Proof of Concept (PoC) – Stenographic File Integrity Checker

This document explains a simple Proof of Concept (PoC) for a File Integrity Checker that uses steganography to hide cryptographic hashes (SHA256) inside cover files (images). The tool allows generating file hashes, embedding them into images, and later extracting and verifying them.

Required Modules

1. hashlib → for SHA256 hashing of files.

2. Pillow (PIL) → for image manipulation and steganography.

Install using:

pip install pillow

Main Parts of the PoC Code

1. Hashing Function: Uses hashlib to compute SHA256 hash of a target file.

2. Embedding Function: Encodes the hash into the least significant bits of an image's pixels.

3. Extraction Function: Reads hidden bits back from the image to retrieve the hash.

4. Verification: Compares extracted hash with the current file's hash to detect modifications.

How to Run in IDLE

1. Save the Python script as steg_integrity_checker.py.

2. Place a target file (e.g., report.pdf) and a cover image (e.g., cover.png) in the same folder.

3. Run the script in IDLE (press F5).

4. Choose the option to either embed or verify.

5. For verification, the script will report whether the file is unmodified or tampered.

Example Output

Embedding: Successfully embedded hash of report.pdf into cover.png

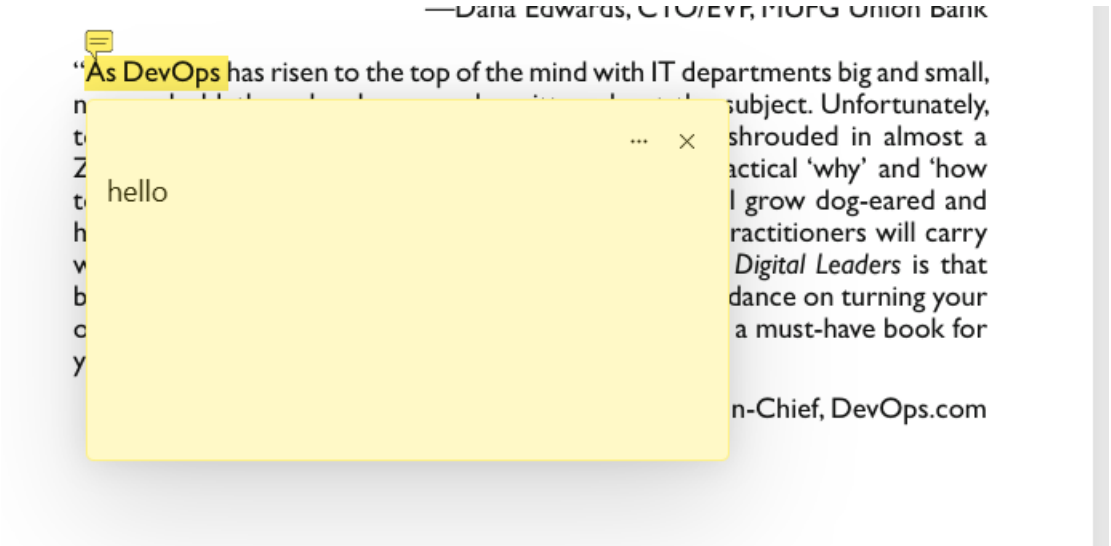
Verification: File integrity check failed! report.pdf has been modified.

```
C:\Users\3520 i5 16GB>pip install pillow
Collecting pillow
  Downloading pillow-11.3.0-cp312-cp312-win_amd64.whl.metadata (9.2 kB)
Downloading pillow-11.3.0-cp312-cp312-win_amd64.whl (7.0 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 7.0/7.0 MB 3.8 MB/s eta 0:00:00
Installing collected packages: pillow
Successfully installed pillow-11.3.0

[notice] A new release of pip is available: 24.0 -> 25.2
[notice] To update, run: python.exe -m pip install --upgrade pip

C:\Users\3520 i5 16GB>
```

```
= RESTART: C:/Users/3520 i5 16GB/AppData/Local/Programs/Python/Python312/Stenogr
aphic.py
=== Stenographic File Integrity Checker ===
Do you want to (E)mbed or (V)erify? E
Enter the path of target file (e.g., report.pdf): C:/Users/3520 i5 16GB/OneDrive
/Desktop/Digisuraksha-week1/DevOps_for_Digital_Leaders.pdf
Enter the path of cover image (e.g., cover.png): C:/Users/3520 i5 16GB/OneDrive/
Desktop/Digisuraksha-week1/shiva_3.jpg
Enter output stego image name (e.g., stego.png): style.png
[+] Hash of target file: 33f4ed98c37d592c6905886130a8617481feb91b6712f22c0346a33
1d31ab664
[+] Hash embedded into style.png
```

```
=== Stenographic File Integrity Checker ===
Do you want to (E)mbed or (V)erify? V
Enter the path of target file (to verify): C:/Users/3520 i5 16GB/OneDrive/Deskto
p/Digisuraksha-week1/DevOps_for_Digital_Leaders.pdf
Enter the path of stego image: style.png
[+] Extracted hash: 33f4ed98c37d592c6905886130a8617481feb91b6712f22c0346a331d31a
b664
[+] Current hash of target: 33f4ed98c37d592c6905886130a8617481feb91b6712f22c0346
a331d31ab664
[✓] File integrity verified — no modification detected.
```

With modification:



After adding a comment.

```
=== Stenographic File Integrity Checker ===
Do you want to (E)mbed or (V)erify? V
Enter the path of target file (to verify): C:/Users/3520 i5 16GB/OneDrive/Deskto
p/Digisuraksha-week1/DevOps_for_Digital_Leaders.pdf
Enter the path of stego image: style.png
[+] Extracted hash: 33f4ed98c37d592c6905886130a8617481feb91b6712f22c0346a331d31a
b664
[+] Current hash of target: 94ea373447efdfb111628027ad9237fb353d888d5f32348441d0
6525c30aec54
[✗] WARNING: File has been modified!
```

Name: Shreya Bishwas Pandey

Intern ID:120