SECURE IMAGE TRANSMISSION USING STEGANOGRAPHY

INTRODUCTION

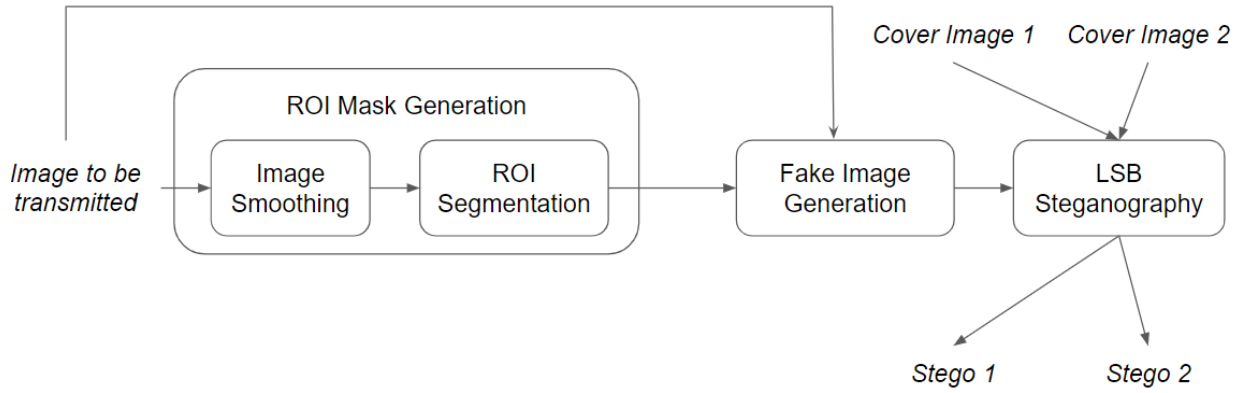
Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection. The secret data is then extracted at its destination. The difference between Cryptography and Steganography is that the presence of cryptography reveals that something is hidden but steganography doesn't attract any attention/ suspicion to the secret data as it is totally hidden behind another and is invisible to any observer. **The key behind steganography is to deceive an attacker by hiding sensitive data behind a typical or non-sensitive image.** In addition to using steganography for secure transmission, we could also fake an image at the sender side, hide it using steganography and unfake it at the receiver side so that, in the worst case, when any attacker finds the hidden sensitive data, he/she gets the fake image. **The key concept behind steganography is used in the latter method too. We try to deceive the attacker by placing a fake image in place of the original image which sometimes might make the attacker believe that the fake one is the actual real one.**

OBJECTIVE

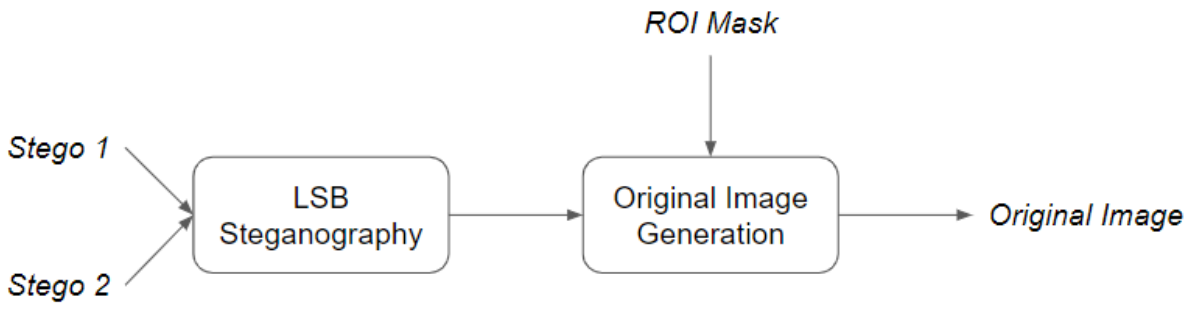
"To design and develop an algorithm for secure transmission of images using Steganography"

MODULE DIAGRAM

SENDER SIDE ALGORITHM



RECEIVER SIDE ALGORITHM



MODULE DESCRIPTION

I. SENDER SIDE ALGORITHM

ROI MASK GENERATION

INPUT: Color Image to be transmitted

OUTPUT: Region of Interest mask

The functionality of this module is to segment the region of interest from the input image using region based segmentation where objects are separated into different regions based on threshold values. Then, we generate a bi-color mask where one color represents the region containing ROI and another color represents the remaining region. Instead of directly applying segmentation on the input image, Image smoothening is carried out in order to remove unwanted noise which helps in producing enhanced segmented image and also the mask ultimately.

FAKE IMAGE GENERATION

INPUT: ROI Mask and Input Color image

OUTPUT: A fake color image

The functionality of this module is to generate a fake image from the original input image in such a way that the process is reversible. Here, instead of using a single function to alter all the pixels in the entire image, we use the ROI mask, apply one function on all pixels existing in the ROI region and apply another faking function on all pixels existing in the other region. The reason for the use of two faking functions is to make it difficult for the attacker to find the original image from the fake image. An attacker trying to reconstruct the original image from the fake image needs to have access to both the faking functions and ROI mask. The faking function used on the ROI pixels is

2 bit swap where the binary places 12345678 gets transformed to 78563412 and the faking function used on other pixels is 4 bit swap where the binary places 12345678 gets transformed to 56781234. The faking functions are applied to all the intensity levels of the R,G,B channels in each pixel of the region.

LSB STEGANOGRAPHY

INPUT: Fake color image, Color Cover Image 1 & 2

OUTPUT: Color Stego Image 1 and 2

The functionality of this module is to hide the input fake image behind two images using LSB steganography technique. The following two techniques are used to produce two cover images.

1. Among the 8 bits in each pixel of the image used as a cover, the 4 bits in the MSB are kept untouched and the other 4 bits in the LSB are replaced with 4 bits in the MSB of the corresponding pixel in the input fake image to be transmitted.
2. Among the 8 bits in each pixel of the image used as a cover, the 4 bits in the MSB are kept untouched and the other 4 bits in the LSB are replaced with 4 bits in the LSB of the corresponding pixel in the input fake image to be transmitted.

We use two different images as cover images and hide different parts of the input image in the two cover images. The two stego images and the encrypted ROI mask are transmitted to the receiver.

II. RECEIVER SIDE ALGORITHM

LSB STEGANOGRAPHY

INPUT: Color Stego Image 1 and 2

OUTPUT: Fake Color Image

The functionality of this module is to reconstruct the hidden fake image from the two stego images. The 4 LSB bits in each pixel of stego image 1 constitutes the 4 MSB bits of the corresponding pixels in the fake image and the 4 LSB bits in each pixel of stego image 2 constitutes the 4 LSB bits of the corresponding pixels in the fake image.

ORIGINAL IMAGE GENERATION

INPUT: Fake Color Image and ROI mask

OUTPUT: Original color Image

The functionality of this module is to reconstruct the original image from the fake image. In order to achieve this, the two regions (ROI and the other) are identified using the ROI mask and the inverse of the faking function is applied to the corresponding regions of the fake image. The inverse of the faking functions is the same as the faking functions. The inverse of the faking function used on the ROI pixels is 2 bit swap where the binary places 78563412 gets transformed to 12345678 and the inverse of faking function used on other pixels is 4 bit swap where the binary places 56781234 gets transformed to 12345678. The inverse faking functions are applied to all the intensity levels of the R,G,B channels in each pixel of the region to obtain the original color image.

CODE: