Image Encrypyion with Edge Detection

May Thu Wint, Yadana Thein
University of Computer Studies, Yangon
glassesmaythu26@gmail.com

Abstract

Steganography is the technique of hiding the communication data by hiding data in another different format of data.Even though many different carrier file formats can be used, digital images are the most commonly used format. For hiding encryption in images, there exist a large variety of steganography techniques; of which some are more complex than others and all of them have their respective strong and weak points. The proposed paper roughly explains and presents the concepts of the combination of cryptography and steganography techniques. This paper proposes 3 techniques for information hiding in RGB color images. (1)Canny Edge Detection for separating am image into edge (2)Least Significant Bit (LSB) technique for hiding encrypted messages in edge, there is no much changes in the embedded image (3) Advance Encryption Standard (AES) for encryption plain text to cipher message.

Keywords: *Image Processing,Steagnography and Cryptography,Canny Edge Detection, Least Significant Bit(LSB), Advance Encryption Standard(AES), Peak Signal to Noise Ratio(PSNR)*

1. Introduction

In the internet age we are living today, telecommunication has become an important part of our lives; in which security has always been a major issue where secure data communication is an essential factor. Our paper intends to present the combination of two techniques of Steganography and Cryptography to enhance better security protocols. Steganography is the art or practice of hiding information to prevent the detection of the encrypted message by hiding a message in appropriate formats such as an image or an audio or a video file. The formats can then sent to a receiver without anyone knowing that it contains a hidden message.

Edge detection, on the other hand is the process or operation of distinguishing the edge regions from the non-edge regions. It has several applications related in image processing and computer vision application. By producing a line drawing of an image, a portion of that scene can be taken. Then important features can be extracted from the edges of that scene (e.g., Coners, lines, curves). These features are used by higher-level computer vision algorithms such as recognition. There are many kinds of edge detection such as Canny Edge Detection, Sobel Edge Detection, Prewitt Edge Detection, Gradient Edge Detection, Isotropic Edge Detection, Robert's Cross Edge Detection, Laplacian of Gaussian Edge Detection. Among such detection techniques, we can use Canny Edge Detection. Cryptography is the art and science of achieving security by encoding messages to make them unreadable to the unauthorized personals; with the purpose of protection the user data.Cryptography involves two basic functions of encryption and decryption. Encryption is the process of transforming plain data into the cipher and decryption the vice versa. There are also many kinds of encryption methods; RSA, Data Encryption Standard (DES), etc. Among them, we will demonstrate how Advance Encryption Standard (AES) works.

2. Image Processing and Steganography

In imaging science, **image-processing** is any form of signal processing for which the input is an image, such as a photograph or video frame; the output of image processing may be either an image or a set of characteristics or parameters related to the image. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it. Image processing usually refers to digital image processing, but optical and analog image processing also are possible. This article is about general techniques that apply to all of them. The *acquisition* of images (producing the input image in the first place) is referred to as imaging.

Steganography, derived from Greek, literally means "covered writing". Steganography has grown explosively in terms of further exploring message hiding within an object, a text or even a picture.

Steganography is a technique to hide information from the observer to establish an invisible communication. Image Steganography requires two files. The first is the innocent-looking image that will hold the hidden information, called the cover image. The second file is the message i.e. the information to be hidden. A message may be plain-text, cipher-text, other images, or anything that can be embedded in a bit stream. When combined, the cover image and the embedded message make a stego-image. A stego-key (a type of password) may also be used to hide then later decode the message.

3. Difference between Steganography and Cryptography

In simple words steganography is hidden writing. The message is there, but nobody notices if. However, once noticed, it can be read. Cryptography is secret writing. Anybody can see the message, but nobody else can read it. Usually, this is because its litters have been re-arranged, of replaced by different letters, according to some scheme that only the sender and receiver know.

a) Cryptography Techniques:

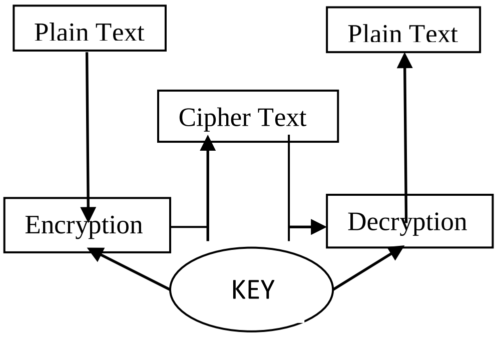


Figure 1.Basic cryptographic technique

b) Steganography Technique

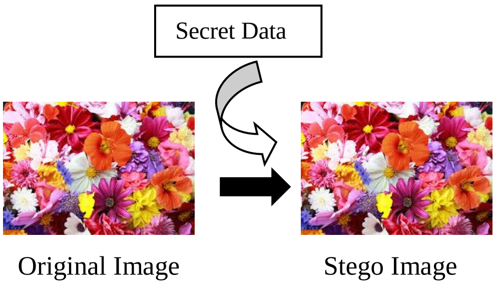


Figure 2. Basic steganographic technique

Cryptography is the art of transmitting original information (Plain Text) in to a jumbled form (Cipher Text). In Steganography, the data is embedded in a cover file and the cover file is transmitted. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to recipients. An unhidden coded message, no matter how unbreakable it is, will arouse suspicion and may in itself be incriminating, as in countries where encryption is illegal. Hence, combining the two techniques would give us a perfectly secure system. This paper aims at attaining this objective.

4. Proposed Method

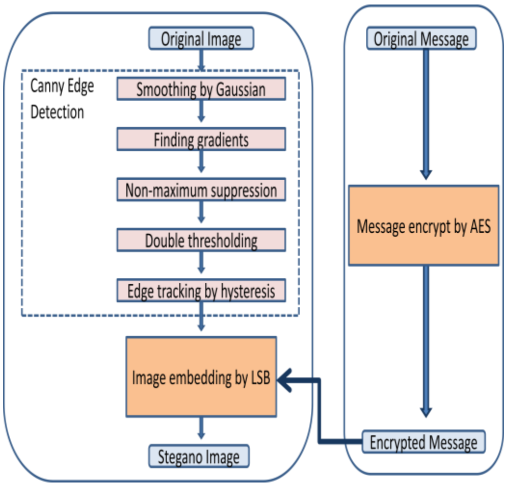


Figure 3. System architecture of image encryption

In order to achieve the desired goal, the whole project has been divided into levels as discussed below:

Level 1: Get a cover Image and locate the edges to embed the texts.

Level 2: Get the secret message and convert the secret message to cipher text.

Level 3: Embed the cipher text into the image as per the embedding process discussed.

Level 4: Finally, send the modified stego image to receiver.

Level 5: At the receiving end, a reverse process is followed in order to decrypt the hidden message.

4.1. Canny Edge Detection

The Canny Edge Detection is one of the most commonly used image processing. It runs 5 steps:

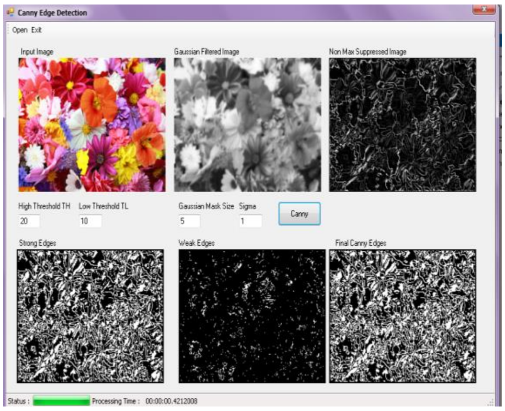
1. **Smoothing** : Bluring of the image to remove noise.

2.**Finding gradients** : The edges should be marked where the gradients of the image has large magnitudes.

3.**Non-maximum suppression** : Only local maxima should be marked as edges.

4.**Double thresholding**: Potential edges are determined by thresholding.

5.**Edge tracking by hysteresis**: Final edges are determined by suppressing all edges that are not connected to a very certain .



High Threshold TH 20 Low Threshold TL 10 Gaussian Mask Size 5 Sigma 1

Status : Processing Time : 00:00:00.4212008

Figure 4. Canny edge detection

4.2. Advance Encryption Standard(AES)

AES encryption of the textual input data takes place. Advanced Encryption Standard (AES) algorithm is symmetric cipher algorithm used in applications that require fast processing. AES algorithm supports data and key combinations of size 128, 192 and 256 bits. AES allow data of length 128 bits. 128 bits data is divided into fourblocks, in which each block perform different operations.The blocks are organised in 4x4 matrixes which is called states. The blocks operate on array of bytes. Encryption of data include four transformation steps and encryption is completed when it completes Nr rounds whereNr= 10, 12, 14. The four transformation steps are Bytesub, Shiftrows, Mixcolumns, and Addroundkey transformations as shown in figure [5].

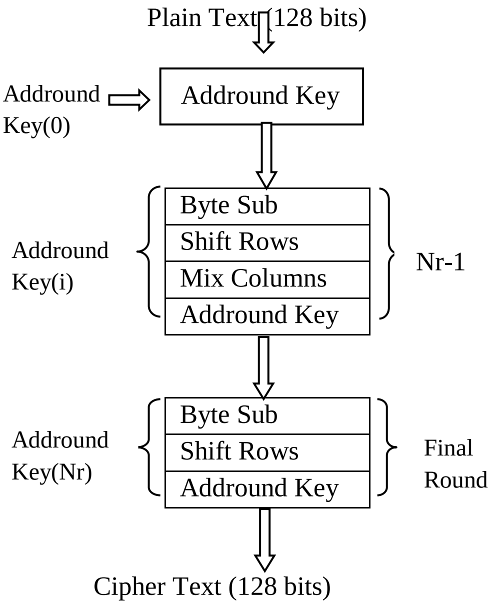
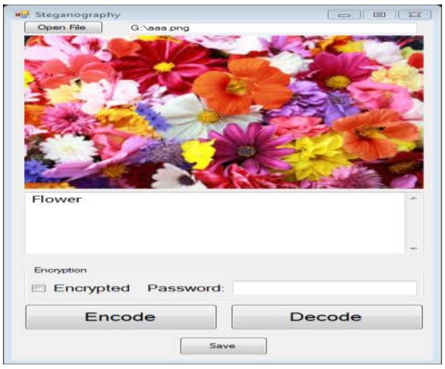


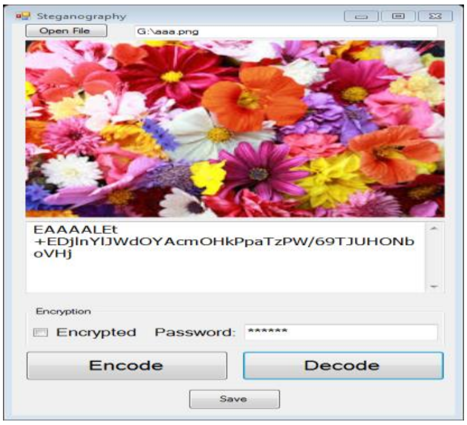
Figure 5.Advance encryption standard



Flower

□ Encrypted Password:

Figure 6. Original message



EAAAALEt
+EDjlnYlJWdOYAcmOHkPpaTzPW/69TJUHONb
oVHj

□ Encrypted Password: ******

Figure 7. Encrypted message

4.2. Least Significant Bit(LSB)

Least significant bit insertion is a common, simple approach to embed information in a cover file. The LSB is the lowest order bit in a binary value. This is an important concept in computer data storage and programming that applies to the order in which data are organized, stored or transmitted. Usually, three bits from each pixelcan be stored to hide an image in the LSBs of each byte of a 24-bit image. Consequently, LSB requires that only half of the bits in an image be changed when data can be hidden in least and second least significant bits and yet the resulting stegoimage which will be displayed is indistinguishable to the cover image to the human visual system.LSB Steganography in Color and Grayscale Images without using the transformation.

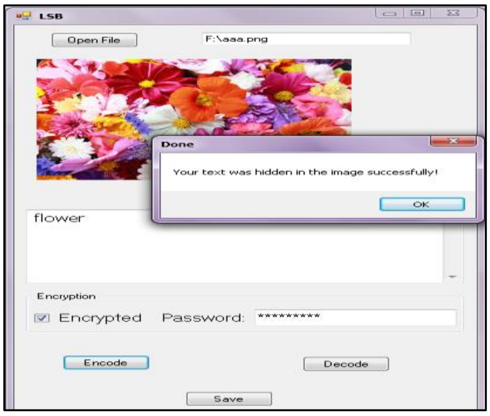
Most Significant Bit Least Significant Bit

1	0	1	1	1	0	1	1

LSB (Least Significant Bit) steganography can be described as follows: if the LSB of the pixel value I(i, j) is equal to the message bit m to be embedded, I(i, j) remain unchanged; if not, set the LSB of I(i, j) to m. The message embedding procedure can be described using an Equation as follows;

$$\text{Is }((i, j) = \begin{cases} I(i, j)-1 & \text{LSB }(I(i, j))=1 \text{ and } m = 0 \\ I(i, j) & \text{LSB }(I(i, j))= m \\ I(i, j)+1 & \text{LSB }(I(i, j))\neq 0 \text{ and } m = 1 \end{cases} \quad [1]$$

For example, if a pixel of the cover image with the RGB (Red-Green-Blue code) color is used, binary 10101000-10101000 10101000, and 1 bit with value 1 is set on each LSB bit of each color component, to hide the message 111, the result would be 10101001-10101001-10101001:



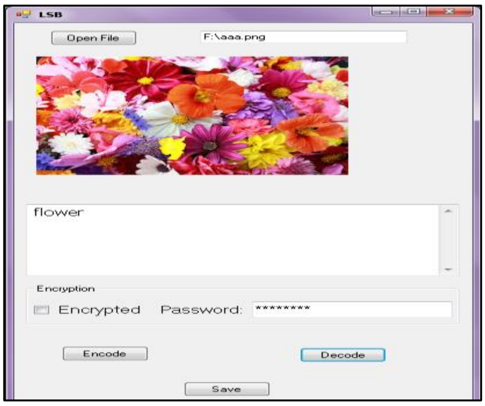
F:\aaa.png

Your text was hidden in the image successfully!

flower

☑ Encrypted Password: **********

Figure 8. Stego image



F:\aaa.png

flower

☐ Encrypted Password: *********

Figure 9. Original image

5. Experimental Results

The experimental results presented in this section describe the performance of our proposed technique. By comparing the output image i.e., embedded cover image with the our original image pixel values, we calculate the accuracy of the proposed method.

Mean Square Error (MSE): It is the measure used to quantify the difference between the initial and the distorted or noisy image. let Pi represents the pixel of one image of size N and Qi that of the other.

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \quad [2]$$

From MSE, we can find Peak Signal to Noise Ratio (PSNR) to access the quality of the Stego image with the respect to cover image given by

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \quad [3] \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \end{aligned}$$

Table 5.1. LSB embedding based results

Image	MSE	PSNR
POOH	57.224	71.113
FLOWER	89.587	67.891
GOOGLE	57.233	70.138
HAIR STYLE	55.195	89.925
FRUIT	88.254	65.243
DESERT	58.248	69.112

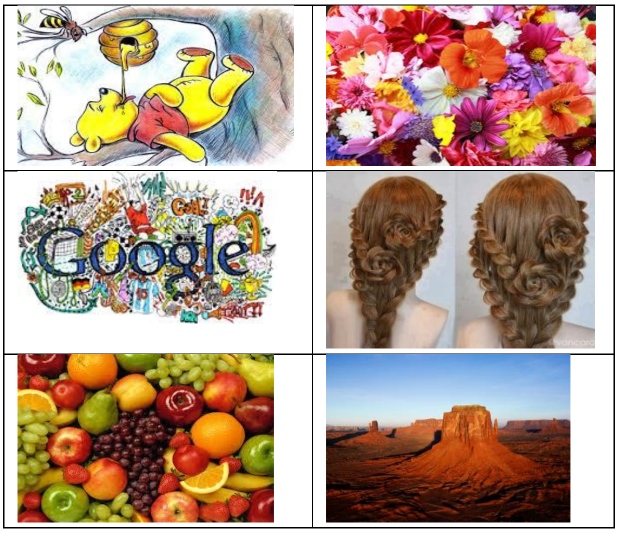


Figure 10. Original images

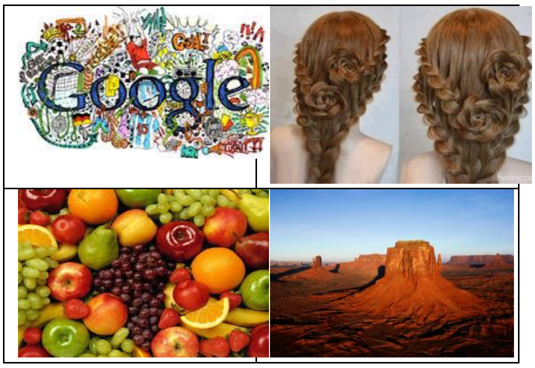


Figure 11. Stego images of proposed method

The maximum value of a pixel in grayscale image is 255. A higher PSRN indicates that the quality of the stego image is better and more similar to the cover. Table .shows the proposed method results. It has quite good embedding capacity. After overall comparison of all the result it is clear that LSB Embedding is simple technique. It gives highest stego image clarity with highest PSNR and lowest MSE value expect in case of " Flower " and " Hair Stylessss " images as given in Table . So, the objects of this paper (clarity, authentication and security) for different kind of images is fulfilled.

6. Conclusion

Data security is a critical issue for efficient data communication. Steganography and Cryptography are two major factors of data security. In this proposed system, cryptographic and steganographic securities are combined in order to give birth to two-tiered security system for the protection of classified data. In proposed scheme, the classified data is encrypted before hiding it into the cover image, giving high level of security to the data. Anny edge detection is used to show the edges of the image. While embedding, we insert texts at B of RGB color range. As a result, the image color has become brighter. And then Advanced Encryption Standard (AES) is used to encrypt secret message and Least Significant Bit (LSB) substitution method is used to hide encrypted secret message into the cover image. Proposed approach intends to be of more significant promotion for adaptability, capacity and imperceptivity. Finally, we strongly believe that the proposed technique is effective and efficient for secure data communications.

References

[1] R.Paseband, P.Pillewar, S.Bangale, A.Nimkar,S.Hadke, R.Joshi, A.M.Borkar, "Text Hiding Technique of Image Stegano-Cryptography using Edgedetetion"

[2] Mamta Juneja* and Parvinder Singh Sandhu**, "A New Approach for Information Security using an Improved Steganography Technique"

[3] Ping ZHOU,Wenjun YE, Yaojie XIA, Qi WANG, "An Improved Canny Algorithm for Edge Detection", Journal of Computational Information Systems 7:5 (2011) 1516-1523 at http://www.Jofcis.com

[4] Ali A.Yassin ,Iraq-Basrah, "Partial Encryption Of Color Image By Edge Detection"

[5] G. Viji and J. Balamurugan, LSB Steganography in Color and Grayscale Images without using the Transformation, Bonfring International Journal of Advances in Image Processing, Vol. 1, Special Issue, December 2011

[6] K.Zotos, A.Litke, "Cryptography and Encryption"

[7]Ajit Singh and Upasana Jauhari, "A Symmetric Steganography with Secret Sharing and PSNR Analysis for Image Steganography", International Journal of Scientific & Engineering Research Volume 3, Issue 6, June-2012 1ISSN 2229-5518

[8] Nitin Jain, Sachin Meshram, Shikha Dubey, "Image Steganography Using LSB and Edge –Detection Technique"

[9] Hemendra Singh Yadav, Prof. Niresh Sharma M.Tech. Scholar RKDF, Bhopal, India,Prof. CSE Dept, RKDF, Bhopal, India "An Enhanced Steganography Technique for Hiding Text and Image Type Secret Messages" Volume 4, Issue 7, July 2014 ISSN: 2277 128XInternational Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com