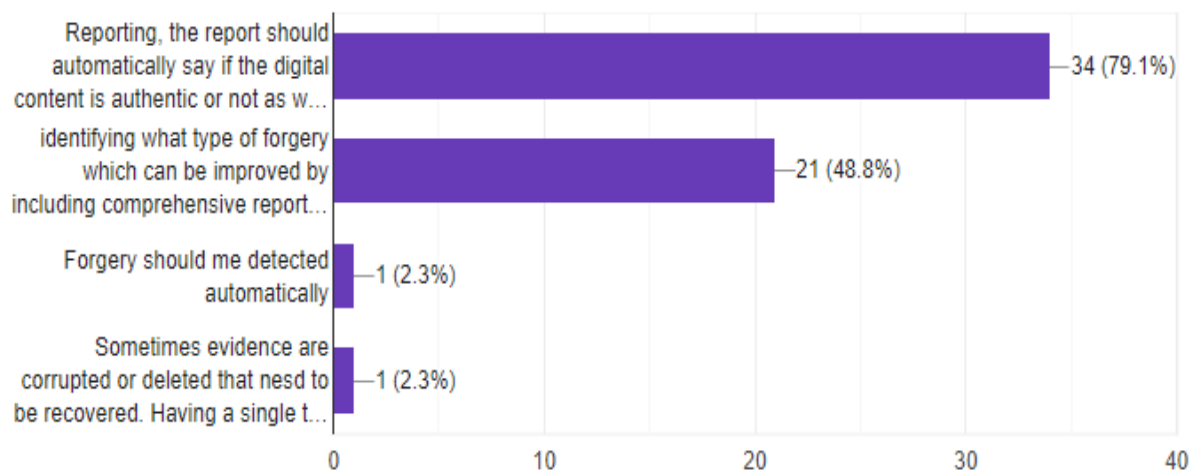


Figure 4: Suggestions

Most users expects the following functionalities in a tool, Graphical user interface (81%).

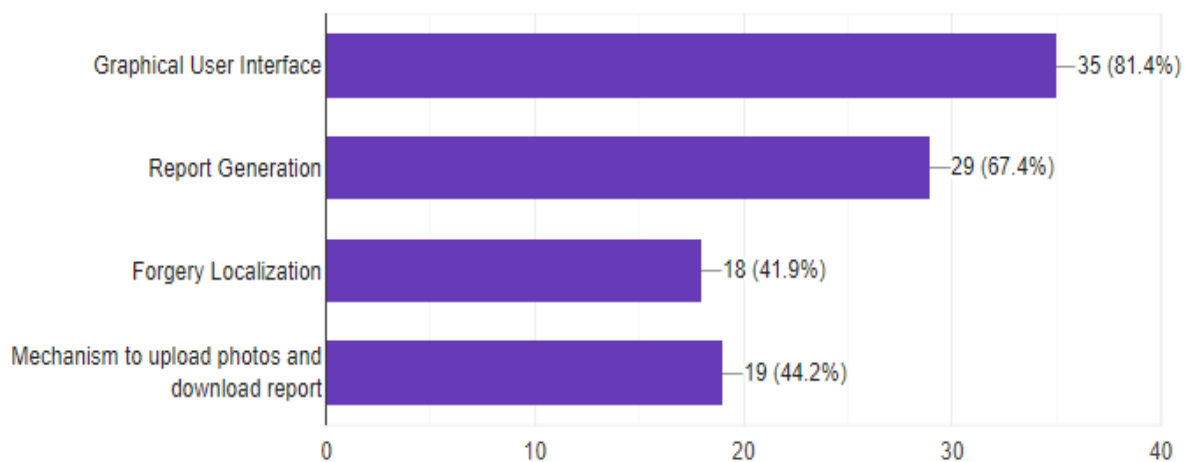


Figure 5: Expected Features

Most types of attacks on digital image

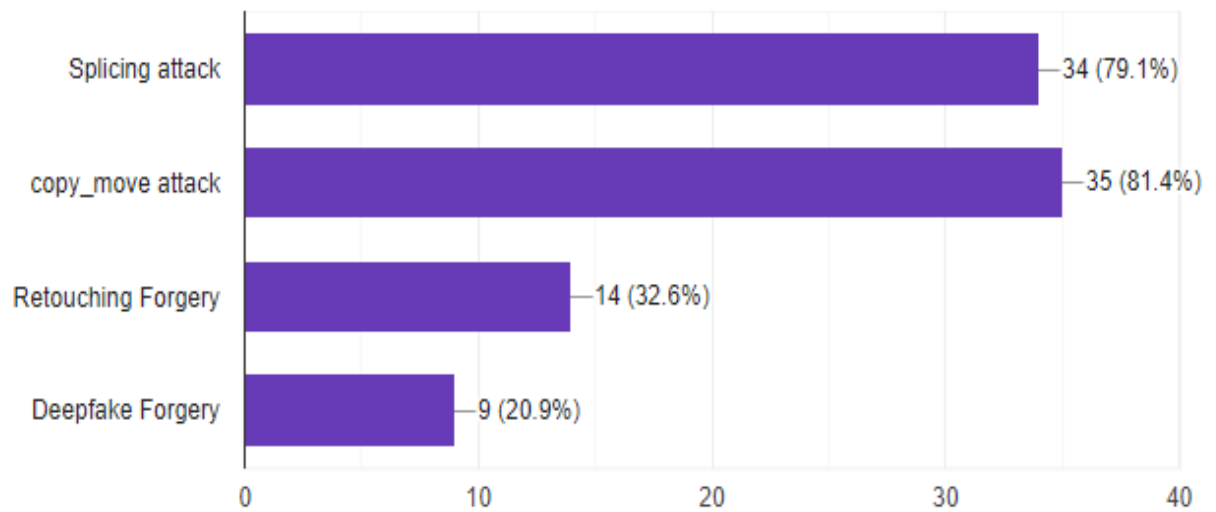


Figure 6: Common image attacks

4.1.1 System requirements

Functional requirements

- i. The tool should allow users to import digital images from local storage and external devices (USB).
- ii. The tool should validate the authenticity of digital image.
- iii. The tool should perform image carving, which involves extracting data from images to recover deleted images.
- iv. The tool should be able to generate report that summarizing the results of image analysis and authenticity of image.

Non-functional requirements

- i. The tool should have a user friendly interface (GUI).
- ii. The tool should be reliable and minimizing the risk of crashes
- iii. Usability: The GUI should be simple and user-friendly, with clear navigation and well-designed interfaces to accommodate users of varying technical experience.

4.2 Objective Two: To design DIFT

During design we have used Architecture diagram, Data flow diagram, use-case diagram, Activity diagram and Sequence diagram.

Context diagram

This provides an overall picture of the tool, it also gives the insight into the inputs and outputs of each entity and the process itself.

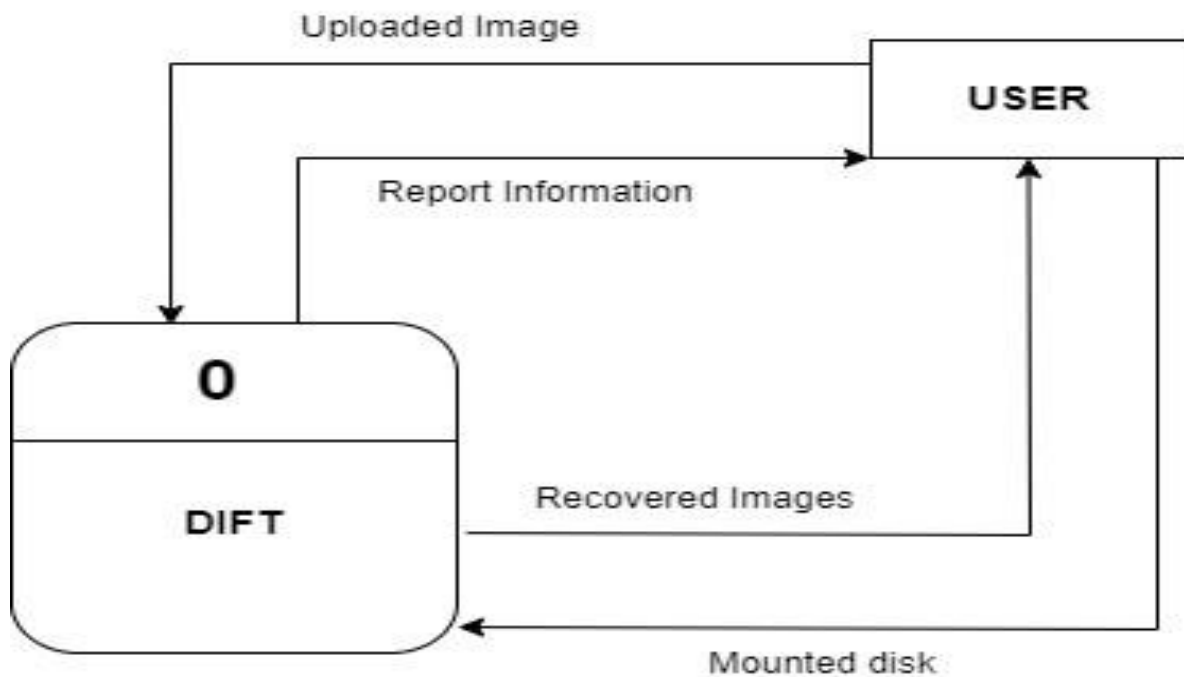


Figure 7: Context diagram

DFD Level 1

This represents the main functions of the system and how they interact with each other.

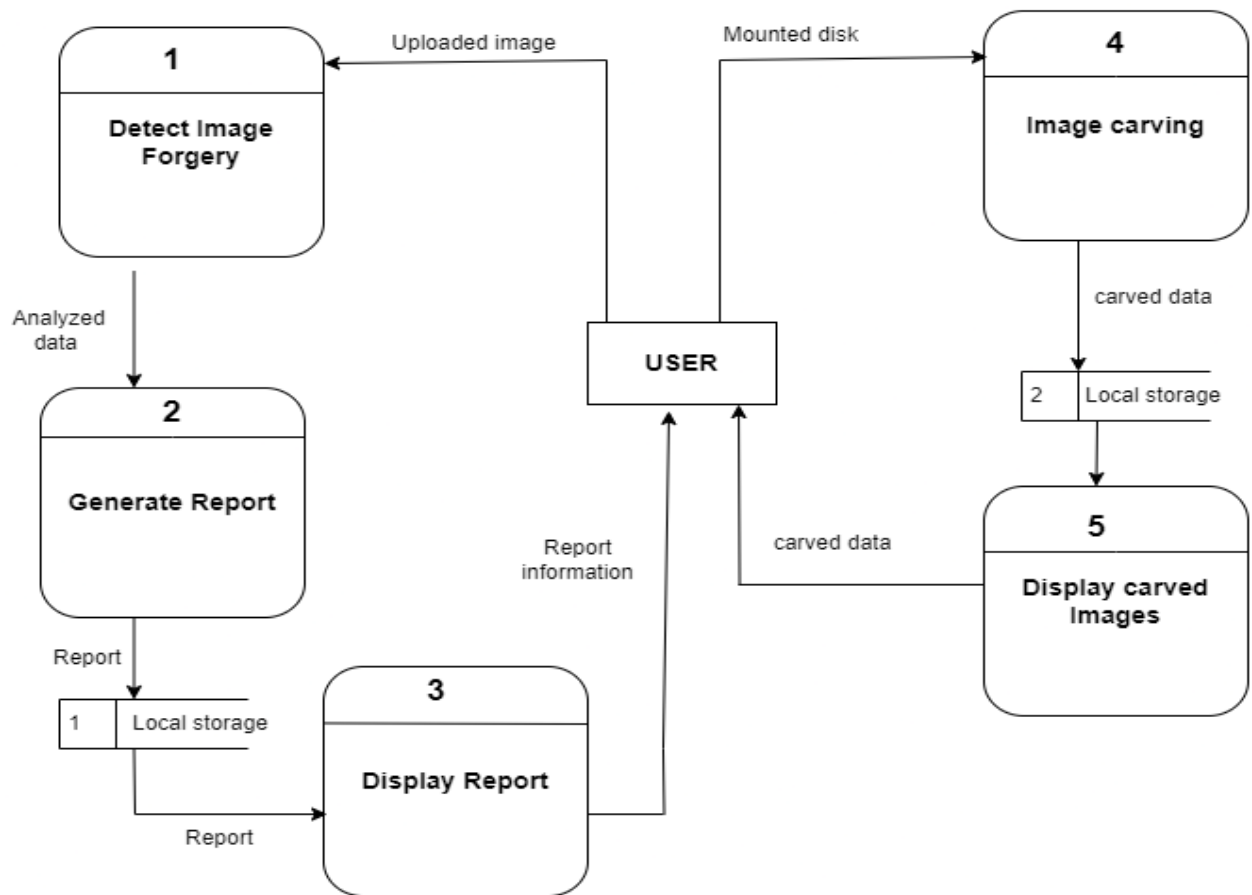


Figure 8: DFD Level 1

Architecture diagram

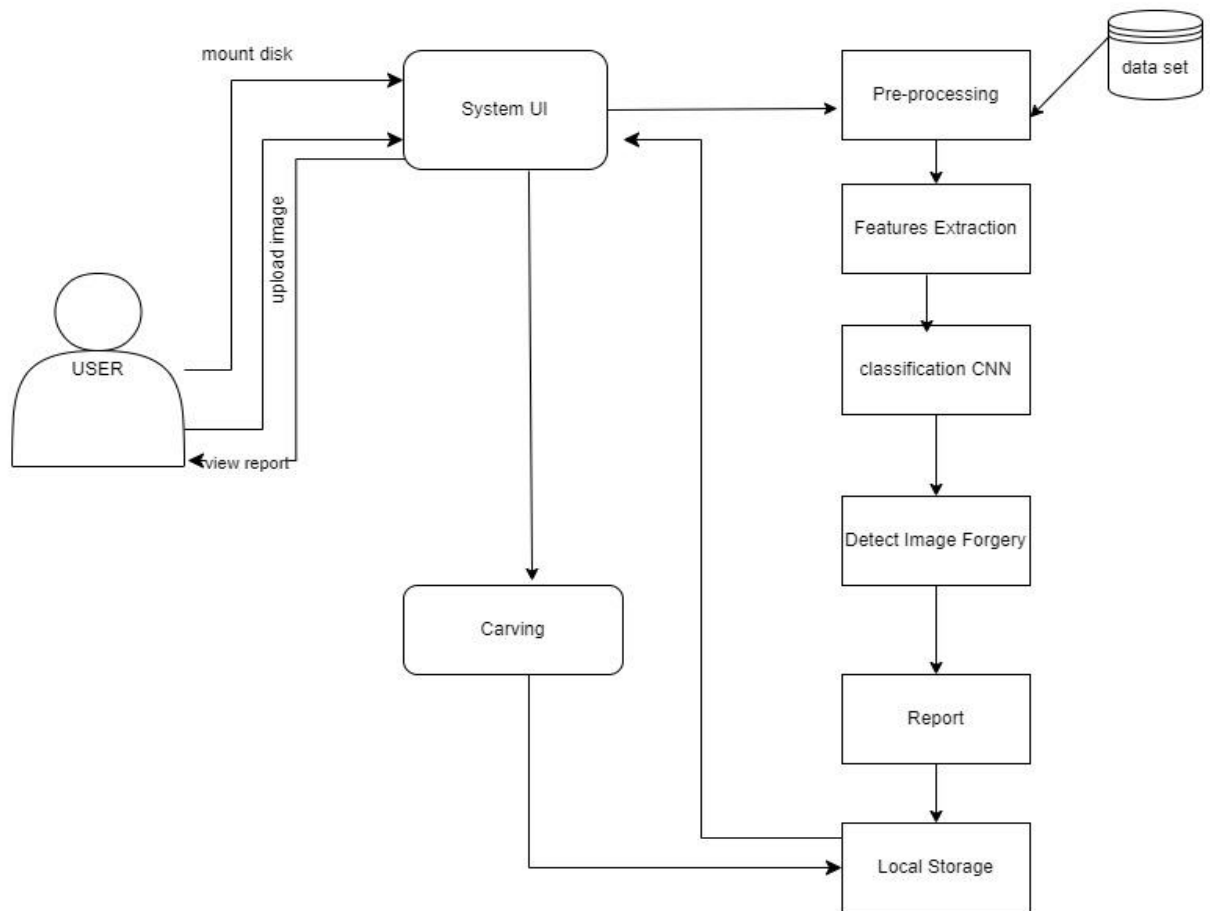


Figure 9: DIFT Architecture

Use case diagram

This represents the interactions between actor and the tool, where it describe functionality and scope the tool.

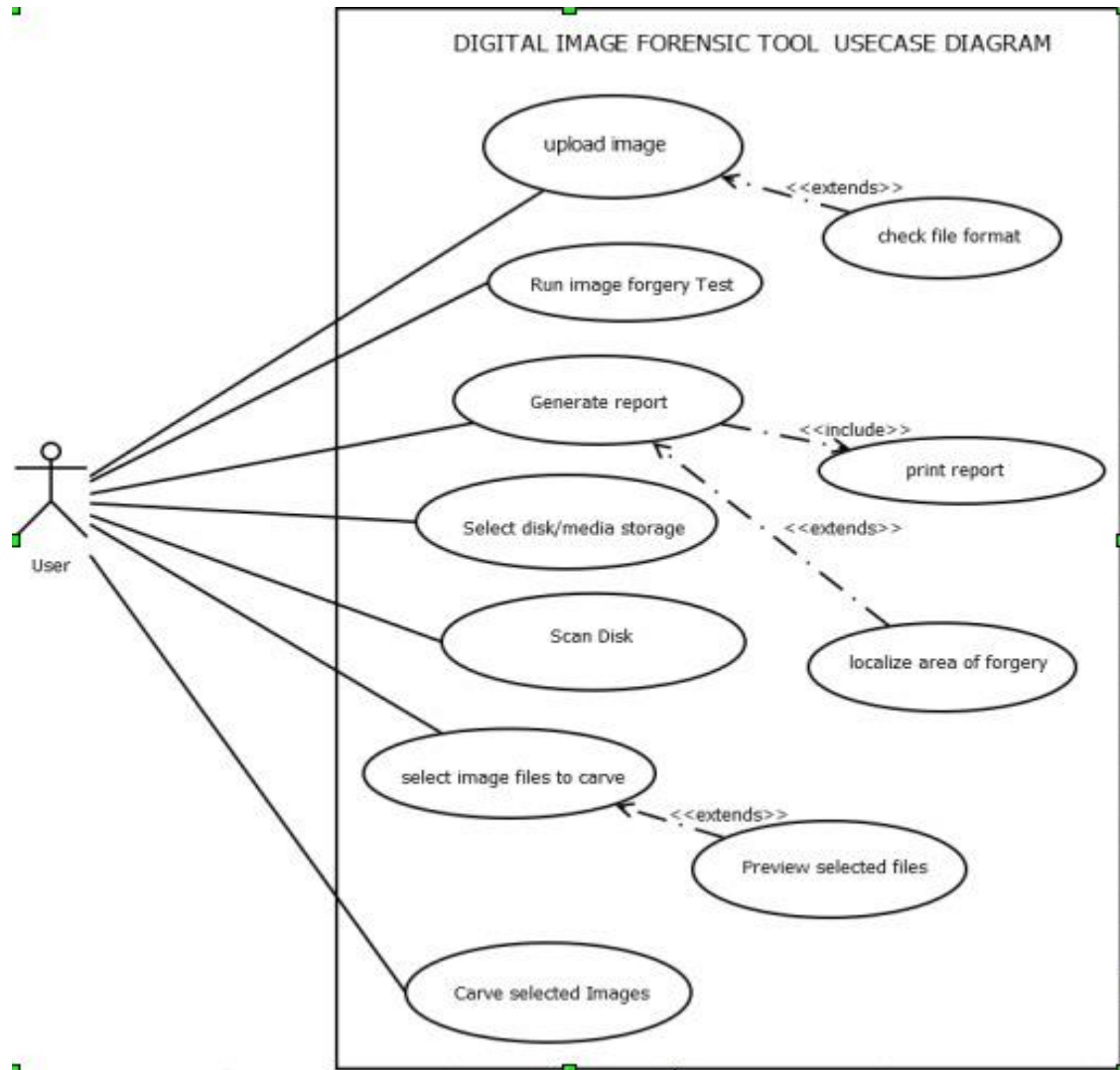


Figure 10: Use case

Activity Diagram

Activity diagram is used to illustrate the flow of control in the system

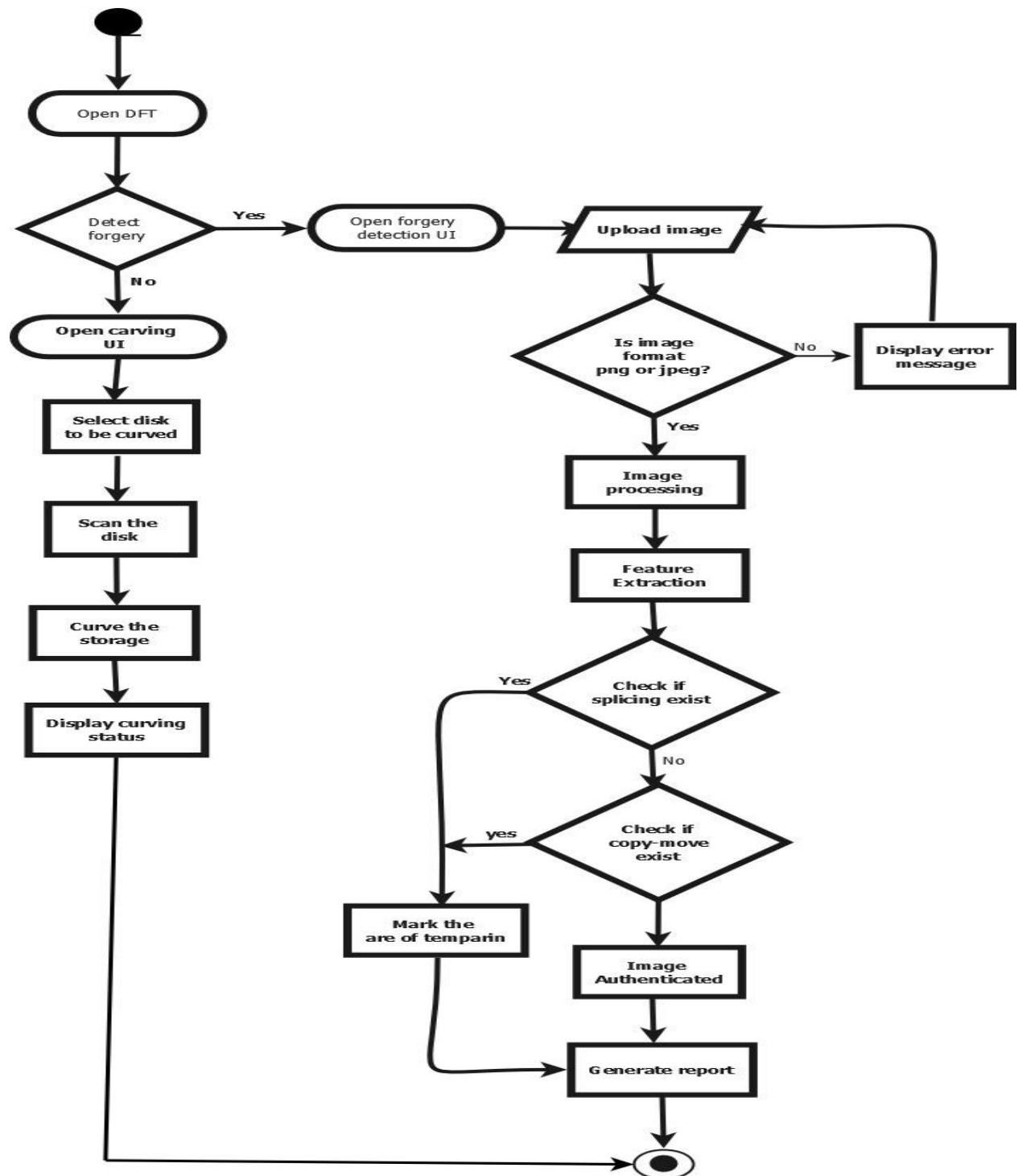


Figure 11: Activity diagram

A SEQUENCE DIAGRAM FOR DIFT.

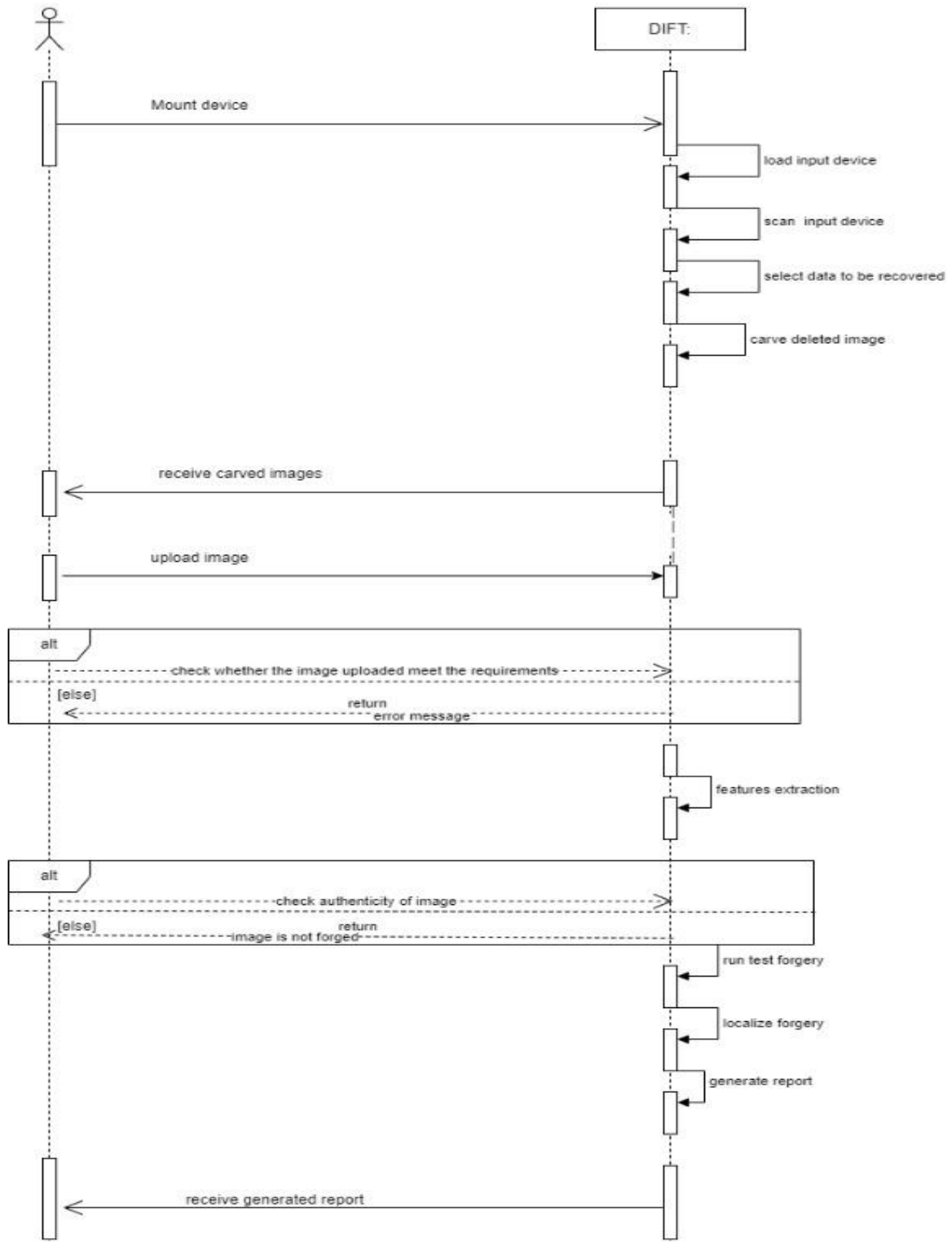


Figure 12: Sequence diagram

References

- Aditya Pandey, A. M. (2022). *Detecting and Localizing Copy-Move and Image-Splicing Forgery*. New York: New York University.
- Bianchi, T. P. (2013). A survey of copy-move forgery detection techniques. *A survey of copy-move forgery detection techniques*.
- Gutierrez, D. (n.d.). A Comparative Study of Image Retargeting. *A Comparative Study of Image Retargeting*, 1-8.
- Memon, N. &. (2006). *Digital image forensics*.
- Ministry of Communication and Information Technology. (2013). *Forensic Data Carving*. New Dehli: Government of India.
- Nadeem Alherbawi *, Z. S. (2013). Systematic Literature Review on Data Carving in Digital Forensic. *The 4th International Conference on Electrical Engineering and Informatics (ICEEI 2013)* (pp. 86-92). Selangor: Elsevier Ltd.
- Shamir, S. A. (2007). Seam Carving for Content-Aware Image Resizing. *Seam Carving for Content-Aware Image Resizing*, 1-10.
- Singh, S. &. (2016). Image forgery detection. *Image forgery detection*, 1-8.
- Sivita Walia, K. K. (2018). Digital Image Forgery Detection: a systematic scrutiny. *Australian Journal of Forensic Sciences*, 1-3.
- Ziad A.Al-Sharif, D. N.-S. (2015). *Towards Carving PDF Files in the Main Memory*. Antalya: SDIWC.