Software Requirement Specification Document for steganalysis application

Ayatullah Hesham , Monad Khaled , Sara Khaled , Mahmoud Kashef
Supervised by : Prof. Rashed Refaat , Eng. Saja Tareq Saadoun

April 9, 2024

Table 1: Version history

Version	**Date**	**Reason for Change**
1.0	14-JAN-2024	SRS First version's specifications are defined.

GitHub: https://github.com/AyaHeshaam/SteganalysisTool

Contents

Abstract

Steganography is the art of hiding the very presence of communication by embedding secret messages into innocuous looking-over documents, such as images, videos, and audio [7] [6] .Furthermore, the detection of steganography ,and its extraction belong to the field of steganalysis. Therefore, steganography and steganalysis are two different sides of the same coin, as well they both have received a lot of attention from law enforcement and other media. steganography VS steganalysis is a never-ending fight . In this paper, a detailed review of steganalysis uses and techniques is offered. So our major goal is to construct a steganalysis application that accepts an uploaded image via an website application and by using CNN technique (convolutional neural network) it can be used to analyze images and detect patterns or unusualities that can point to the existence of hidden data. CNNs can be used by researchers and practitioners to train models that can discriminate between normal, unaltered images and those that have been altered using steganographic techniques to conceal information [4].

1 Introduction

1.1 Purpose of this document

This paper will outline the methods and techniques employed to detect and analyze hidden information within digital images . In addition , the document will have diagrams to discuss the process of detection in details .

1.2 Scope of this document

In this document, the system's purpose and functions will be emphasized. Moreover, the system's functional, non-functional requirements, design constraints and data design will be explained. Lastly, the operational scenarios of the project and the project plan will be mentioned.

1.3 Business Context

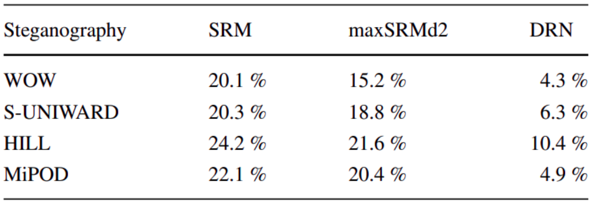
As safeguarding sensitive information is important nowadays and hidden data concealment strategies became more common , steganalysis becomes an essential tool for strengthening corporate data security . Scientists focused on developing techniques for extracting hidden information from digital images in the 1990s and early 2000s [1]. Thus, this discipline provides an efficient defence against covert data breaches and increases the protection of proprietary assets in a changing business environment by helping companies detect hidden information. In addition, the proposed system may review images for potential vulnerabilities and ensure that concealed data is restored from backups in the original format to prevent corruption or unauthorised modifications.

2 Similar Systems

2.1 Academic

Deep residual learning for image Steganalysis, 2018[2]: The authors proposed a CNN model which is based on residual learning. The proposed model have 2 main advantages than existing

CNNs model, the first one being the many network layers contained and the second one being the perservation of the stego signal coming from secret messages due the residual learning.They tested the proposed model againts Spatial Rich model and maxSRMd2(which is an improved SRM) and were met with the results in the table below. The proposed system showed the least error rates against 4 different steganographic techniques.



Steganography	SRM	maxSRMd2	DRN
WOW	20.1 %	15.2 %	4.3 %
S-UNIWARD	20.3 %	18.8 %	6.3 %
HILL	24.2 %	21.6 %	10.4 %
MiPOD	22.1 %	20.4 %	4.9 %

Figure 1: Table 1 Detection error rates for four states of the art steganographic algorithms at payload 0.4 bpp [2]

GBRAS-Net: A Convolutional Neural Network Architecture for Spatial Image Steganalysis,2021[5]: The authors proposed a CNN based architecture named GRABS which is an enhancement for previous spatial image steganalysis networks. The system proposed uses 30 SRM filters and also unlike usual CNN, it evades using fully connected network by the direct use of a global average pooling followed by a softmax activation function that shows the probabilities for classification. The system showed exceptional accuracy in detecting stego images. The below figure shows a comparison between the proposed system and different steganalytic methods.

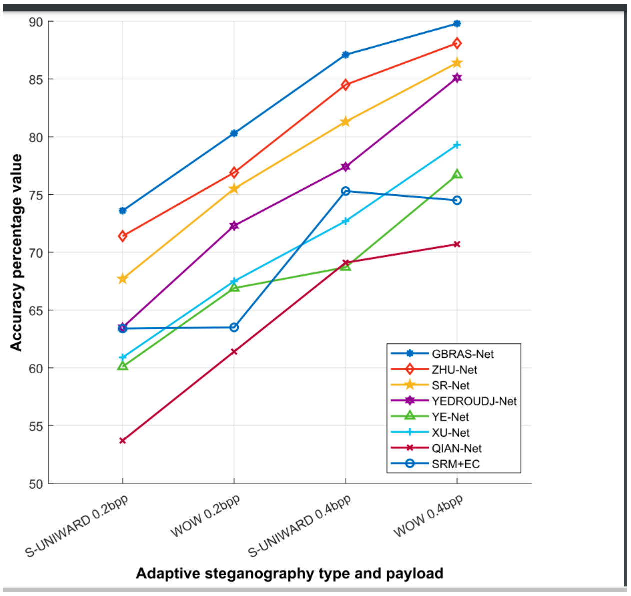
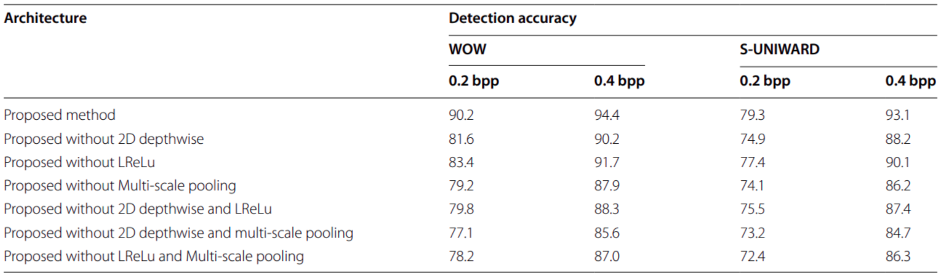


Figure 2: Comparison between GRABS and other steganalytic techniques.[5]

A convolutional neural network to detect possible hidden data in spatial domain images,2023[9]:The authors proposed an architecture that is composed of 3 stages (pre processing,feature extraction and classification). Their main aim was to tackle the training phase stability in spatial domain images and the stego detection accuracy.The proposed system uses 2D



Architecture	Detection accuracy			
	WOW		S-UNIWARD	
	0.2 bpp	0.4 bpp	0.2 bpp	0.4 bpp
Proposed method	90.2	94.4	79.3	93.1
Proposed without 2D depthwise	81.6	90.2	74.9	88.2
Proposed without LReLu	83.4	91.7	77.4	90.1
Proposed without Multi-scale pooling	79.2	87.9	74.1	86.2
Proposed without 2D depthwise and LReLu	79.8	88.3	75.5	87.4
Proposed without 2D depthwise and multi-scale pooling	77.1	85.6	73.2	84.7
Proposed without LReLu and Multi-scale pooling	78.2	87.0	72.4	86.3

Figure 3: Accuracy comparison between the system with and without some functions[9]

depth-wise separable convolutions,LReLu and using multi-scale pooling. They experimented on a combination BOSSBase 1.01 with BOWS 2 and also ALASKA2 to veirfy training phase stability.

3 System Description

3.1 Problem Statement

The problem addressed by our project is that steganographers are actively aiming to create ways and methods that are difficult to detect to hide information. Steganographic techniques pose a significant challenge to conventional approaches for detecting hidden information in digital images. Therefore, conventional steganalysis methods struggle to capture the subtle changes introduced by steganographic techniques. So, in order to protect digital security and privacy and prevent illegal activity, reliable and precise steganalysis solutions are essential. So our purpose is to design and implement a steganalysis system based on CNN techniques. The primary goal is to enhance the steganalysis models' overall performance with respect to detection accuracy, resistance to different steganographic techniques, and deep network handling capabilities.

3.2 System Overview

The development of the system is split into mainly five stages, as shown in Figure(4):

- In the first stage, known as the input stage, User authentication/login: Users must log in to the system to access the steganalysis functionality. Authentication guarantees that only authorized users can upload images to the system.

  User upload: Once logged in, users can upload images to the stegasus mobile app.

- In the second phase, which is the image preprocessing phase, it is about preprocessing the image itself by applying some methods such as image loading, image resizing, and normalization.

  Feature extraction is the process of detecting and measuring relevant patterns or properties in preprocessed images. These retrieved attributes are used as input for machine learning models that detect steganographic content.

- In the third stage, the trained model phase, this phase contains five steps, which are

  1. Data collection: gather a dataset of images containing both original and steganographic images; this dataset serves as the foundation for training the stegananalysis model.

  2. Data preprocessing: Prepare the dataset by performing preprocessing tasks such as image loading, resizing, normalization, and noise reduction.

  3. Feature extraction: extract relevant features from the preprocessed images; these features will serve as input to the machine learning model.

  4. Model training: train a machine learning model using the extracted features and corresponding labels (original or steganographic) from the dataset. experiment with various ML algorithms and CNN techniques to find the best-performing model.

  5. Model evaluation: Evaluate the trained model's performance to assess its effectiveness in detecting steganographic content accurately.

- In the fourth stage , it's about the detection phase. The detection phase is a crucial step in the steganalysis system since it examines uploaded images to determine whether they contain hidden content/steganographic data or not.

- In the fifth stage, it's about the extraction phase.

  Upon detecting hidden content within the uploaded image, the system initiates the extraction phase to retrieve and present this hidden information to the user.

- In the final stage , is the output and results stage. Present the steganalysis results to the user, indicating whether hidden content was detected in the uploaded image and offering extra information as needed.

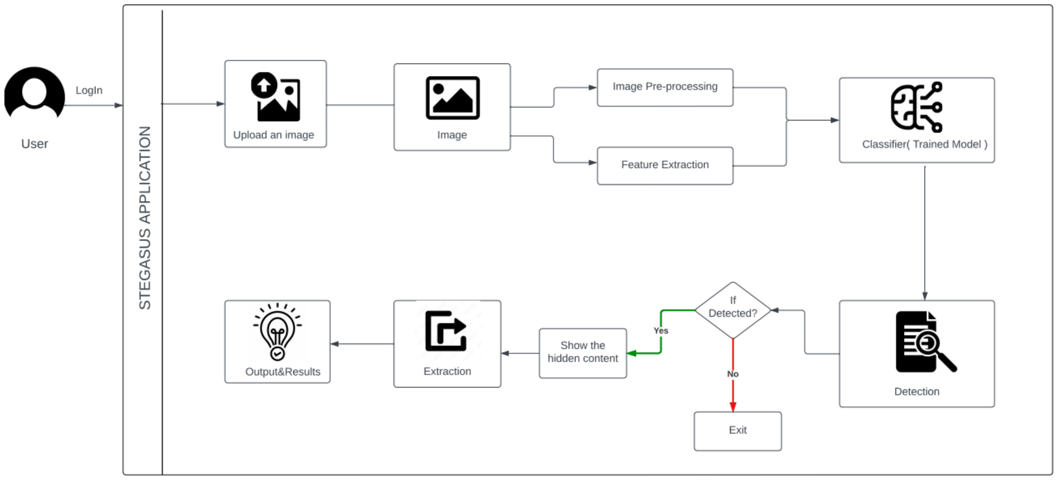


Figure 4: System's overview

3.3 System Scope

The system aims to:

- Create a user-friendly steganalysis web/mobile application that enable cybersecurity professionals, forensic analysts, educational organizations and researchers to apply steganalysis techniques effectively. Steganalysis may also attempt to recover the hidden information. This entails retrieving the concealed content and making it available for further investigation.

- Provide a steganalysis system that can bolster an organization's security framework and guarantee the identification of secret communication channels.

- Develop a steganalysis system that leverages the capabilities of the technique to achieve high detection accuracy.

- Enable To help researchers and analysts to determine which features are involved in the identification of steganographic content , enhancing transparency and trust in the system.

- By using the CNN technique in the system, it handles images with varying properties , which makes the system reliable and useful in the real-world scenarios where images may possess disparate characteristics.

- By using the CNN technique in the system , It gives the system the ability to detect hidden content regardless of the specific embedding technique used.

3.4 System Context

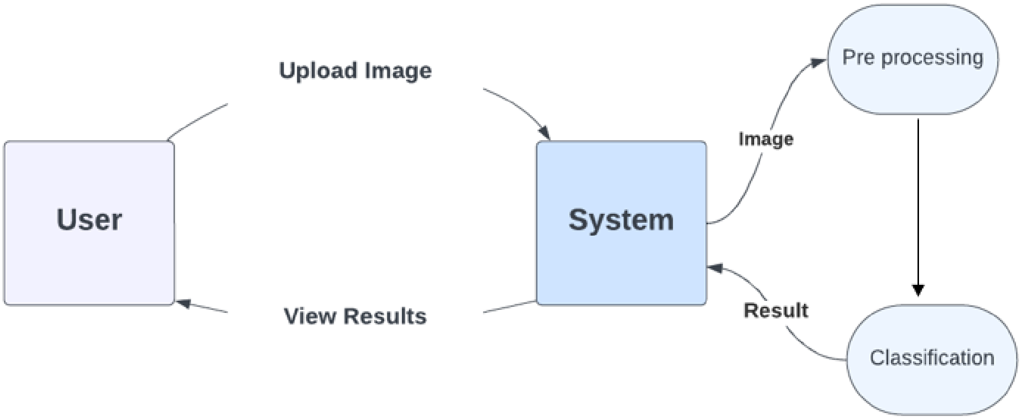


Figure 5: Context diagram.

3.5 Objectives

The main purpose of our system, which uses CNN algorithms for image steganalysis, is to address specific issues related to identifying the hidden information or steganographic content within digital images. These objectives include:

- Enhanced feature learning: it enable the network to discover more discriminative features associated with steganographic content as Traditional steganalysis methods may struggle to capture subtle features introduced by steganographic algorithms. but by using ML it enhance the representation of hidden information.
- Improved Training Convergence: increase the rate of convergence during training.
- Robustness to Various Steganographic Methods: Make sure the steganalysis model works properly with a variety of steganographic algorithms. as there are a variety of strategies that can be used to hide information inside an image. The CNN should be reliable and able to identify steganographic material regardless of the particular steganographic technique used.
- Interpretable Feature Extraction: Facilitate a better understanding of the features learned by the network.
- Achieving State-of-the-Art Performance: achieve high accuracy and outperform steganalysis methods.

So The main objectives of CNN for image steganalysis revolve around enhancing feature learning, handling training diffculties , ensuring robustness , achieving interpretability and achieving the state of the art performance.

3.6 User Characteristics

The system will include individuals , professionals , and organizations in the fields of cybersecurity , digital Forensics and information security. Here are some user characteristics that might be associated with our system.

- Educational organizations
- Law enforcement and government agencies
- Security consultants
- Social Media security
- Machine Learning and AI Researchers

4 Functional Requirements

4.1 System Functions

The below figure represent the use case diagrams of the project. Figure (3) shows the use case diagram of users interacting with the application and on the other side it shows the system use case diagram.

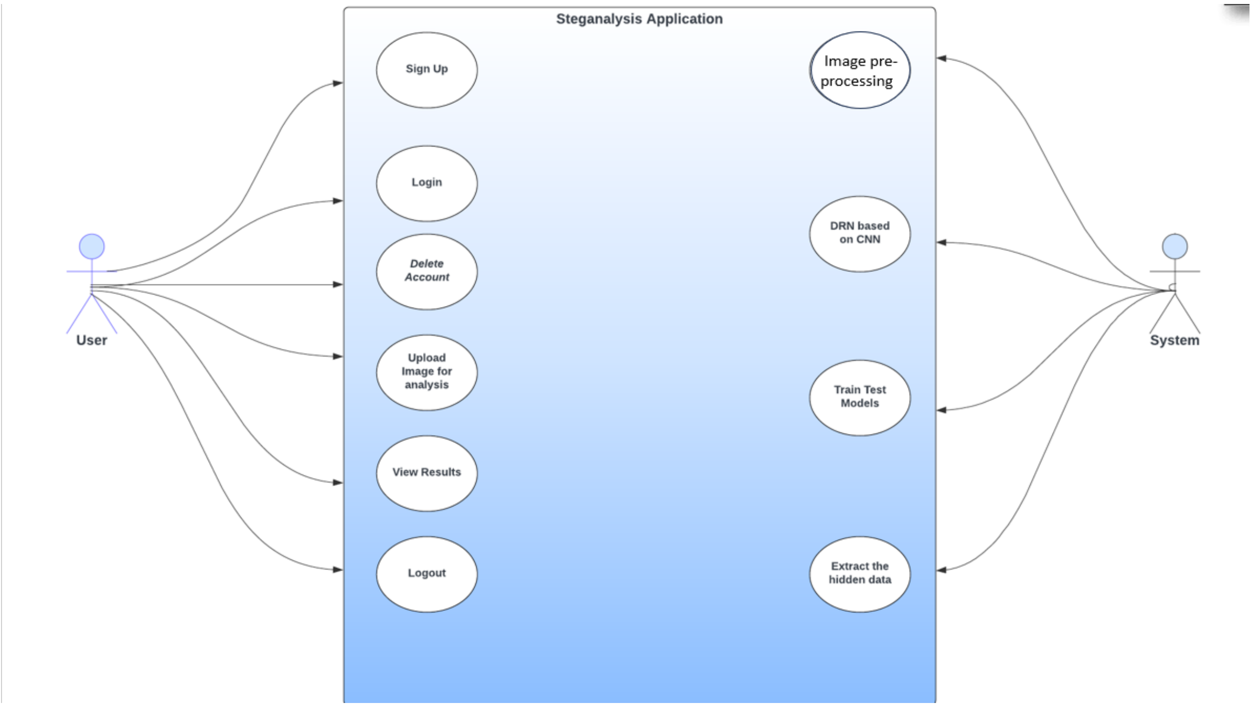


Figure 6: System's use case

- **ID:1** The user will have the ability to sign up.
- **ID:2** The user will have the ability to access his/her accounts.
- **ID:3** The user will have the ability to delete their account.
- **ID:4** The user will have the ability to Log off their account.
- **ID:5** The user will have the ability to upload an image for analysis.
- **ID:6** The user will have the ability to view the results.
- **ID:7** The user will have the ability to delete their account.
- **ID:8** The System will be able to extract the uploaded image.
- **ID:9** The system will be able to apply CNN algorithms to the image.
- **ID:10** The system will be able to train models.

4.2 Detailed Functional Specification

Table 2: Uploading image Function Description

Name	Upload an Image
Code	ID:5
Priority	High
Critical	To make data available to process and classify.
Description	The function role is to upload an image to the system to get processed and classified.
Input	Image
Output	Boolean: true if image is accepted.
Pre-condition	User having a previously saved image on their device.
Post-condition	The Image being processed
Dependency	depends on the presence of a saved image to upload.
Risk	No image uploaded

Table 3: Image Extraction Function Description

Name	Extract the hidden info.
Code	ID:8
Priority	High
Critical	To extract information from image.
Description	The function is responsible extracting features from image.
Input	Image
Output	Boolean: true if image is accepted.
Pre-condition	User having an uploaded an image.
Post-condition	Hidden content is extracted
Dependency	depends on the presence of an image.
Risk	No image uploaded

Table 4: View Results Function Description

Name	View results
Code	ID:6
Priority	High
Critical	To allow user to view the results of the process
Description	The function is responsible for showing the results of the user's inquiry.
Input	Image
Output	Success or error message.
Pre-condition	User having an uploaded an image from their device.
Post-condition	The Image is processed
Dependency	depends on the presence of a saved image to upload.
Risk	No image uploaded

Table 5: CNN Algorithm Function Description

Name	CNN
Code	ID: 9
Priority	High
Critical	To allow user to view the results of the process
Description	The function is responsible for applying CNN algorithms to images.
Input	Image
Output	Boolean.
Pre-condition	Data Availability.
Post-condition	Data is processed
Dependency	depends on the presence of data.
Risk	Classification failed

5 Design Constraints

This section is to provide the system limitations that would be an issue for us and for the users while using the system .

5.1 Standards Compliance

The user should be connected to internet to use the stegasus application .

5.2 Network Constraint

It is cruical to have a stable internet connection, due to the process of the image classification and message extraction being done on the web application.

5.3 Other Constraints as appropriate

our stegasus application supports English language only .

6 Non-functional Requirements

6.1 Security

our stegasus application protects users information that will be uploaded .

6.2 Availability

Users can access the system at any time because it will always be available.

6.3 Usability

We'll make sure our online applications are easy to use for everyone by offering an intuitive user experience.

6.4 Performance

Depending on how quickly the user can access the internet, the detecting process shouldn't take long time.

6.5 Portability

Any device with internet connection can view the stegasus application.

7 Data Design

- BOSSbase 1.01 is dataset that consists of 10,000 uncompressed grayscale images. The images' size is 512x512. It's know to be the most commonly used dataset for steganalysis [8].The images contained are of PGM type [9]. Due to the general settings in recent CNN based steganalysis, the images are cropped to the size 256x256[2] to use in training.

Figure 7: A sample from the dataset.

- The CIFAR-10 dataset consists of 60000 32x32 colour images in 10 classes, with 6000 images per class. There are 50000 training images and 10000 test images. With 10,000 photos apiece, the dataset is split into five training batches and one test batch. There are precisely 1000 randomly chosen photos from each class in the test batch. The remaining photographs are divided into training batches and are arranged randomly; however, certain training batches may have more images from a particular class than others. The training batches have exactly 5000 photos from each class combined.

8 Preliminary Object-Oriented Domain Analysis

The **initial** class diagram.

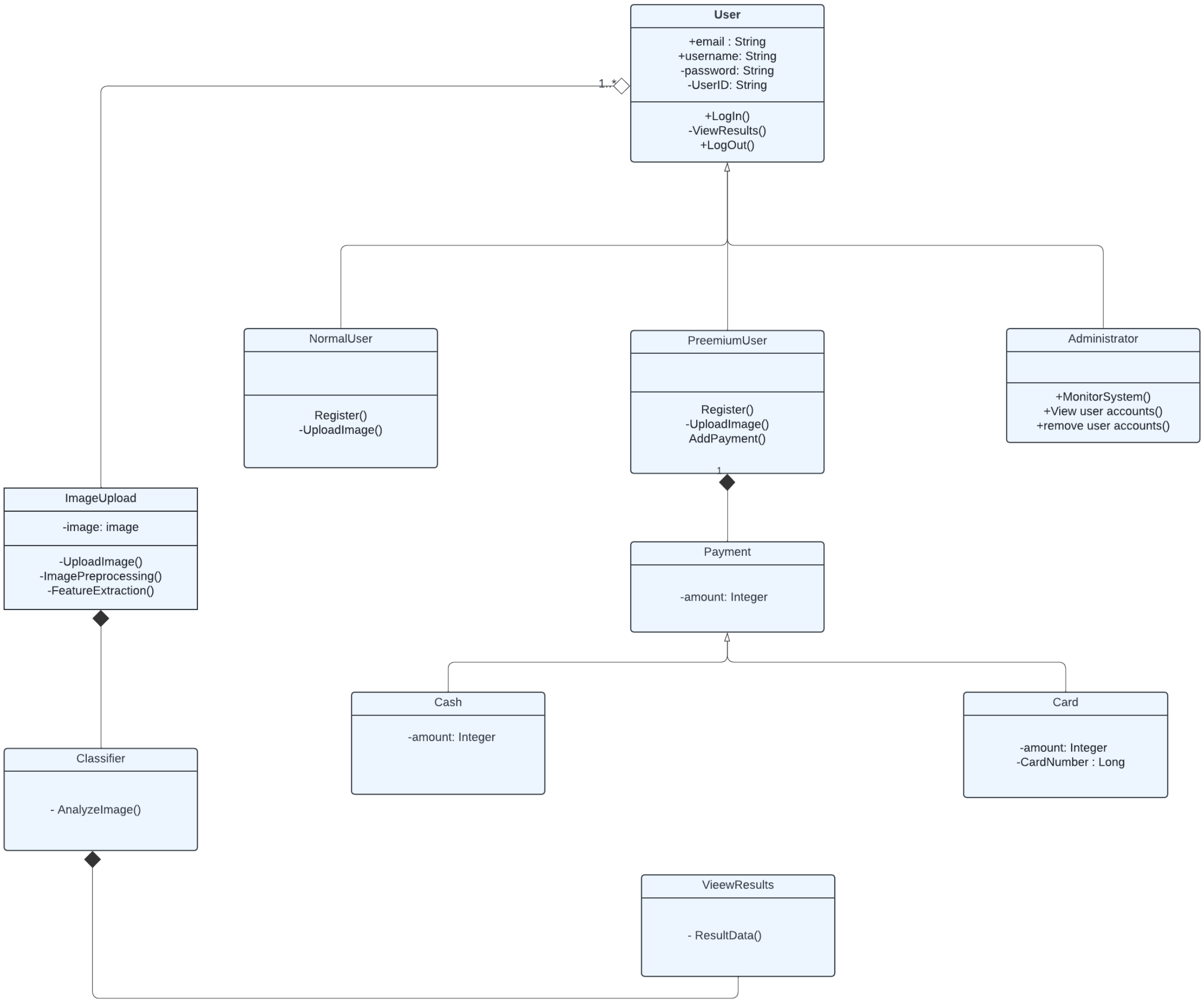


Figure 8: Initial UML class diagram

9 Operational Scenarios

9.1 Scenario 1:

The user starts by siging up /logging into the web application to be able to access the tool . then he will be able to upload an image. Furthermore , the system will detect if there is any malicious content or anything hidden in the uploaded image .

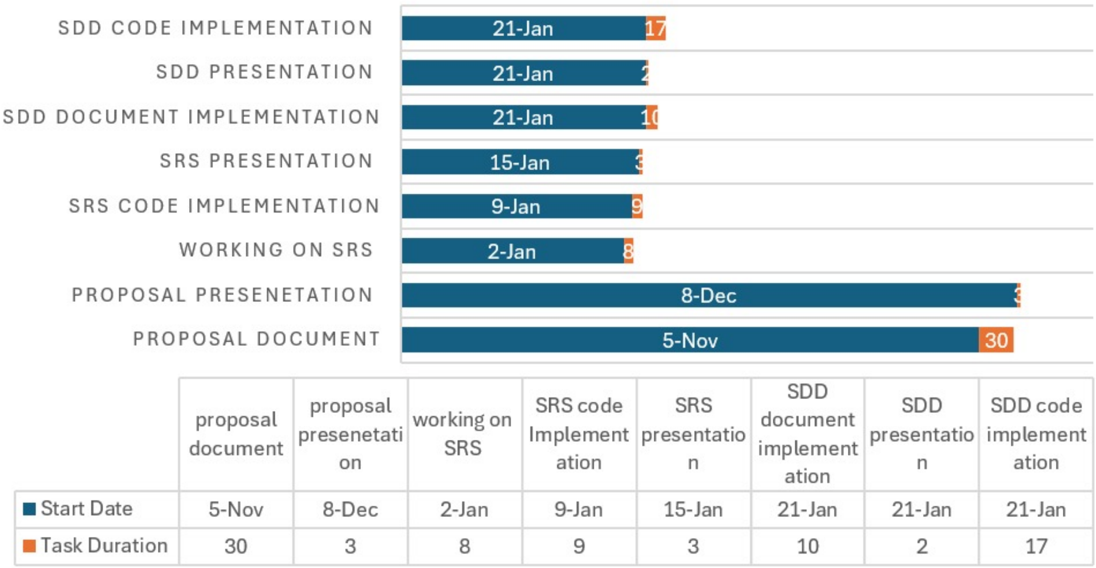
9.2 Scenario 2:

After the image has been processed the user will be able to view the results and see if there is any hidden information or steganographic content . Moreover , the user has the option to save the results.

9.3 Scenario 3:

The system will check the image uploaded and start the process.If it classifies as a stego image or cover image, it will report to the user.

10 Project Plan



	proposal document	proposal presenetation	working on SRS	SRS code Implementation	SRS presentation	SDD document implementation	SDD presentation	SDD code implementation
■ Start Date	5-Nov	8-Dec	2-Jan	9-Jan	15-Jan	21-Jan	21-Jan	21-Jan
■ Task Duration	30	3	8	9	3	10	2	17

Figure 9: Project Time Plan

11 Appendices

11.1 Definitions, Acronyms, Abbreviations

CNN	Convolutional Neural Network that is used in object detection and recognition [3].

11.2 Supportive Documents

We made a survey to help us understand and know the user's information about Steganalysis. The following are the results.

1. When asked about if familiar with the term "CNN"

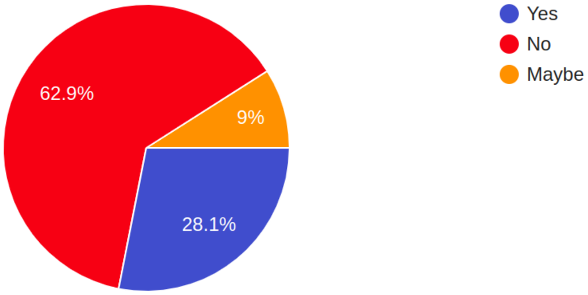


Figure 10: Survey's first question answers.

2. When asked about the importance of CNN algorithm, with 5 being very important and 1 being not important.

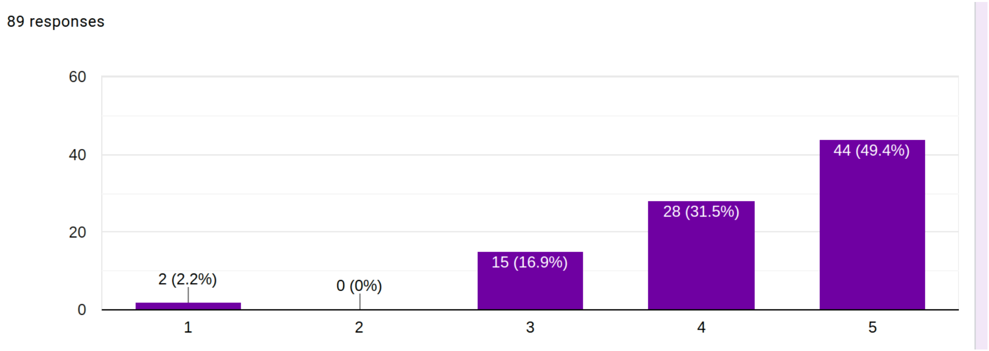


Figure 11: survey's second question answers.

3. When asked about which media type is most used in Steganalysis?

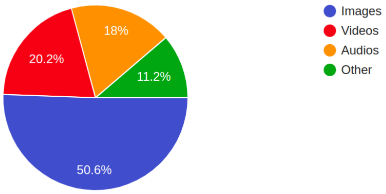


Figure 12: Survey's third question answers.

4. When asked about if interested in learning about Machine learning algorithms.

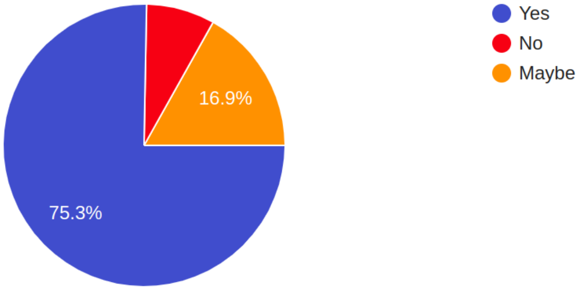


Figure 13: Survey's fourth and last question answers.

References

[1] Siwei Lyu and Hany Farid. "Steganalysis using higher-order image statistics". In: *IEEE Transactions on information Forensics and Security* 1.1 (2006), pp. 111–119.

[2] Songtao Wu, Shenghua Zhong, and Yan Liu. "Deep residual learning for image steganalysis". In: *Multimedia tools and applications* 77 (2018), pp. 10437–10453.

[3] Jaeyoung Kim, Hanhoon Park, and Jong-Il Park. "CNN-based image steganalysis using additional data embedding". In: *Multimedia Tools and Applications* 79 (2020), pp. 1355–1372.

[4] Weike You, Hong Zhang, and Xianfeng Zhao. "A Siamese CNN for image steganalysis". In: *IEEE Transactions on Information Forensics and Security* 16 (2020), pp. 291–306.

[5] Tabares-Soto Reinel et al. "GBRAS-Net: a convolutional neural network architecture for spatial image steganalysis". In: *IEEE Access* 9 (2021), pp. 14340–14350.

[6] Baraa Tareq Hammad, Ismail Taha Ahmed, and Norziana Jamil. "A Steganalysis Classification Algorithm Based on Distinctive Texture Features". In: *Symmetry* 14.2 (2022). ISSN: 2073-8994. DOI: 10.3390/sym14020236. URL: https://www.mdpi.com/2073-8994/14/2/236.

[7] Trivikram Muralidharan et al. "The infinite race between steganography and steganalysis in images". In: *Signal Processing* 201 (2022), p. 108711. ISSN: 0165-1684. DOI: https://doi.org/10.1016/j.sigpro.2022.108711. URL: https://www.sciencedirect.com/science/article/pii/S016516842200250X.

[8] Lei Zhang et al. "Dataset mismatched steganalysis using subdomain adaptation with guiding feature". In: *Telecommunication Systems* 80.2 (2022), pp. 263–276.

[9] Jean De La Croix Ntivuguruzwa and Tohari Ahmad. "A convolutional neural network to detect possible hidden data in spatial domain images". In: *Cybersecurity* 6.1 (2023), p. 23.