**COIMBATORE INSTITUTE OF TECHNOLOGY**

**(GOVERNMENT AIDED AUTONOMOUS INSTITUTION)**

**COIMBATORE , TAMILNADU**



**DEPARTMENT OF COMPUTING**

**(DECISION AND COMPUTING SCIENCES)**

**SUBJECT CODE: 22MDCEL61**

**GOLANG LAB**

**REGISTER NUMBERS: 71762233013**

**71762233018**

**71762233024**

**Problem Description:**  
In the digital age, the protection of visual data from unauthorized access is crucial, especially when it involves sensitive or personal content. With the rise in cyber threats and data breaches, securing image files through cryptographic methods has become essential. Existing solutions often lack user-friendliness or are dependent on proprietary software.

The Image Encryption/Decryption App addresses this challenge by offering a secure, efficient, and user-friendly approach to encrypt and decrypt image files. This application is built using the Go programming language, taking advantage of its efficiency and strong support for concurrency and cryptography. The core of the app employs the Advanced Encryption Standard (AES) with CFB (Cipher Feedback) mode, ensuring that image data is securely transformed into an unreadable format that can only be accessed with a valid decryption key.

The solution supports uploading image files, applying encryption with a user-provided key, and saving/downloading the encrypted output. Likewise, users can decrypt previously encrypted images by supplying the correct decryption key, ensuring that only authorized users can access the original image. The system is ideal for professionals, such as photographers or doctors, and can be further extended for broader use cases.

**Functional Requirements:**  
1. Image Encryption using AES  
- Accepts user-uploaded image files.  
- Converts image into byte stream and encrypts using AES in CFB mode.  
- Saves the encrypted file securely.

2. Image Decryption using AES  
- Reads encrypted image file and decrypts it using provided key.  
- Restores and displays/downloads the original image.

3. Frontend Interface (Optional)  
- HTML5/CSS3/JavaScript-based GUI for uploading and downloading files.  
- Interface for key entry and operation selection.

4. Backend Implementation (Go Language)  
- Uses Go standard libraries like crypto/aes, crypto/cipher, image/jpeg, image/png, os, and io.  
- Optional base64 encoding for transport compatibility.

5. Secure Key Handling  
- Utilizes strong 128-bit or 256-bit AES keys.  
- Users can enter keys directly or derive them from passwords.

6. Platform Support  
- Runs on any system supporting Go (Windows, macOS, Linux).

**Additional Features:**  
- Batch Image Processing: Ability to encrypt/decrypt multiple images simultaneously.  
- Cloud Upload/Download Support: Integration with Google Drive, AWS S3, etc. (optional).  
- Key Management Enhancements: Future support for key stores or hardware security modules (HSM).  
- REST API (Optional): To expose encryption/decryption functionality via HTTP.

**Use Case Scenario:**  
A professional photographer needs to share confidential wedding photos with clients. Using this app, they encrypt the images and share the files securely. The client, using the valid decryption key, decrypts and accesses the images, ensuring full data confidentiality even over public networks.

**Conclusion:**  
The Image Encryption/Decryption App is a practical and secure solution for handling sensitive image data. By leveraging the AES encryption standard and the power of the Go language, the application ensures data privacy and integrity. Its modular design allows for future scalability and the integration of enhanced security and usability features. This project is highly relevant for modern digital ecosystems where privacy and data protection are non-negotiable.