



Bhuvaneshwar-Naidu / DF_Lab



Code

Issues

Pull requests

Actions

Projects

Wiki

Security



DF_Lab / Exp_8_StegExpose.md



Bhuvaneshwar-Naidu Update Exp_8_StegExpose.md

7095d80 · now



64 lines (45 loc) · 2.41 KB

Preview

Code

Blame



Raw



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.

[Encode](#)[Decode](#)

Encode message

To encode a message into an image, choose the image you want to use, enter your text and hit the **Encode** button.

Save the last image, it will contain your hidden message.

Remember, the more text you want to hide, the larger the image has to be. In case you chose an image that is too small to hold your message you will be informed.

Neither the image nor the message you hide will be at any moment transmitted over the web, all the magic happens within your browser.

 No file chosen

Enter your message here

Step2: Select Images for Encryption

- 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`.

Encode message

To encode a message into an image, choose the image you want to use, enter your text and hit the **Encode** button.

Save the last image, it will contain your hidden message.

Remember, the more text you want to hide, the larger the image has to be. In case you chose an image that is too small to hold your message you will be informed.

Neither the image nor the message you hide will be at any moment transmitted over the web, all the magic happens within your browser.

 Screenshot 2025-10-22 221648.png

Hi,
I'm Bhuvan...
This is my Encrypted Message!!

Original

[Submissions](#)[Contact Chairs](#) [Help Center](#) [Select Your Role :](#) [Author](#) [ICISSCT2025](#) [M J Bhuvaneshwar Naidu](#)

Author Console

[+ Create new submission](#)

1 - 1 of 1 < < < 1 > >> Show: 25 50 100 All Clear All Filters

Paper ID

Title

904

Clear

Files

Actions

Clear

StegoDetect: A Multi-Modal Open-Source Framework for Image and Audio Steganography Detection
[Show abstract](#)

904

Submission files:
④ DF Research paper.pdf**Submission:**
 Edit Submission Edit Conflicts Delete
Supplementary Material:
 Upload Supplementary Material

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

The screenshot shows the 'Author Console' interface. At the top, there are navigation links: Submissions, Contact Chairs, Help Center, Select Your Role: Author, ICISSGT2025, and M J Bhuvaneswar Naidu. Below this is a search bar with 'Paper ID' and 'Title' fields, and a 'Clear' button. The main area displays a single submission entry for paper ID 904, titled 'StegoDetect: A Multi-Modal Open-Source Framework for Image and Audio Steganography'. The submission includes a file named 'DF Research paper.pdf'. On the right side, there are 'Actions' buttons for 'Edit Submission', 'Edit Conflicts', 'Delete', 'Submission', and 'Supplementary Material'.

Message hidden in image (right click → save as)

This screenshot is identical to the one above, showing the same submission entry for paper ID 904. The only difference is the text 'Message hidden in image (right click → save as)' displayed prominently at the top left of the interface.

Step4: Run Decode on a Stegno Image

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

The screenshot shows the 'Decode' interface. At the top, there are two buttons: 'Encode' and 'Decode'. Below them is a section titled 'Decode image' with the instruction: 'To decode a hidden message from an image, just choose an image and hit the **Decode** button.' A note below states: 'Neither the image nor the message that has been hidden will be at any moment transmitted over the web, all the magic happens within your browser.' A file input field shows 'Choose file Stegno image.png' and a 'Decode' button.

Input

This screenshot shows the 'Author Console' again, this time with the 'Input' tab selected. It displays the same submission entry for paper ID 904. The 'Actions' column includes buttons for 'Edit Submission', 'Edit Conflicts', 'Delete', 'Submission', and 'Supplementary Material'.

Step5: Analyze the Output

Encode Decode

Decode image

To decode a hidden message from an image, just choose an image and hit the **Decode** button.

Neither the image nor the message that has been hidden will be at any moment transmitted over the web, all the magic happens within your browser.

Stegno image.png

Hidden message

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.