Ex.No.8: Use StegExpose to Detect Hidden Data in Images

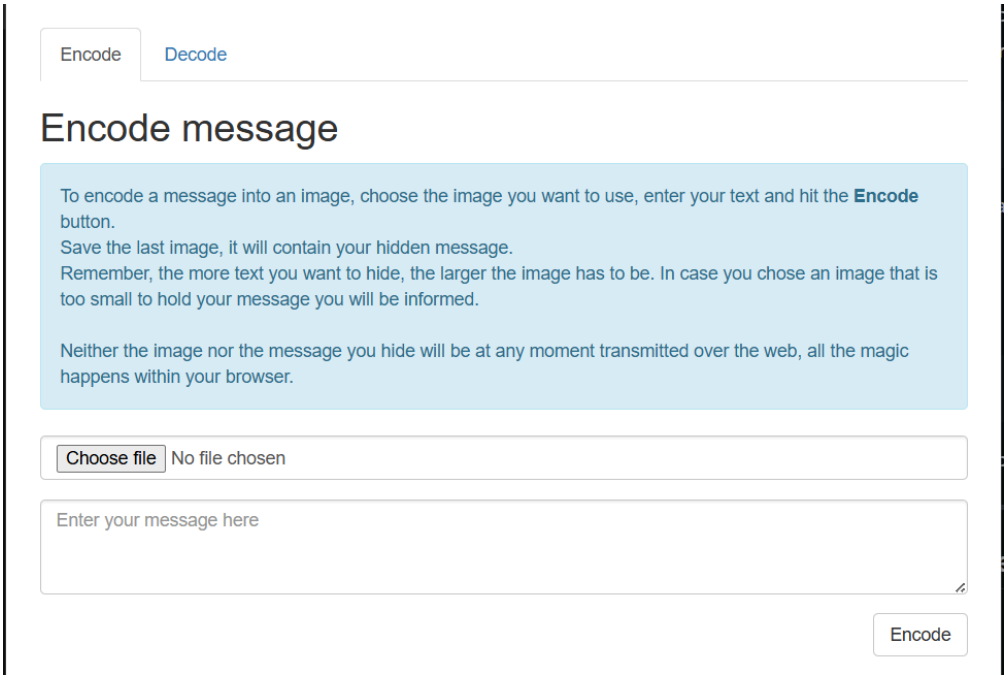
Aim

To detect the presence of hidden data within digital images using **StegExpose**, a steganalysis tool that evaluates image statistics to identify steganographic content.

Step-by-Step Procedure

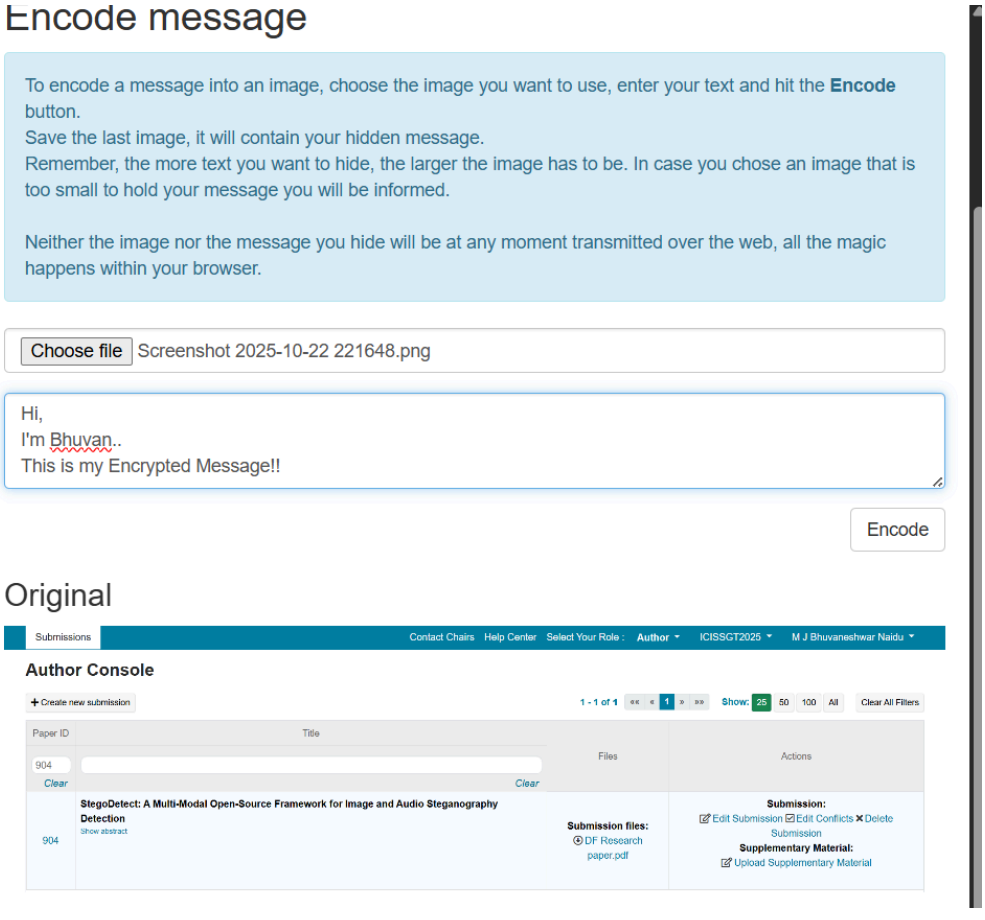
Step1: Download and Set Up for Steganography

1. Visit the **StegExpose GitHub page** and download the `.jar` file.
2. Ensure **Java** is installed on your system. If not, download it from Oracle's official website.
3. Place the `StegExpose.jar` file in your working directory (e.g., `C:\DF\StegExpose\`).
4. Or you can run it online, using any Steganography tools available online.



Step2: Select Images for Encrytion

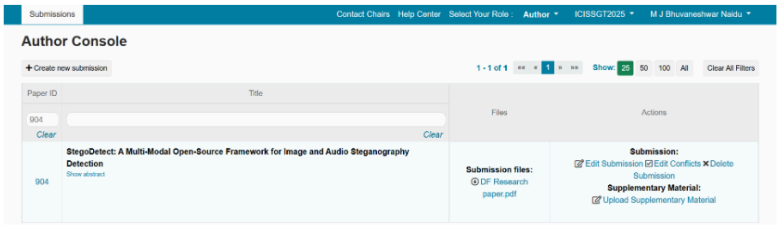
- Select the file you want to hide data.
- Give the message you want to encrypt in the file.
- Supported formats include `.png` , `.jpg` , `.bmp` and `.pdf` .



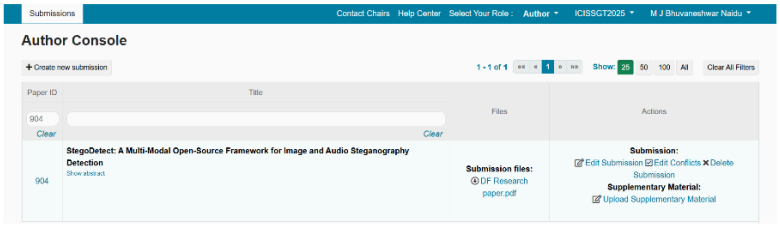
Step3: Compare and Save the Stegno Image

1. Compare the difference between the normal and the stegnoimage.
2. Right click the image and click on save image.
3. Name the file as **Stegno image** and click on save.

Normalized

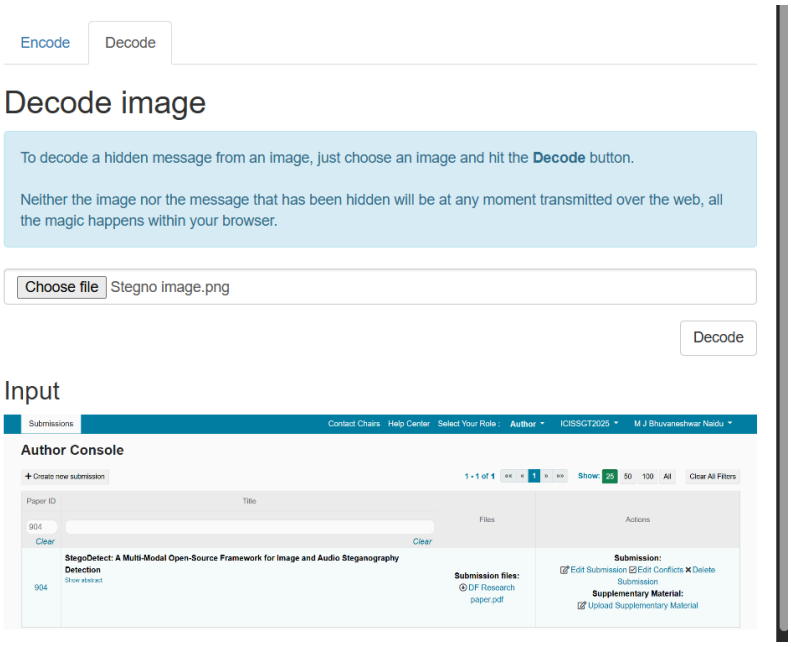


Message hidden in image (right click ➡ save as)

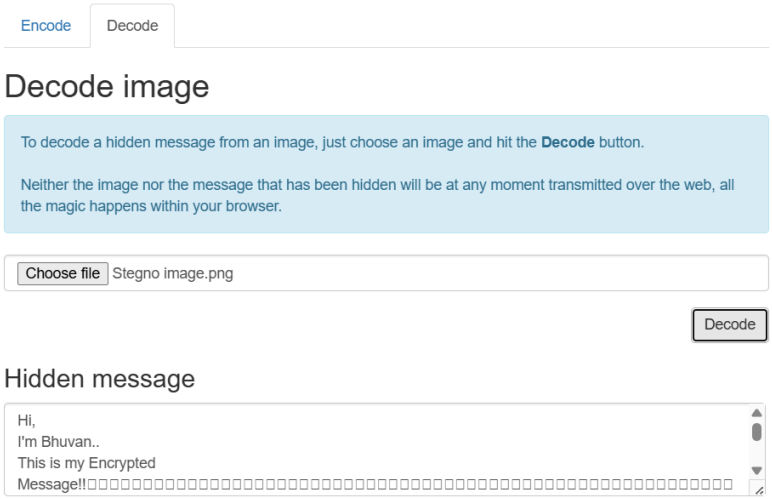


Step4: Run Decode on a Stegno Image

1. Select the image you want decode.
2. Click on decode.



Step5: Analyze the Output



Rubrics

Criteria	Mark Allotted	Mark Awarded
1. GitHub Activity & Submission Regularity	3	
2. Application of Forensic Tools & Practical Execution	3	
3. Documentation & Reporting	2	
4. Engagement, Problem-Solving & Team Collaboration	2	
Total	10	

Result

Successfully used **StegExpose** to perform steganalysis on images, identified potential hidden data through suspect scores, and interpreted the likelihood of steganography based on the tool's statistical output.