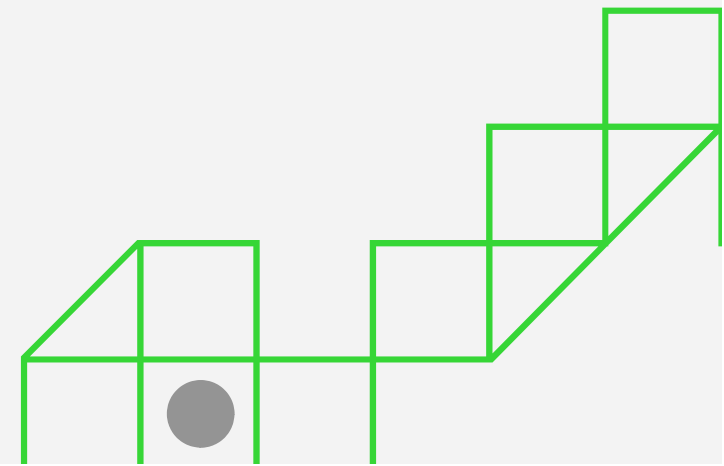
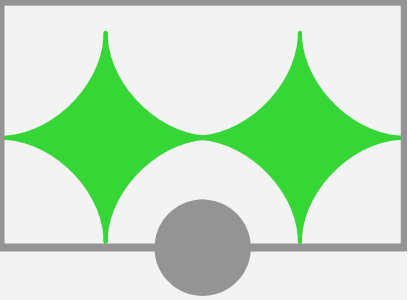




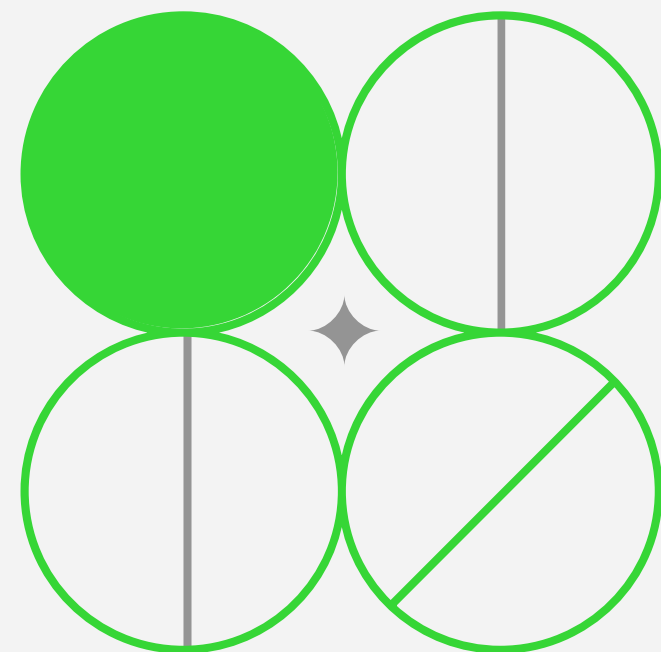
Developing a Web-Based Tool for Image Analysis of Hidden Data Through LSB Encoding: A Cybersecurity and Forensic Approach Using Python, Flask, and React





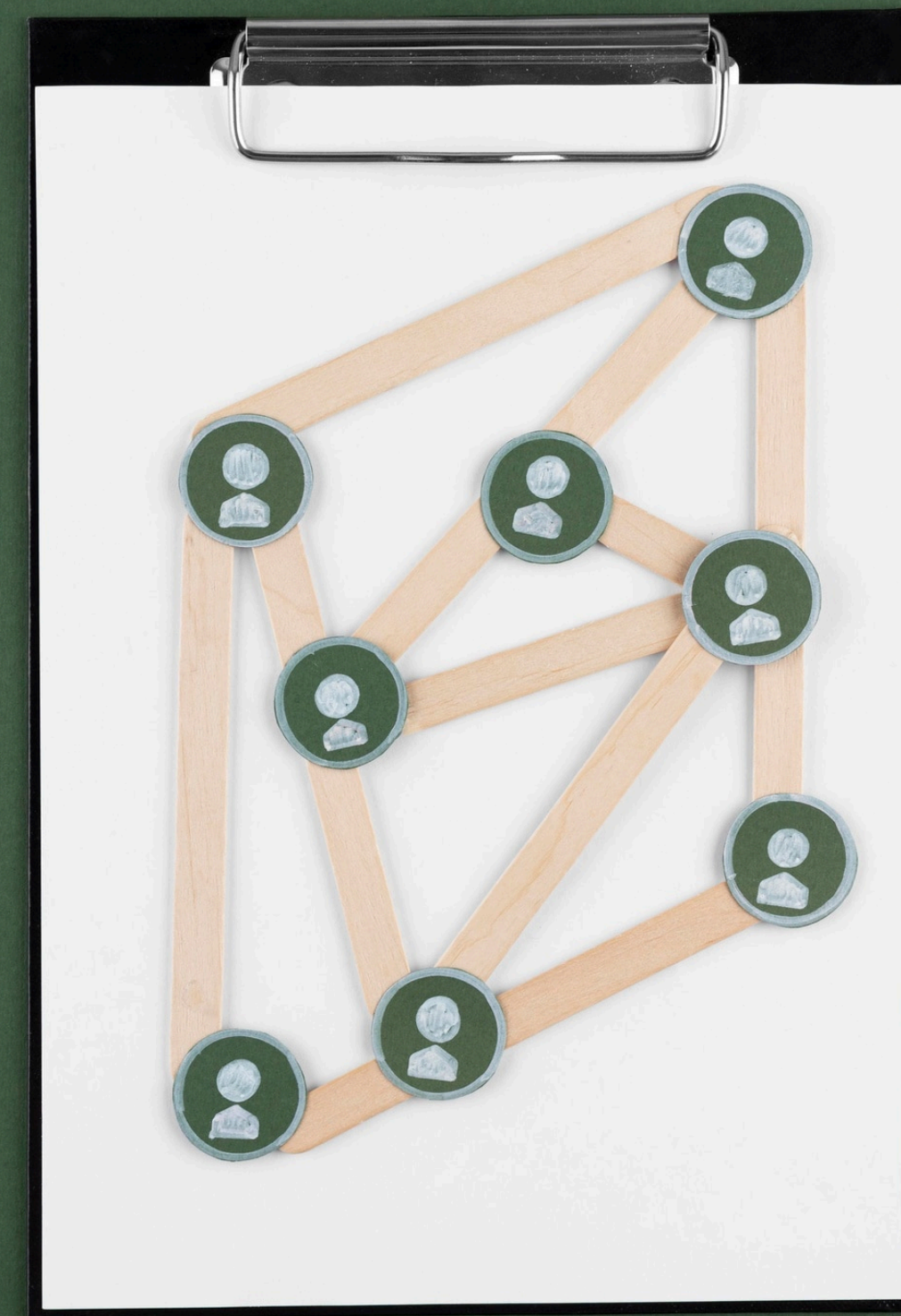
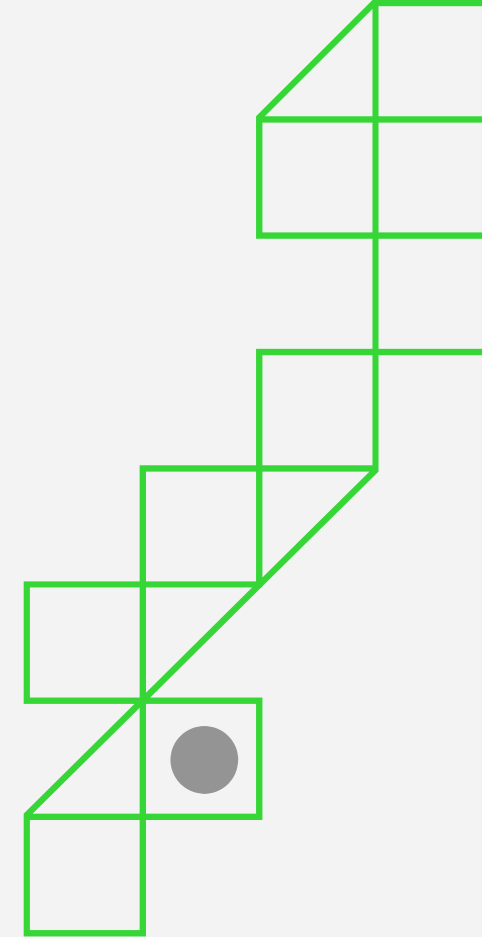
Introduction

Developing a Web-Based Tool for image analysis is crucial in uncovering hidden data through **Least Significant Bit (LSB)** encoding. This presentation explores a **cybersecurity** and **forensic** approach using **Python**, **Flask**, and **React**. We aim to enhance the detection and extraction of concealed information.



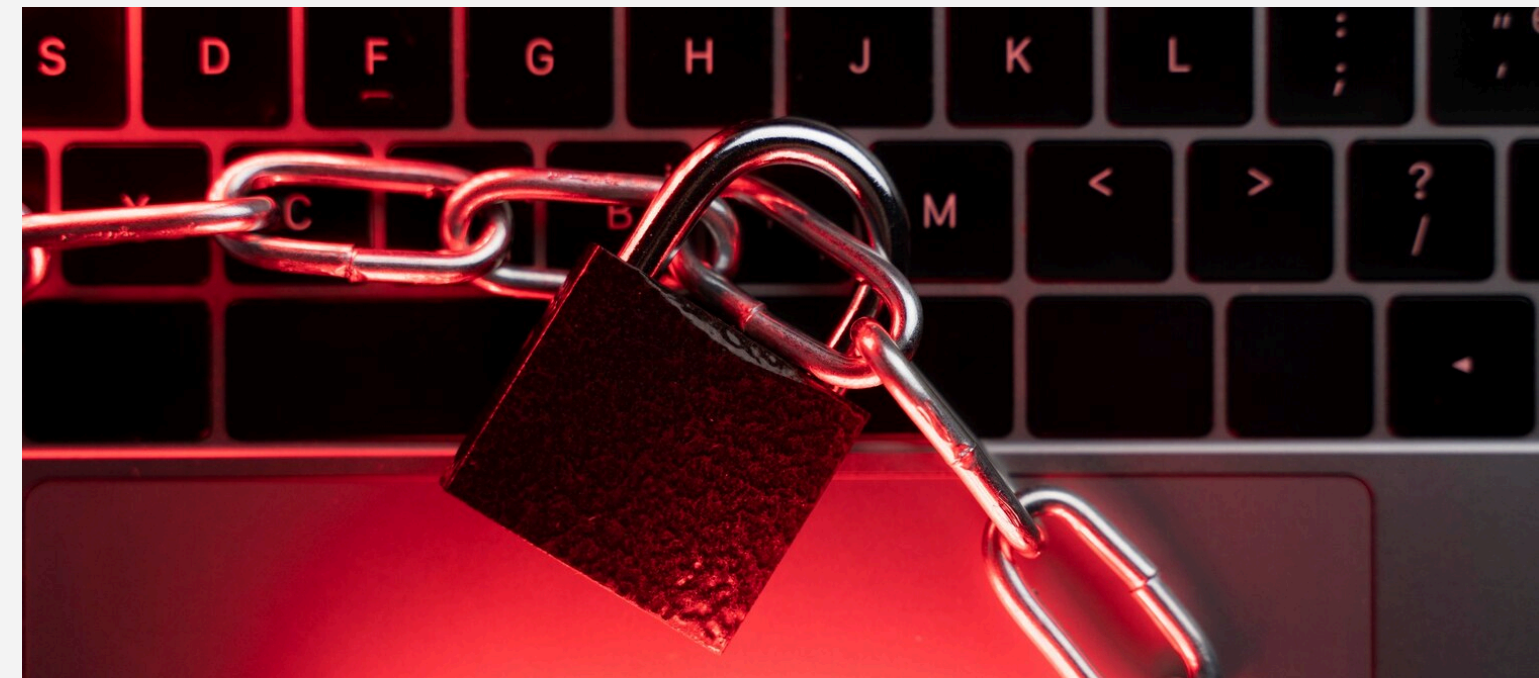
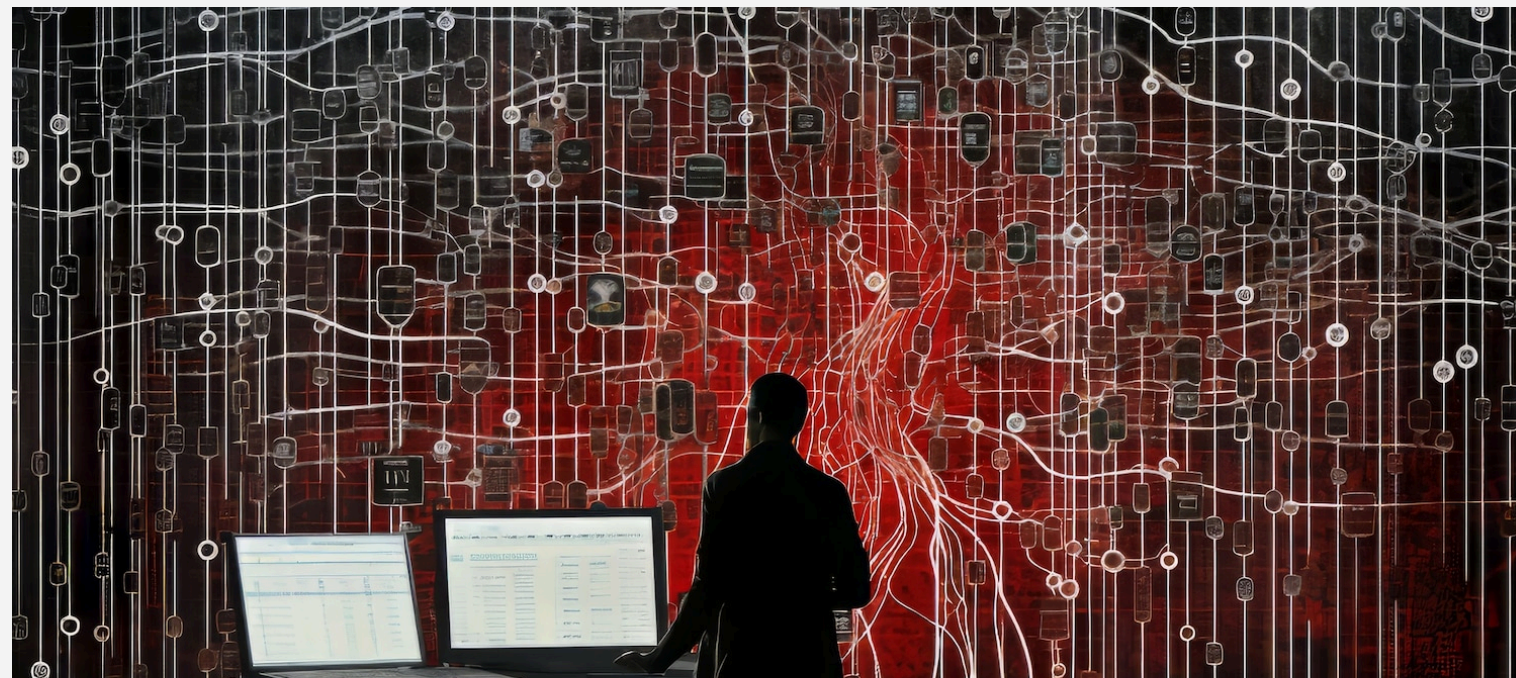
Understanding LSB Encoding

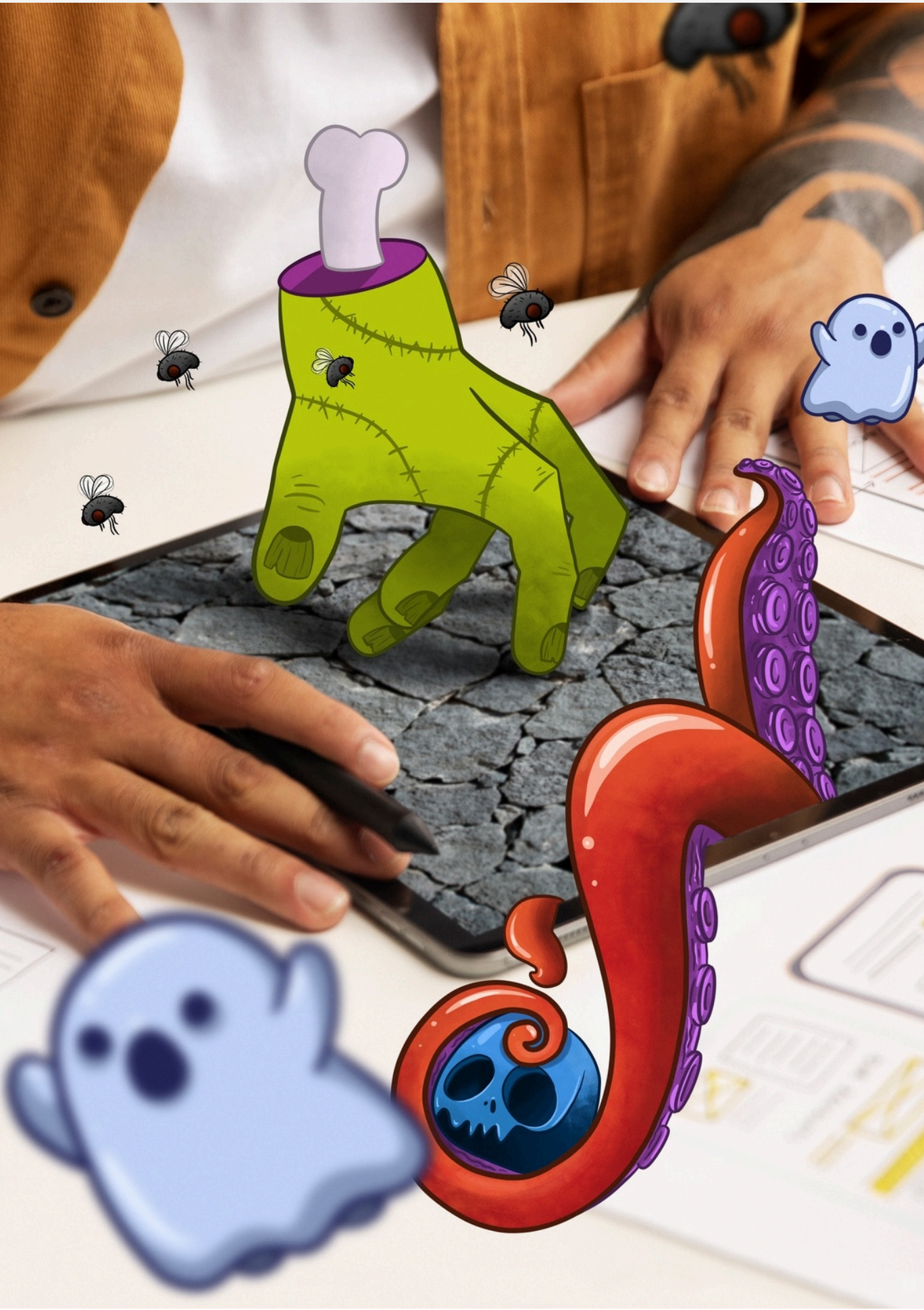
Least Significant Bit (LSB) encoding is a technique used to hide data within digital images. By altering the least significant bits of pixel values, we can embed secret information without significantly affecting the image's appearance. This method is widely used in **steganography** for secure communication.



CYBERSECURITY IMPLICATIONS

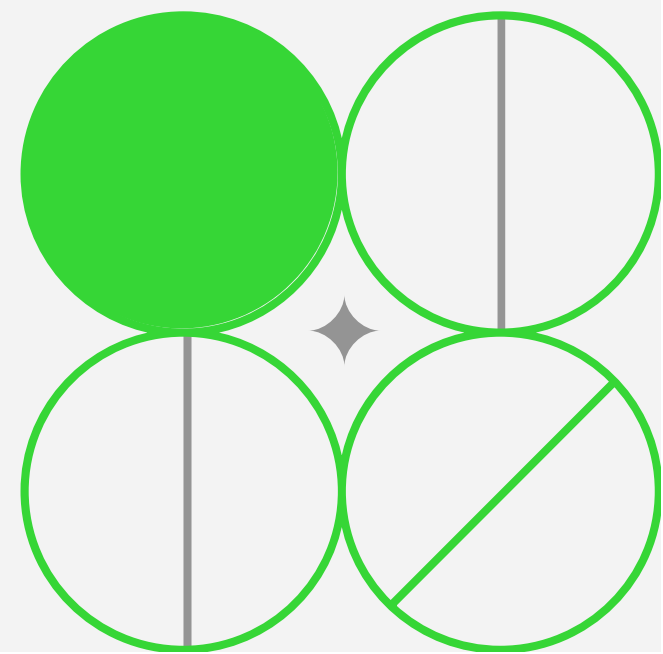
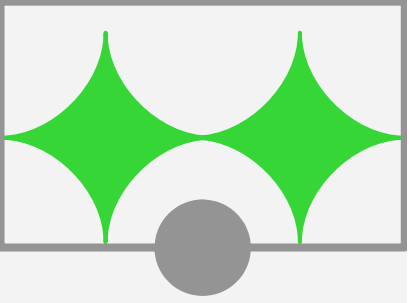
The use of **LSB encoding** raises significant **cybersecurity** concerns. Hidden data can be exploited for malicious purposes, making it essential to develop tools that can detect and analyze such techniques. Understanding these implications is vital for protecting sensitive information.





Forensic Analysis Techniques

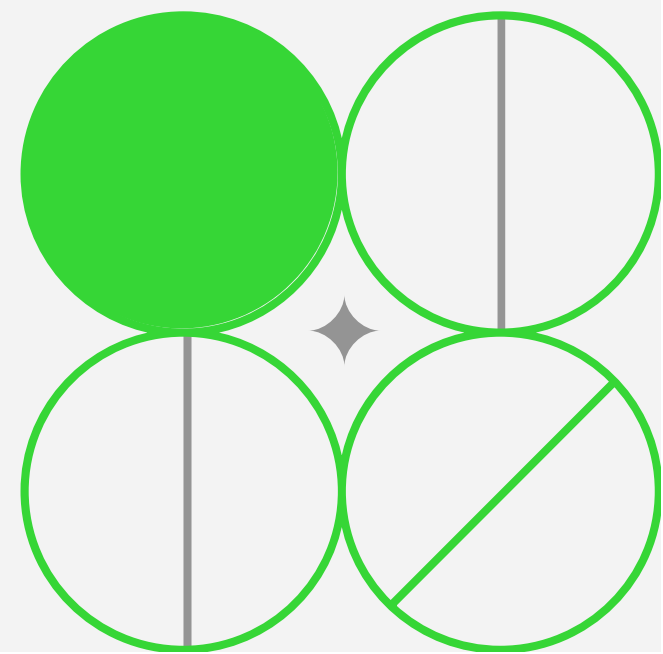
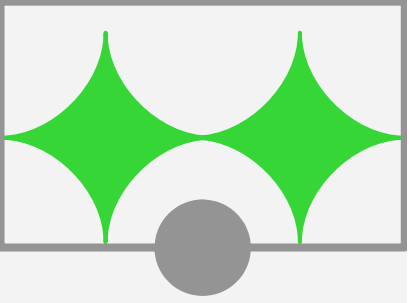
In **digital forensics**, analyzing images for hidden data is a critical task. Techniques such as **statistical analysis** and **pattern recognition** are employed to identify anomalies in image files. This presentation will detail how our tool integrates these techniques for effective analysis.





Technology Stack Overview

Our web-based tool leverages **Python** for backend processing, **Flask** for web framework capabilities, and **React** for a dynamic user interface. This combination provides a robust platform for implementing **image analysis** and enhances user experience through responsive design.

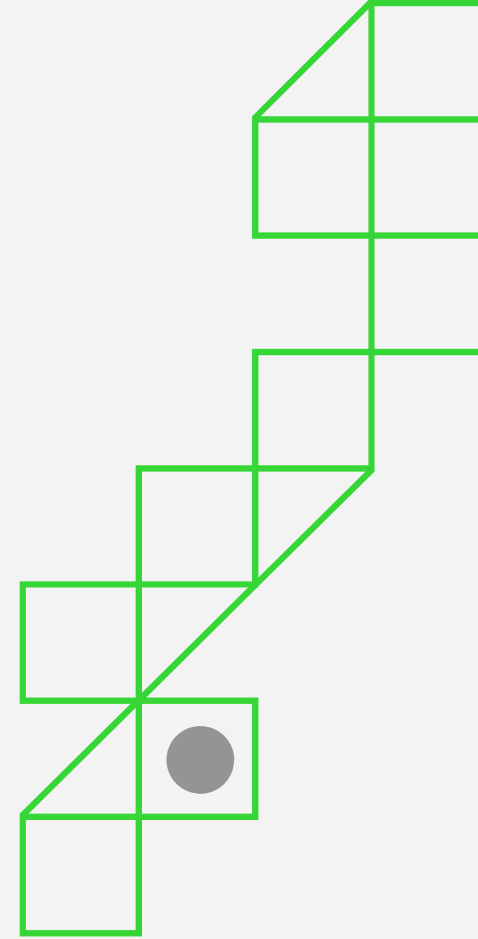




Tool Features

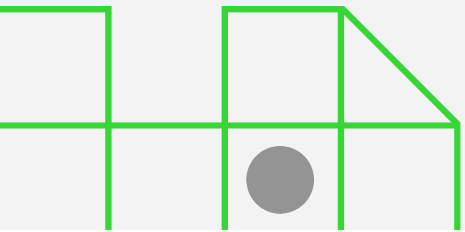
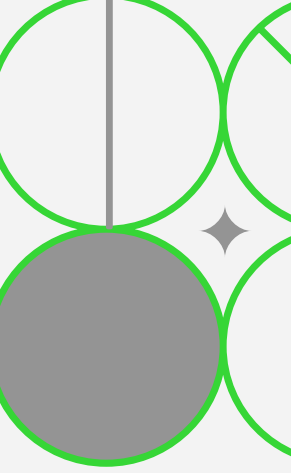
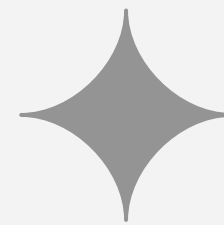
The developed tool offers several key features: **image upload**, **data extraction**, and **report generation**.

Users can upload images, analyze them for hidden data, and generate comprehensive reports detailing the findings. This functionality supports both **cybersecurity** professionals and forensic investigators.



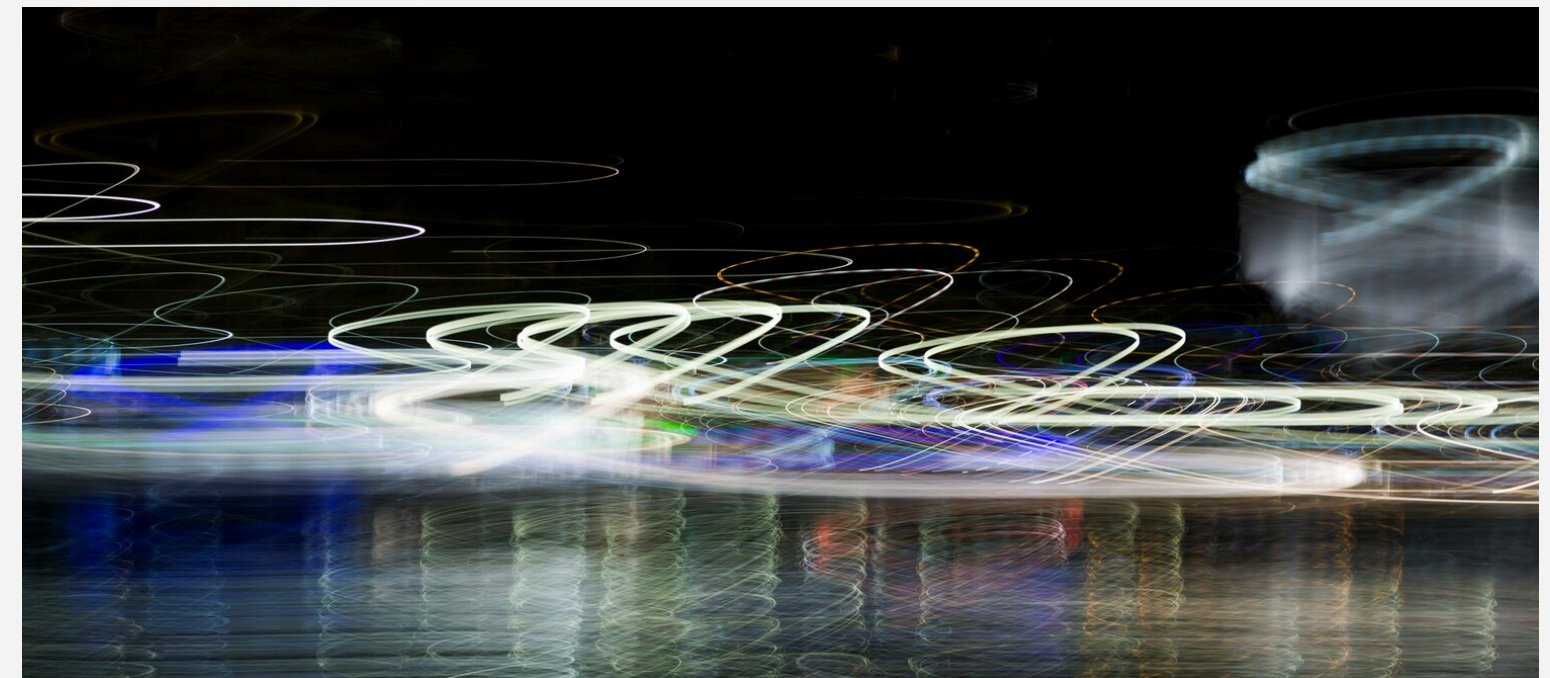
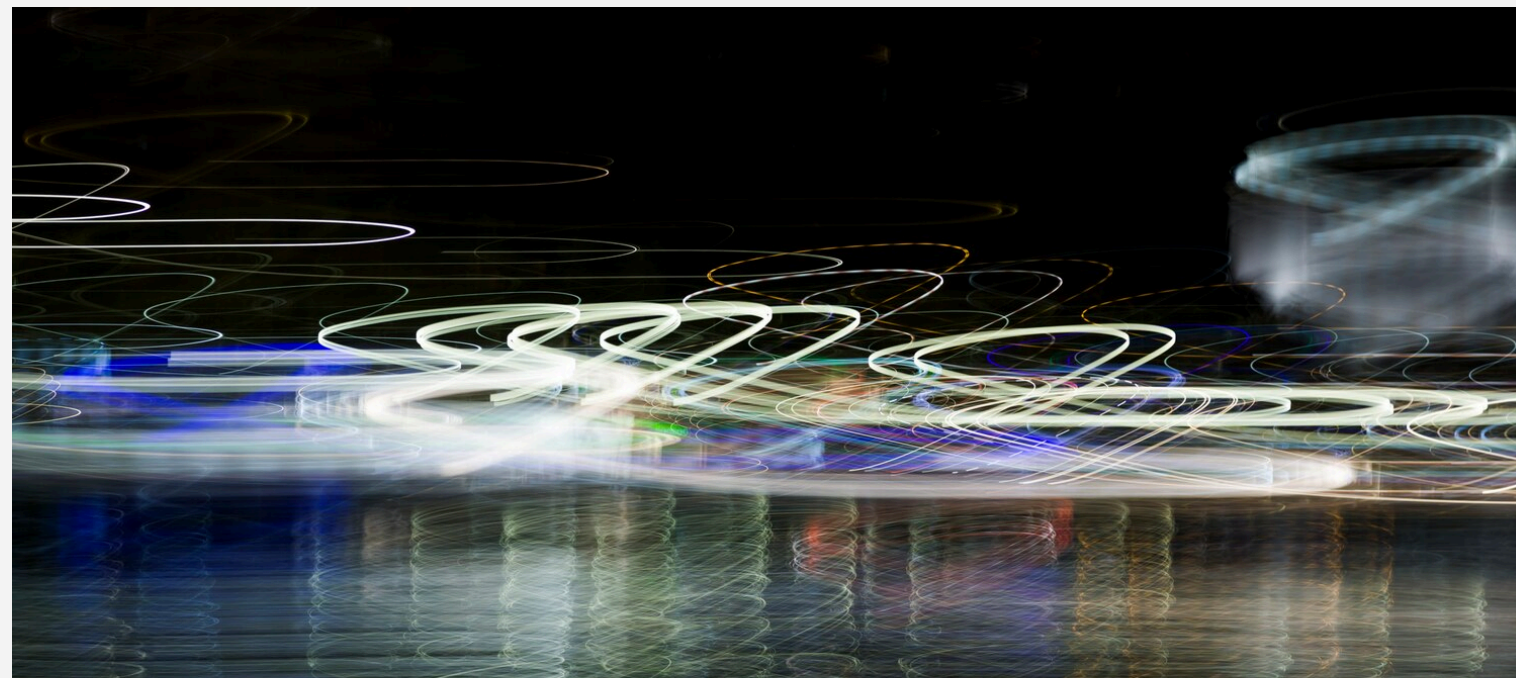
Challenges Faced

During development, we encountered challenges such as **data integrity** issues and the need for **real-time analysis**. Balancing performance with accuracy was crucial. This section will discuss the strategies implemented to overcome these obstacles while ensuring the tool's reliability.



FUTURE ENHANCEMENTS

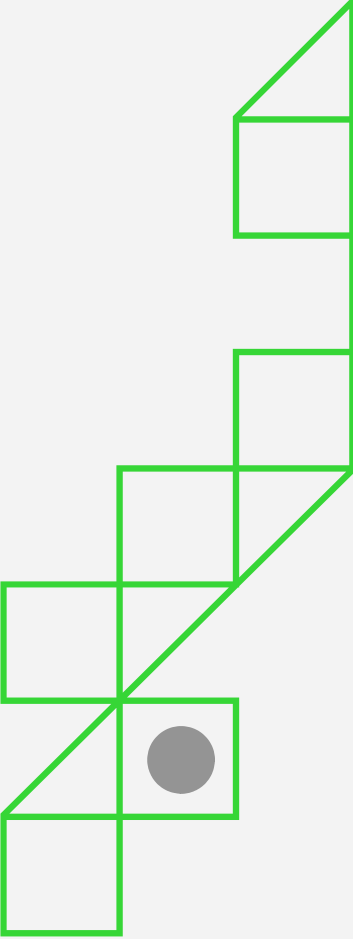
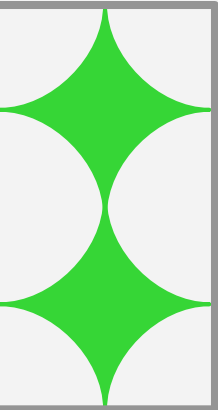

Looking ahead, we plan to incorporate **machine learning** algorithms to improve detection rates of hidden data. Additionally, expanding compatibility with various image formats will enhance the tool's usability. Continuous updates will ensure it remains effective against evolving threats.

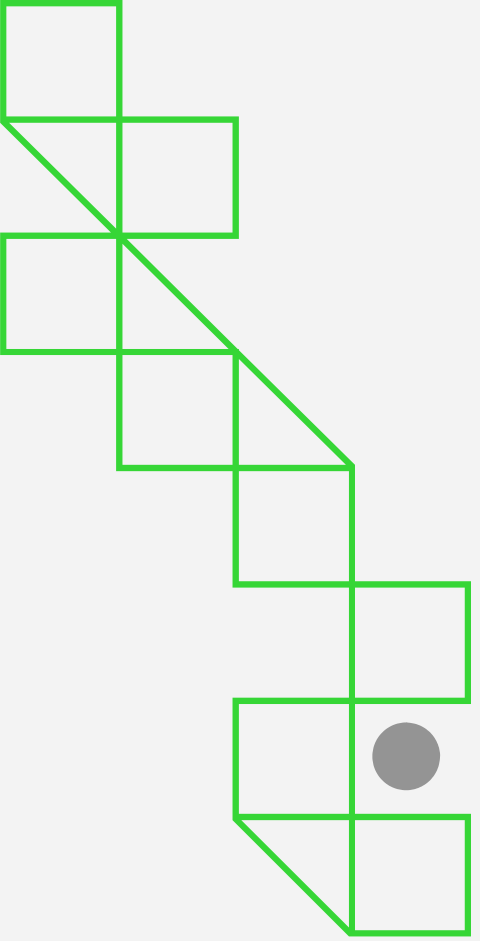




CONCLUSION

In conclusion, developing a web-based tool for image analysis using **LSB encoding** provides valuable insights into **cybersecurity** and **forensic** investigations. By leveraging modern technologies like **Python**, **Flask**, and **React**, we can enhance the detection of hidden data, contributing to safer digital environments.





Thanks!

ANY QUESTIONS?

wassimna0@gmail.com+

216 27309687

AI text generation failed.

