Beyond Syllabus

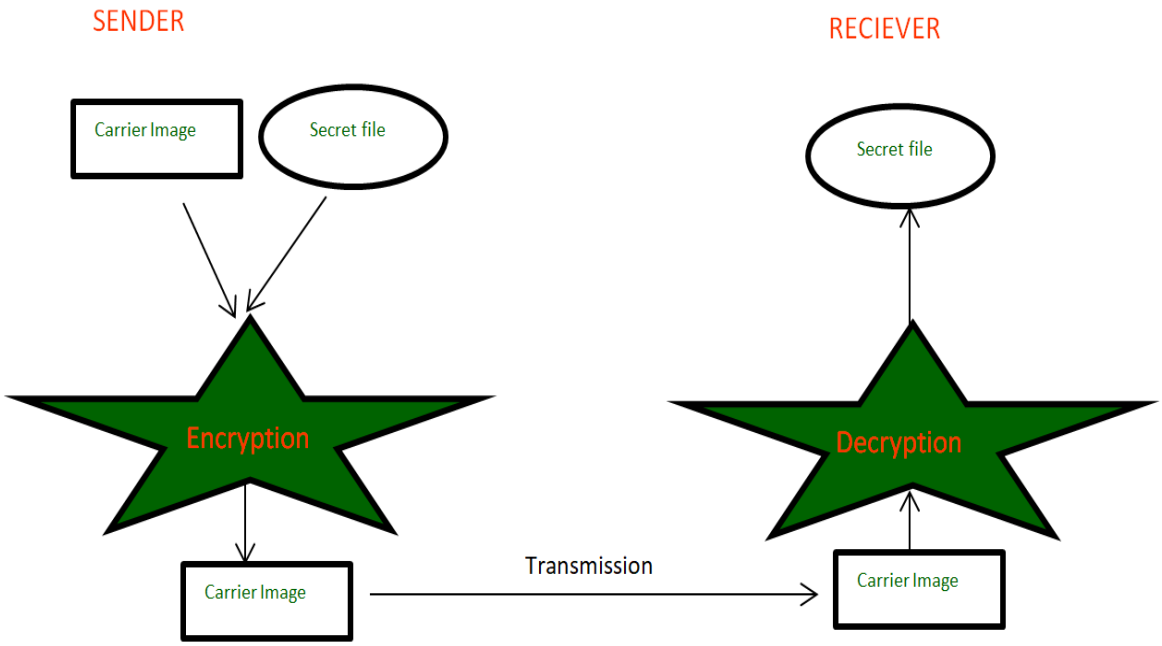
Study of Visual Cryptography

1. Introduction

The Internet is the fastest growing communication medium and essential part of the infrastructure, nowadays. To cope with the growth of internet it has become a constant struggle to keep the secrecy of information and when profits are involved, protect the copyright of data. To provide secrecy and copyright of data, many of the steganographic techniques have been developed. But each of the technique has their respective pros and cons. Where one technique lacks in payload capacity, the other lacks in robustness. So, the main emphasis of cryptography is to overcome these shortcomings.

2. What is visual cryptography?

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption can be done just by sight reading. Visual cryptography, degree associated rising cryptography technology, uses the characteristics of human vision to rewrite encrypted photos. Visual cryptography provides secured digital transmission that is used just for merely the once.



Numerous guidance like military maps and business identifications are transmitted over the internet. Whereas pattern secret photos, security problems ought to be compelled to be taken into thought as a result of hackers may utilize weak link over the communication network to steal info that they need.To touch upon the protection problems with secret photos, varied image secret sharing schemes are developed. anyone will use it for coding with none science information and any computations.

3. Proposed Methodology:

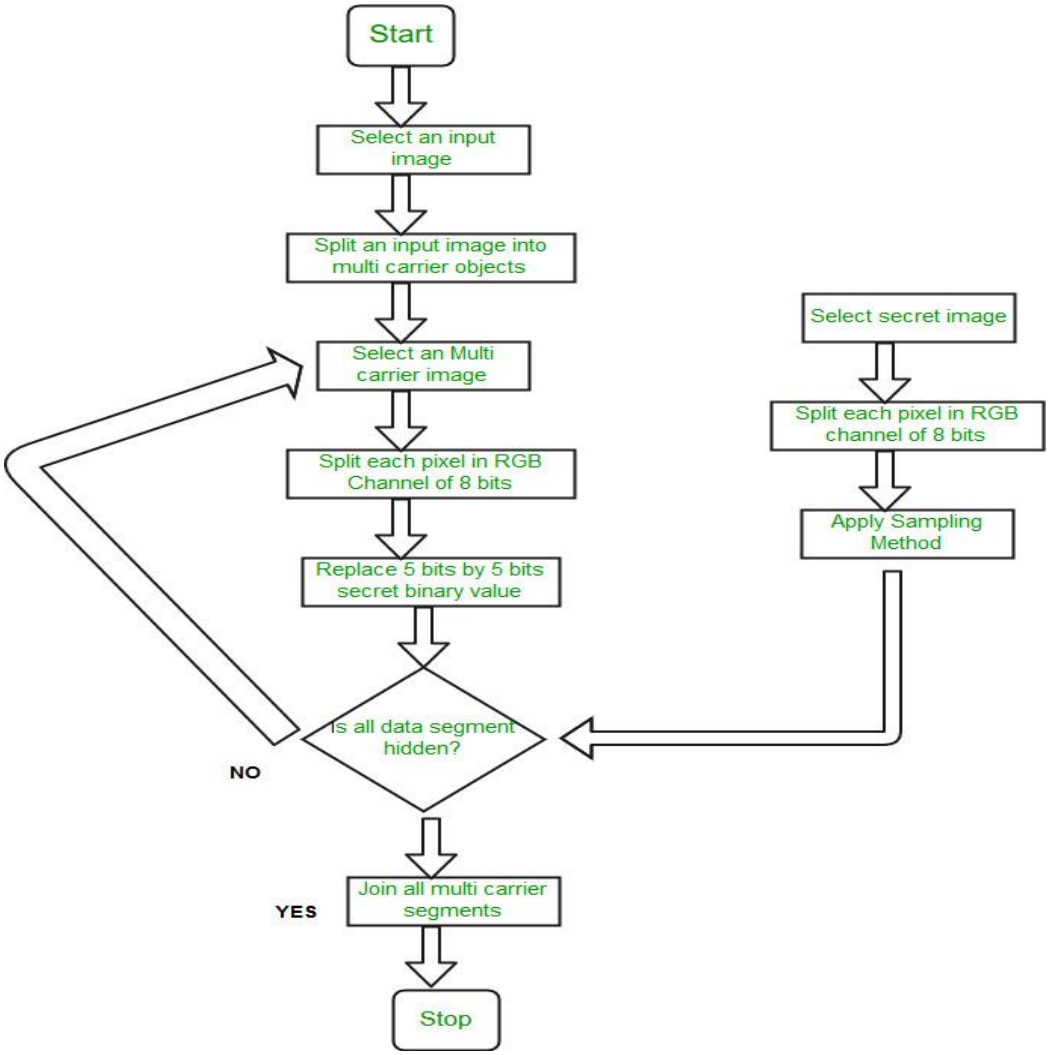
The proposed work is basically a framework design with two modules:

I. Data Hiding using multiple bits replacement scheme.

II. Visual Cryptography using Multi-layer Multi-shares method. An input image is accepted as a cover image for the secret image to be hidden.

I. Data Hiding

Algorithm: Data Hiding
Algorithm Input: Any image.
Output: Other Image Hidden by Input Image.



- **Step 1:** An input carrier image will be selected.
- **Step 2:** An input image gets split into 4 multi carrier objects. One multi carrier image object is selected from all 4 image objects.
- **Step 3:** The Secret image to be hidden get splits into RGB Channels each of 8 bits. Split each pixel in RGB channels of 8 bits each and separate each of 3 colors 8-bit component into 3 bits and 5 bits.
- **Step 4:** As Image comprises of pixel contribution from red, green and blue components, each pixel has numbers from the color components (for 24-bit bitmap image each of red, green and blue pixel has 8

bit).Split each pixel in RGB channel of 8 bits each and separate each of 3 color 8 bit component into 3 bits and 5 bits and then replace 5 bit of color component by 5-bit binary secret value.

- **Step 5:** Our visual system cannot detect changes in pixel and thus it is possible to replace Secret image bits with image pixel bit. Lastly, it will check that whether all data objects are hidden. And all the above steps are repeated for other remaining carrier objects. Finally, by joining all multi-carrier image objects, we get a hidden image.

II. Visual Cryptography

• Proposed Image Encryption Method

Algorithm: Image Encryption.
Input: Hided Image.
Output: Encrypted Image.

- **Step 1:** An input image will be selected. It must be an RGB image.
- **Step 2:**Red, Green and blue Channels are separated from an input Image.
- **Step 3:** Each Channel is then further encrypted into 8 shares. This encryption will depend on key used.
- **Step 4:** From Step 3, we get 24 shares, it means each channel has 8 shares each. These 8 shares of an each channel then further compress to 3 shares. Thus we get an o/p of 9 shares at step 4.
- **Step 5:** Compress 3 Shares from step 4 to one final encrypted image.

• Proposed Image Decryption Method

Algorithm: Image Decryption.
Input: Final Encrypted Image.
Output: Decrypted Image.

- **Step 1:** Select an Encrypted Image. It must be RGB Image.
- **Step 2:** Separate Red, Green and Blue Channels from an Encrypted image.
- **Step 3:** Create 3 Shares from each channel. So at step 3, 9 Encrypted images will be the output.
- **Step 4:** Create 8 Channels from Each channel.
- **Step 5:** From 8 shares each of step 4, Create 3 Shares (i.e red, green and Blue each).
- **Step 6:** Compress Step 5 Images to Plain Image (Decrypted Image).

4. Applications:

There are many applications of Visual Cryptography some of them are following:

1. Secret Communication
2. Copyright Protection
3. Document Authentication
4. Secret data storing