RESEARCH ARTICLE OPEN ACCESS

Modified Approach for Hiding Secret Data and Improving Data Embedding Capacity

Swati Patil, Komal More
Department of Computer Engineering Dr. D.Y Patil College of Engineering, Ambi, Pune, India.
Department of Computer Engineering Dr. D.Y Patil College of Engineering, Ambi, Pune, India

Abstract
Security of the secret information has been a challenge when the large amount of data is exchanged on the internet. A secure transfer of information can be very much achieved by steganography and Cryptography. Steganography is a tool for hiding information inside an image. Cryptography is a tool which provides encryption techniques for secure communication. In the traditional steganograhy techniques principle was either to replace a special part of the frequency components of the carrier image, or to replace all the least significant bits of a multi-valued image with the secret information. Our new steganography uses an image as the carrier data, and we embed secret information in the bit-planes of the carrier. This technique makes use of the characteristics of the human vision system whereby a human cannot perceive any shape information in a very complicated binary pattern. We can replace all of the ―noise-like‖ regions in the bit-planes of the carrier image with secret data without deteriorating the image quality.
Keywords- Bit Plane, BPCS, Hybrid Cryptography, LSB, Modified BPCS, Steganography.

I. Introduction

Information security is a major issue of concern while exchanging a data in an open network, as internet is not only a single network it is worldwide collection of loosely network. Anyone can hack the information and then make misuse from that or corrupt it or we can say that anyone can destroy the information if it is not fully secured or protected. Steganography and Cryptography both plays a very important role in information security.

Steganography is information security tool which stores the secret information in any media file in such way that no one else except the sender of the information and the intended receiver can only suspect the existence of any sort of information. Cryptography is also an information security tool which provides encryption techniques to hide the secret information.

A good information hiding technique shall include the following requirements:

1) Imperceptibility: the difference between the stego medium and the original one must be very slight such that the illegal party cannot detect the embedded information.
2) Security: the illegal party cannot extract out the hidden information even if he has detected that there are some information concealed in the stego medium.
3) Capacity: the total number of secret message which can be embedded in the medium.
4) Robustness: the stego medium shall be able to resist general image processing.

The merits of BPCS-Steganography found by the experiments are as follows.

1) The information hiding capacity of a true color image is around 50%.
2) A sharpening operation on the dummy image increases the embedding capacity quite a bit.
3) Customization of a BPCS - Steganography program for each user is easy.
4) It is most secured technique and provides high security.
5) Randomization of the secret data by a compression operation makes the embedded data more intangible.

1.1 Problem Statement

Focus in this paper is towards information or data security when communication takes place.

1) Prevent form hacking.
2) To provide the better data security.
3) Improve data embedding capacity and maintain quality.

In this paper we are putting forward different algorithms for explaining encoding and decoding.

The structure of this paper is as follows:

Section I consist of introduction with problem statement of the paper Section II presents the related work Section III includes the Existing system Section IV consist of the proposed system Section V represent the example with experimental analysis and Section VI consist of conclusion.

II. Related Work

Abbreviations

DES Data Encryption Standard.

RSA Rivest Shamir Adleman

LSB Least Significant Bit

BPCS Bit Plane Complexity Segmentation

2.1 Objectives

Focus in this paper is towards information and data security during internet communication.

1) To provide the better data security.

2) Prevent form hacking.

3) Improve data embedding capacity and maintain quality

2.2 LSB

Simple method in which the least significant bits of the bytes in an image is replaced by bits of secret message.

A large amount of data can be embedded by LSB without observable changes. Very effective, easy to implement, takes very less space but it has low imperceptibility.

2.3 BPCS

In this segmentation of image are used by measuring its complexity. It replaces the noisy blocks of bit plan with the binary patterns mapped from a secret data. Noisy blocks are determined with help of complexity. It has Very large embedding capacity.

2.4 Modified BPCS

It uses an image as the vessel data, and we embed secret information in the bit-planes of the vessel. This technique makes use of the characteristics of the human vision system whereby a human cannot perceive any shape information in a very complicated binary pattern. We can replace all of the "noise-like" regions in the bit-planes of the vessel image with secret data without deteriorating the image quality. Input data will be vessel image and data to embed in byte format. Load the vessel image into memory. Get width and height of the memory image. Generate a threshold value.

III. Existing System

Information send through any network have a chance to attack by hackers. After data embedding, the quality of image may be affected.

Encryption provides an obvious approach to information security, and encryption programs are readily available. However, encryption clearly marks a message as containing "secret" information, and the encrypted message becomes subject to attack. Furthermore, in many cases it is desirable to send information without anyone even noticing that information has been sent secret information.

IV. Proposed System

In steganography, data is hidden inside a vessel or container that looks like it contains only something else. A variety of vessels are possible, such as digital images, sound clips, and even executable files.

All of the traditional steganographic techniques have limited information-hiding capacity. They can hide only 10% (or less) of the data amounts of the vessel.

This Technique uses an image as the vessel data, and we embed secret information in the bit-planes of the vessel. We can replace all of the "noise-like" regions in the bit-planes of the vessel image with secret data without deteriorating the image quality.

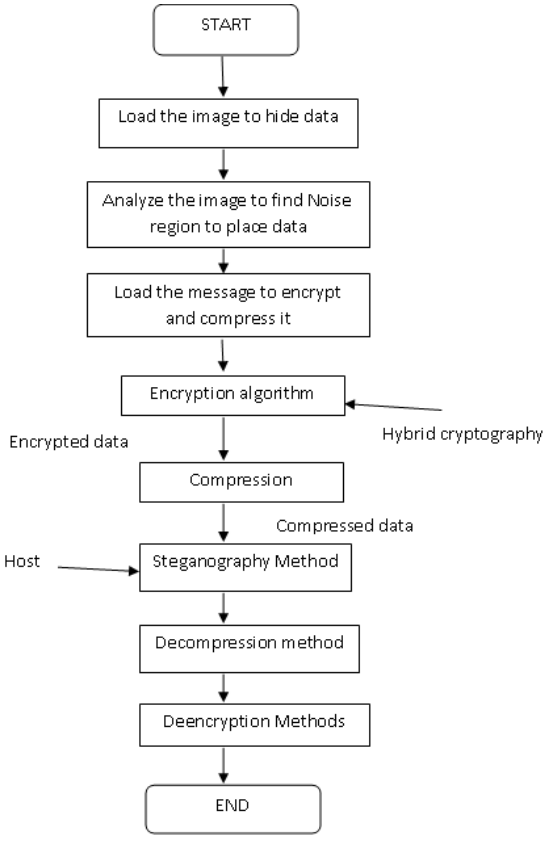

Fig. Flow of proposed system

4.1 Encoding

The encoding process follows the steps listed below:

Step 1: Calculate the size of the secret data and cover-image.

Step 2: Determine the total bytes from the RGB pixels needed in cover-image to encode the secret data.

bits per pixel=bits per byte x 3 (1)

number of pixel of cover=(cover lengh*8)/bit per pixel (2)
number of pixel of data=(cover lengh*8)/bit per pixel (3)
Step 3: The system reads the bytes of the secret data. Convert the amount of bits of the secret data in
(3) from integer into binary string.
Step 4: Segment the pixel into three blocks which are red, green and blue.
Step 5: Get the total LSB or LSBs needed for encoding.
Step 6: Calculate the arrays from the first seven pixels (from the 0th pixel to the 6thpixel) of the bitmap cover-image to store the secret data details as depicted in Table 3. The number of k pixels will be used to store the file name of the secret data.

$$k=n-7 \quad (4)$$

Denote:
k: Capacity of the file name used in term of pixels.
n: The kth pixel after the 6th pixel. The remaining pixels of the cover-image will be used to store the contents of the secret data.
Step 7: Calculate the number of LSB or LSBs in the colour pixels of the cover-image that are being used to encode data

$$x=8-m \quad (5)$$

$$\text{Total encoded LSBs}=(s1-x1)+(s2-x2)+(s3-x3) \quad (6)$$

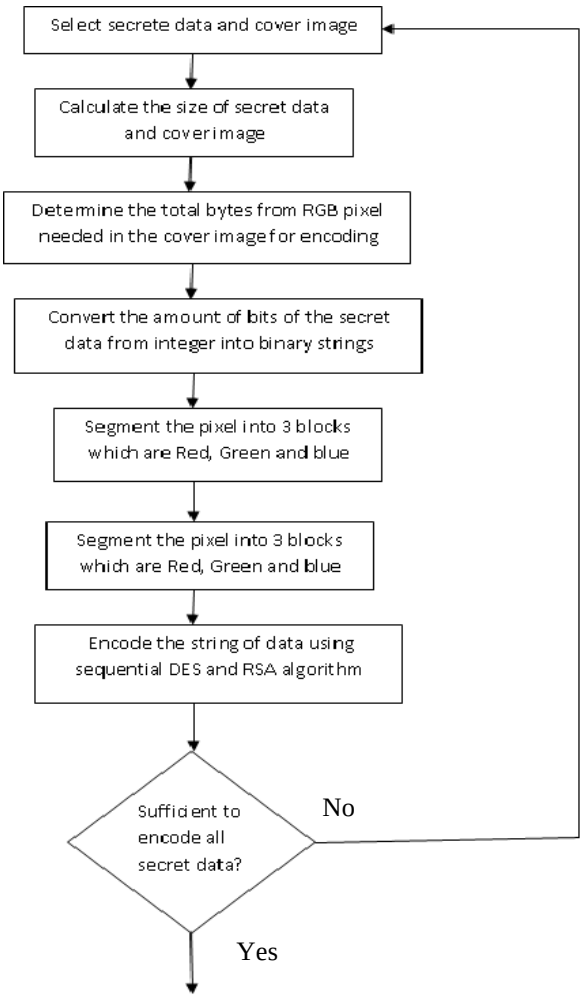

Fig. Encoding process

The following computation obtains the total encoded LSBs and the value of a new pixel with encoded data:

Total encoded LSBs=(s1- x1)+(s2- x2)+(s3- x3)

New pixel value with encoded data=original byte + total encoded LSBs.

4.2 Decoding

After encoding secret data into the cover-image, the secret data has to be decoded for retrieval.

The following are steps for decoding:
Step 1: Calculate the size of the stego-image.
Step 2: The system reads the bytes of the stego-image.
Convert the amount of bits of the stego-image
from integer to binary string.
Step 3: Determine encoding method for the number of LSBs to be used
Step 4: Calculate and identify the number of pixels

in the stego-image and also the embedded secret data respectively using 1, 2 and 3.

Step 5: Use the last three byte values 216, 224 and 232 to obtain the offset of the string. Each of the values mentioned will deduct the LSB used in order to discard unused bits for secret data embedding.

first offset=16-encoded LSB (7)

second offset=24-encoded LSB (8)

third offset=32-encoded LSB (9)

Step 6: Extract and combine the remaining LSB at each pixel in the BMP-24 file in order to retrieve back the original secret data.

decoded string= (7)+(8)+(9)

(10)

From 10, the decoded string is the secret data retrieved.

Figure 8 shows the decoding process of the proposed scheme when a receiver decodes a stego-image.

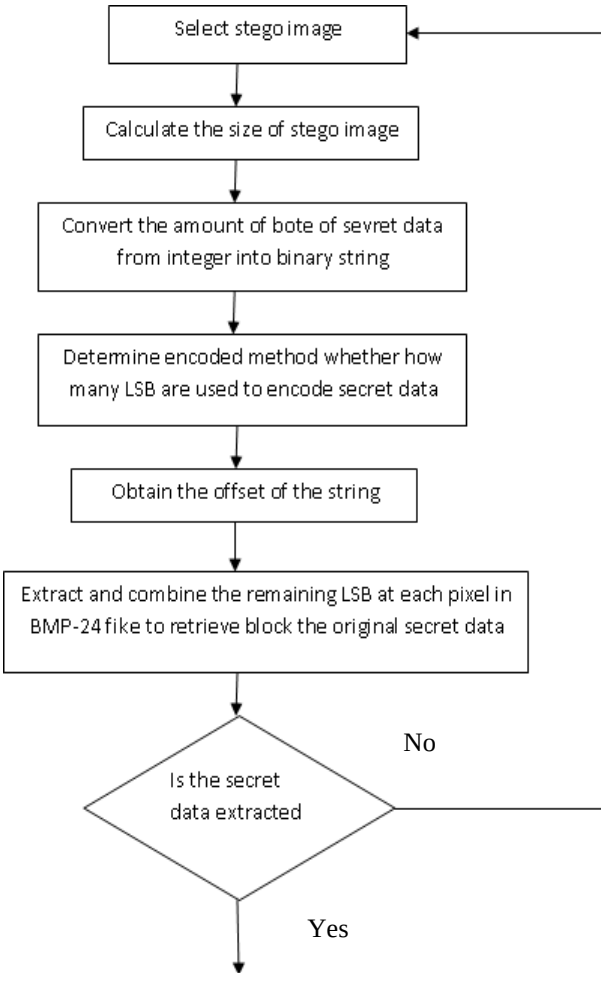

Fig. decoding process

V. Experimental Results

Consider following figure [a] is an original Lena Image and considered embed text file capacity is 90077bytes. Figure [b] is a stego-image with alpha value 0.03 and bit plane sets as 3. Figure [c] is a cover image with alpha as 0.03 and gamma as 0.5 after encryption and data compression as per proposed method.

Hence observed results of the proposed method produce more data embedded capacity and also preserved the visibility of the image.

[a]

Figure Original image

[b]

Figure Modified BPCS stego image

[c]

Figure Proposed method stego image

The experiment prefers peak-signal to-noise ratio (PSNR) as objective criteria of visual imperceptibility. The definition of PSNR as follow:

PSNR = 10 * log10 (Imax / MSE) db= 20 * log10 (I max / √MSE) db

Where, Imax is equal to 255 for grayscale images, and the mean squared error MSE is defined [13] to be: MSE = (1/MN) * Σ(i=1) M Σ(j=1) N(|CI(i,j) – SI(i,j)|)

Where, M and N represent the number of horizontal and vertical pixels respectively of the cover(C) and stego(S) image. The greater the PSNR is, the better the fidelity is, and the similar the two images are shown above.

Following table shows the details about the stego image

Image	Capacity	PSNR for modified BPCS			PSNR for modified BPCS		
		R	G	B	R	G	B
Lena	99298	33.4	33	33.2	43.2	34.8	34.9

Table Experimental result of proposed method

VI. Conclusion

The proposed scheme contributes a multi-layered embedding feature that enable senders to encode secret data into several cover-images sequentially to create a stealth camouflage to avoid intruder's unwanted attention.

It provides two levels of security, hybrid cryptography and steganography. If at all the intruder suspects it is quite impossible for him to steal the data because embedding byte positions are decided based on modified BPCS approach. After the cipher text is embedded, the degradation in image quality is not apparent to normal human eye. Threshold is customaries; hence sender can decide data hiding capacity as well as quality of the image. This approach can be extendable to send secret images in carrier image. This steganography is a strong information security technique, especially when combined with hybrid encrypted embedded data should be convinced.

References

[1] Yeshwanth srinivasan "high capacity data hiding system using Bpcs steganography"

[2] Abhishek Patidar Gajendra Jagnade Laxmi Madhuri Pranay Mehta Ronak Seth," Data Security Using Cryptosteganography in Web Application" 2012

[3] Eiji Kawaguchi and Richard O. Eason, "Principle and Applications of BPCS-Steganography", Kyushu Institute of Technology, Kitakyushu, Japan–University of Maine, Orono, Maine

[4] Lip Yee Por, Delina Beh, Tan Fong Ang, and Sim Ying Ong" An Enhanced Mechanism for Image Steganography Using Sequential Colour Cycle Algorithm" Malaysian Institute of Information Technology, Universiti Kuala Lumpur, Malaysia 2010

[5] Sheetal Mehta, Kaveri Dighe, Meera Jagtap, Anju Ekre," Web Based BPCS Steganography"

[6] Tao Zhang Zhaohui Li Peipei Shi," Statistical Analysis Against improved BPCS Steganography" Nankai University, College of Information Technical Science Tianjin, China 2010

[7] Sandeep Singh, Aman Singh,"A Review on the Various Recent Steganography Techniques"Department of Computer Science Engineering, Lovely Professional University Phagwara, Punjab, India 2013

[8] Smita Bansod, Vanita Mane, Leena Ragha "Modified BPCS steganography using Hybrid Cryptography for Improving Data embedding Capacity" Information Technology SAKEC, RAIT, Mumbai 2012