Proof of Concept (PoC) – Stenographic File Integrity Checker

Name : Shivani Yadav

Intern ID : 279

This document explains a simple Proof of Concept (PoC) for a File Integrity Checker that uses QR codes to store and verify cryptographic hashes (SHA256) of files.

The tool allows generating file hashes, converting them into QR codes, and later scanning/decoding the QR codes to verify file integrity.

Required Modules

1. hashlib → for SHA256 hashing of files.
2. qrcode → for generating QR codes.
3. opencv-python (cv2) → for reading and decoding QR codes.

Install using:

```
pip install qrcode opencv-python
```

Main Parts of the PoC Code

1. Hashing Function: Uses hashlib to compute SHA256 hash of a target file.
2. QR Code Generation: Converts the hash into a QR code and saves it as an image.
3. QR Code Decoding: Reads the QR code back to retrieve the stored hash.
4. Verification: Compares the decoded hash with the current file's hash to detect modifications.

How to Run in IDLE

1. Save the Python script as qr_integrity_checker.py.
2. Place a target file (e.g., report.pdf) in the same folder.
3. Run the script in IDLE (press F5).
4. Choose the option to either generate QR or verify.
5. For verification, the script will report whether the file is unmodified or tampered.

Example Output

QR Generation:

```
Successfully generated QR code of report.pdf hash as
report_qr.png
```

Verification (Unmodified):

```
File integrity verified! report.pdf has not been changed.
```

Verification (Modified):

```
File integrity check failed! report.pdf has been altered.
```
