Image Steganography with Cryptography

Name: Ketaki Mahajan
Roll Number: 16014022050
Course: Information & Cyber Security

Internal Assessment 02
Under the guidance of Prof. Makrand Kulkarni

SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College of Engineering

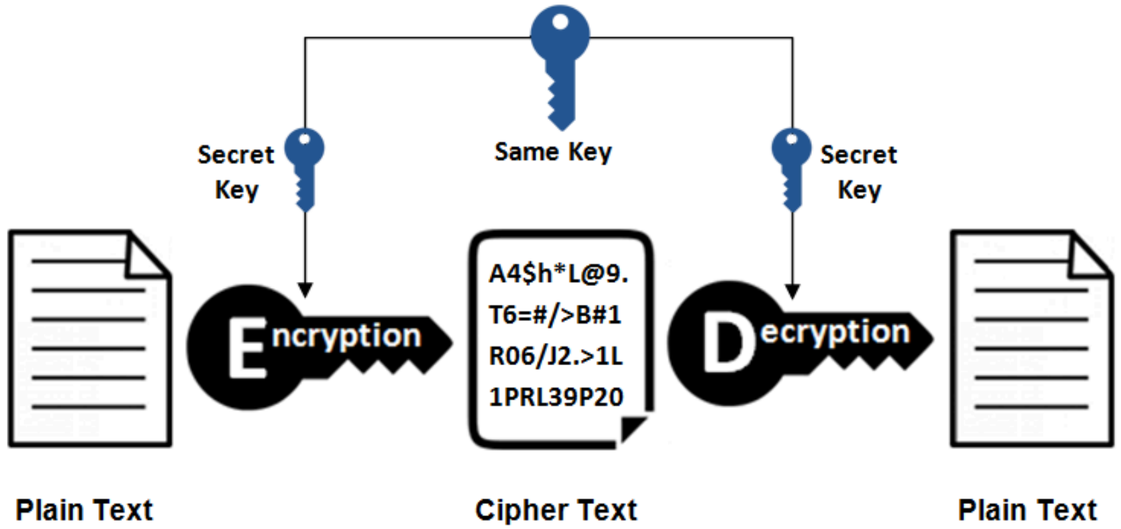
Somaiya TRUST

What is Cryptography?

- Cryptography secures communication by **transforming information** into an **unreadable** format for **unauthorized** users

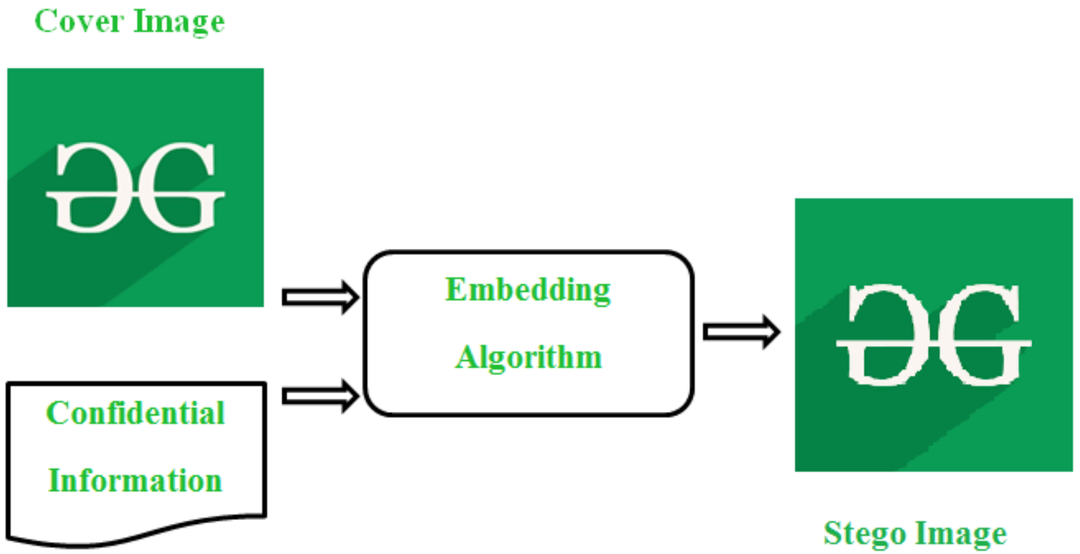
- **Plaintext** (original data) → **Ciphertext** (encrypted) using algorithms and keys
- Only authorized parties with the key can decrypt it back to plaintext
- Main goals: **Confidentiality**, **Integrity**, **Authentication** & **Non-repudiation**

Cryptographic algorithms can be **Symmetric** (like AES, DES) & **Asymmetric** (like RSA, ECC)



What is Steganography?

- Steganography is the **art of hiding secret information** within a **cover medium** (such as image, audio, video, or text) in a way that conceals the very existence of the information.
- For example, an image can look **visually unchanged**, but it can contain a hidden message embedded within its pixel values.
- The original image is called the **cover image**.
- After embedding, the image containing secret data is called the **stego image**.



Unlike cryptography, which makes **data unreadable but visible**, steganography makes **data invisible but not necessarily unreadable**.

Security Challenge – Why Combine Both?

Each method alone has weaknesses:

- **Cryptography alone:** The message is encrypted, so attackers cannot read it. However, the presence of a secret message is obvious. If attackers obtain the ciphertext, they may attempt brute force or cryptanalysis.
- **Steganography alone:** The message is hidden inside an image or file, so its existence is concealed. But if an attacker suspects and successfully extracts it, the secret message can be read in plaintext.

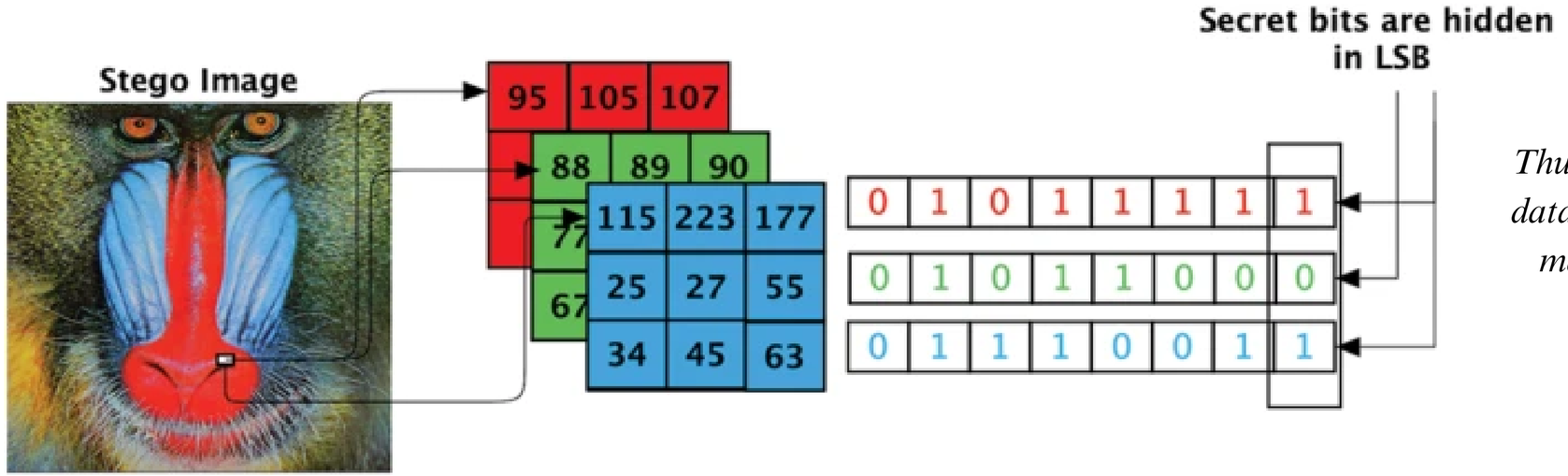
Hybrid Approach

Uses Crypto + Stego to encrypt the message (unreadable), then hide it in an image (invisible) providing dual-layer protection where detection still requires breaking encryption

How Image Steganography Works

(LSB Technique)

- Digital image is represented as a **matrix of pixels**. Each pixel has values for colors like RGB. Each color channel is stored as an **8-bit binary number**.
- The **Least Significant Bit (LSB)** technique works by modifying the **last bit of a pixel's binary value**.
- Changing an LSB does not significantly affect the pixel's color, so human eyes cannot detect it.



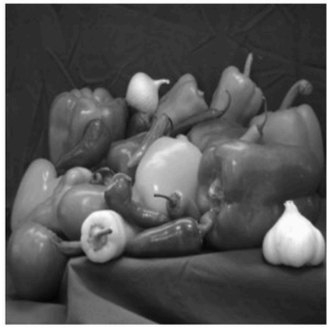
Thus, large amounts of secret data can be distributed across many pixels with minimal visual change

How Image Steganography Works

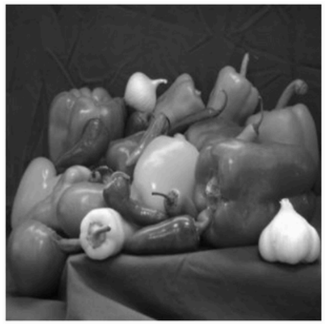
(LSB Technique)

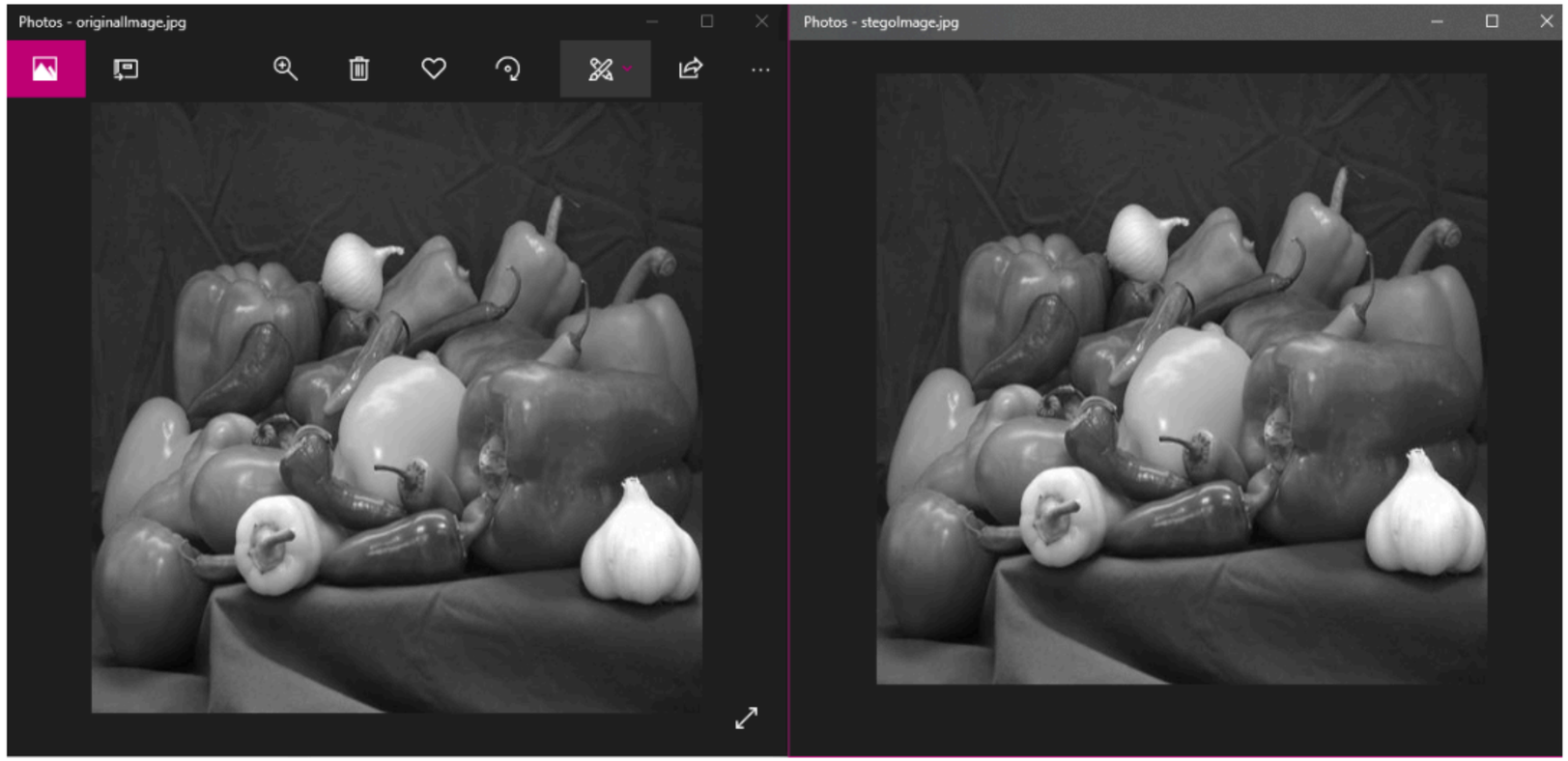
Example:

Input : message='geeksforgeeks'



Output : Image with the given message embedded:

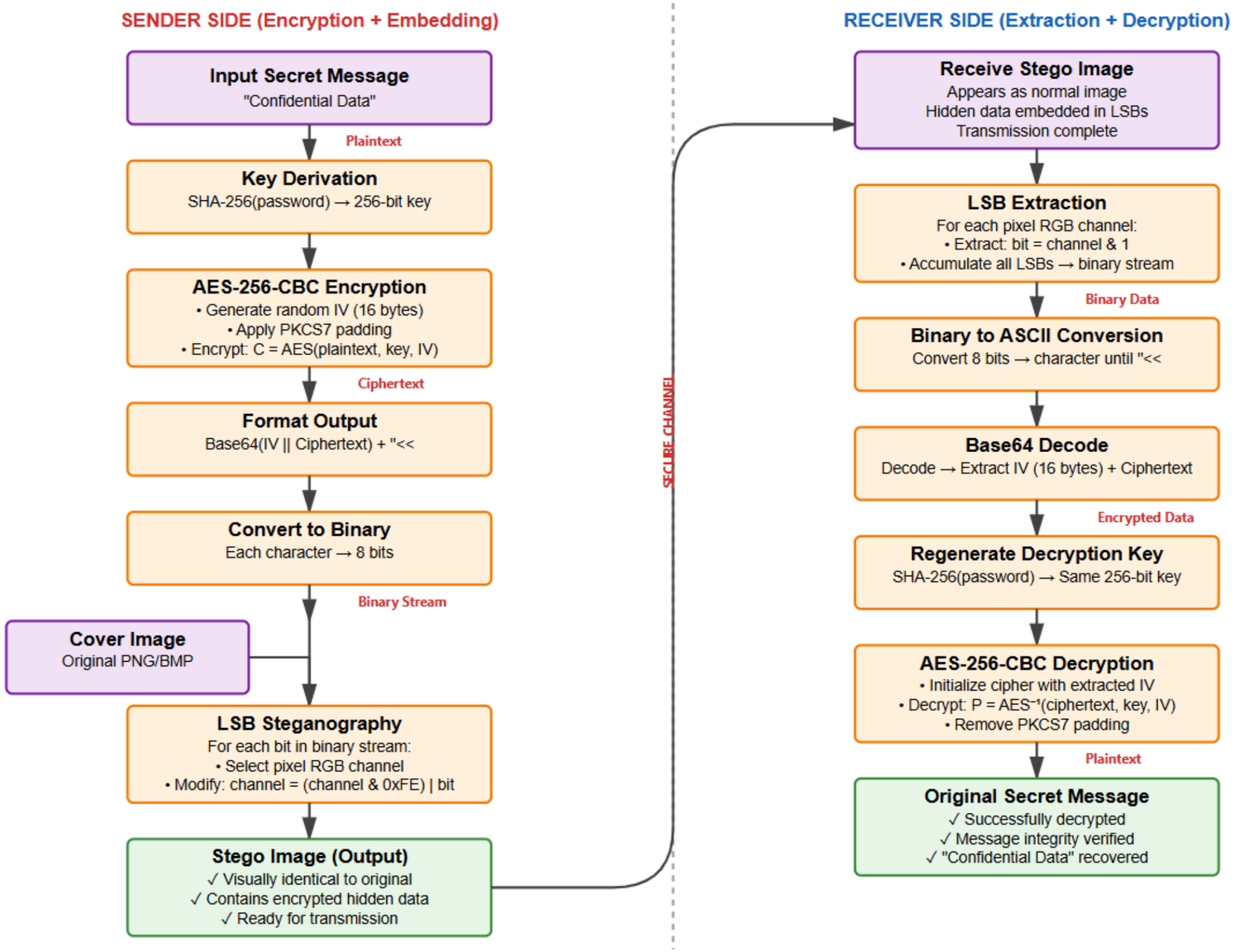




ORIGINAL IMAGE

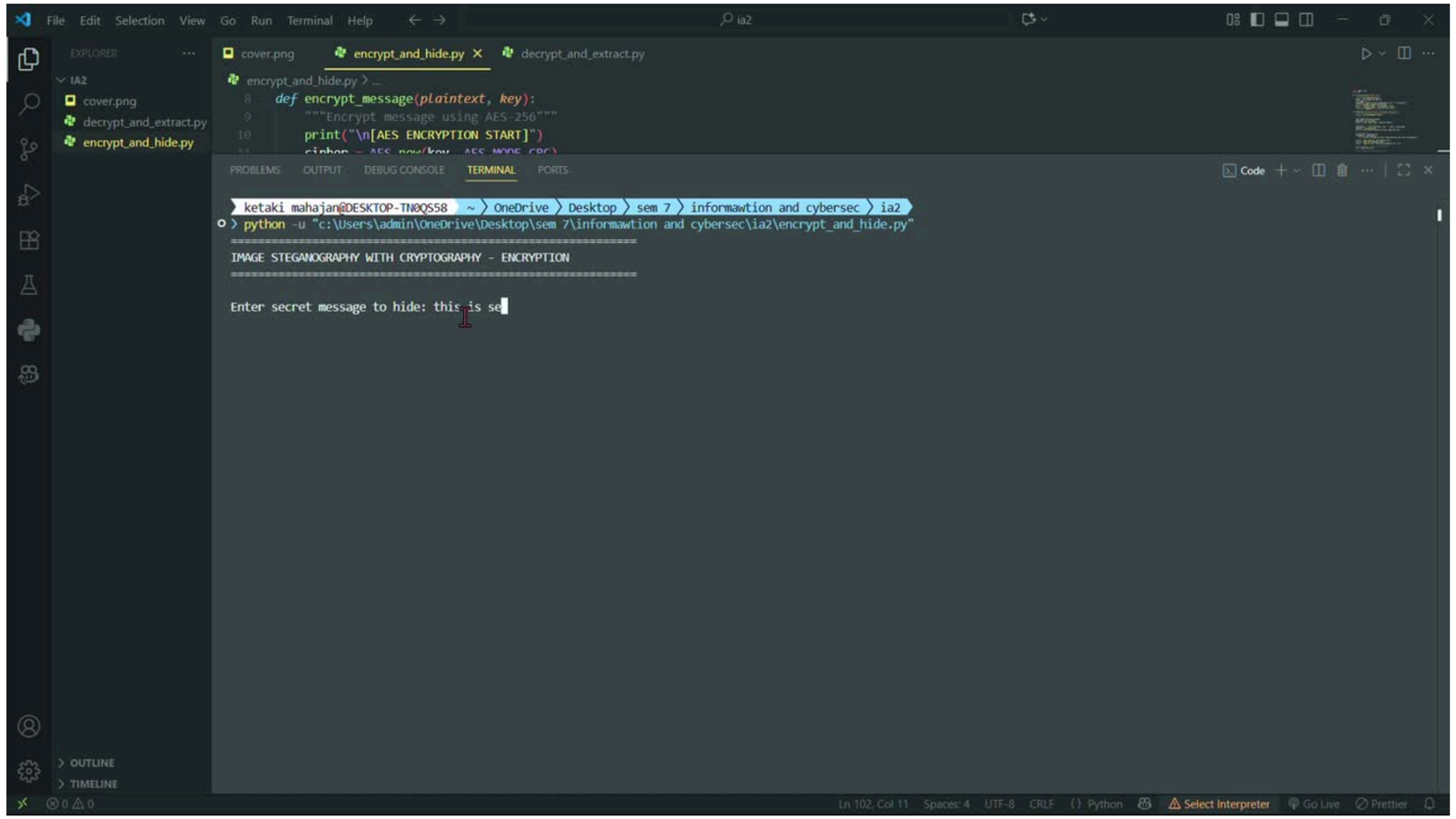
STEGO IMAGE

Algorithm Flow



This process ensures that the message is both **concealed** and **protected**.

Implementation & Demo



https://drive.google.com/file/d/1x6oxWLf2VEbtA7IXijCG5N2rdJaJQGAt/view?usp=sharing

Performance Metrics

To evaluate the system, some metrics are used:

- **PSNR (Peak Signal-to-Noise Ratio):** Measures image quality after embedding. Higher PSNR = less distortion.
- **MSE (Mean Square Error):** Measures pixel difference between cover and stego images. Lower MSE = better quality.
- **Embedding Capacity:** Maximum size of data that can be hidden without noticeable changes.
- **Robustness:** Resistance to attacks like compression, cropping, or noise addition.
- **Security:** Strength of cryptography used (AES, RSA) and resistance to steganalysis.

Advantages & Limitations

ADVANTAGES

- **Dual-layer protection**: encrypted + hidden.
- Stego image looks **visually identical** to cover image.
- Useful for **covert communication** and **secure file transmission**.

LIMITATIONS

- Embedding **capacity is limited** by image size.
- **Susceptible** to **image compression** or **format conversion** (lossy formats can destroy hidden data).
- **Computationally heavier** compared to using only one technique.
- If steganography is detected, attackers may still attempt cryptanalysis.

Applications & Future Scope

APPLICATIONS

- **Medical field:** Hide and protect patient records/scans.
- **Defense & Military:** Secret communication without detection.
- **Cloud storage:** Secure transmission of confidential files.
- **Digital watermarking:** Protect intellectual property.

FUTURE SCOPE

- **Combine** with **deep learning** to improve adaptive embedding and resistance to steganalysis.
- Use **robust techniques** (DCT, DWT) for **higher resilience** against **compression**.
- Implement **lightweight cryptography (ECC)** for faster performance on mobile/IoT devices.

Conclusion

- Cryptography ensures **message secrecy**; Steganography ensures **message invisibility**.
- Combining both yields a **robust hybrid security model** for modern communication.
- Provides strong protection against eavesdropping, detection, and cryptanalysis.
- Essential in fields requiring high confidentiality such as healthcare, defense, and secure internet communication.

Image Steganography in Cryptography

Your All-in-One Learning Portal: GeeksforGeeks is a comprehensive educational platform that empowe...

GeeksforGeeks / Aug 22, 2023

(PDF) Comprehensive Review of Cryptography and Steganograph...

PDF | On Jan 10, 2025, Halima Abbas Assied Ahmed Essilini and others published Comprehensive Review of...

researchgate.net

Thank You!