Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Improved Image Encryption scheme

Vaidehi Sridhar
Department of IT,
VIT university, Vellore-6, India.

Karthikeyan.P.
Department of IT,
VIT university, Vellore-6, India.

Shalini.C.
Department of IT,
VIT university, Vellore-6, India.

Abstract— In this paper, an enhanced mechanism for securing the information is proposed. Over the years people have used encryption and hiding individually for enabling secure data transfer but the proposed scheme deals with combining both these strategies at different level. This paper introduces two techniques that accompany the above mentioned mechanisms. One, the image to be encrypted is broken down into pixels and is then shuffled at the start of the process. Two, the format of the required file changed into some other format so that the information remains undetected. The results of several experimental, statistical analyses and key sensitivity tests prove that the proposed scheme is more efficient in securing text as well as digital images.

Keywords— Cryptography, Steganography, Chaotic Cryptography, OCML, Cipher, LSB

I. Introduction

Cryptography is the art and science of protecting the information by transforming the plaintext into cipher text such that no one but the intended recipient would be able to retrieve it. Steganography is the art and science of hiding messages within information such that no one but the intended recipient would know the existence of a message without involving the presence of key of any sorts unlike cryptography which uses key for both encryption as well as decryption.
In this paper, an improved scheme is proposed which makes use of both cryptography and steganography [1] in order to get better and enhanced security. Cryptography process that we have adopted involves two crucial steps where the image is first cut and shuffled before encrypting them using the Chaotic Encryption method. Owing to the increased security threats, cryptography is widely considered as the best way to protect data against passive and active threats over the network. Current cryptographic techniques are based on mathematical concepts of which the most promising scheme is the one based on Chaos [2]. But there is one little problem, an encrypted message can be easily detected even if it cannot be decrypted that fast. This paper mainly deals with developing a scheme with extra and better security features in order to overcome the problems with the existing algorithms.

Hiding the information has same advantages as encrypting a message, however in steganography the existence of the information is itself disguised and even if the information is extracted, it will still be encrypted. In order to overcome the drawback[1], in the proposed scheme the image in which the information has been inserted is eventually encrypted to provide extra protection. Finally introducing the file conversion technique to dodge the detection overcoming the drawbacks of encryption[2]. In section 2, we will discuss the procedure of image encryption and in section 3, we will prove the security of the proposed encryption scheme against common attacks by performing statistical analysis. Conclusion and future work are included in the final section.

II. Basic Concepts

In this section, we discuss the proposed scheme involving both steganography and cryptography[1]. The scheme breaks into four steps: firstly, the image is inserted into a cover image and then the stego image is encrypted using Chaotic scheme. Finally, the stego image which is encrypted is subjected to file conversion, changing the format of the image.

A. Chaos Based Algorithm In Cryptography

Chaotic behaviour implies random distribution that is not easily computable. The most important characteristics of chaos are its extreme sensitivity to initial conditions. The scheme[2] consists of two parts: firstly, choose one of the eight different types of operations to change the RGB values of the image pixels and secondly, transforming the RGB values with OCML model.

1) Advantages of chaos based encryption:

Advantages of chaos based encryption are as follows
1. Extremely secure.
2. Deterministic but simple.
3. Rapid means of data protection.

B. Lsb Steganography

In this method binary equivalent of the message to be hidden is distributed among the LSBs of each pixel[5]. The main idea behind this is that the least significant bit of a byte can change with little change to the overall file. For example we

will try to hide the character 'A' into an 8-bit colour image. We are taking eight consecutive pixels from top left corner of the image. The equivalent binary bit pattern of those pixels may be like this: -

00100111 11101001 11001000 00100111 11001000 11101001 11001000 00100111

Then each bit of binary equivalence of letter 'A' i.e. **01100101** are copied serially(from the left hand side) to the LSB's of equivalent binary pattern of pixels, resulting the bit pattern will become like this: -

00100110 11101001 11001001 00100110 11001000 11101001 11001000 00100111

1) Advantages of LSB Steganography:

Advantages of LSB Steganography are as follows

1. Does not change with the size of the file.
2. Hard to detect than other steganography techniques.

III. Proposed Encryption Scheme

The thought behind combining two different techniques may sound little difficult to grasp, so they are broken down for easier understanding. The whole process is as follows: using distortion again on the cover message and finally converting the file format to a totally undetectable format. While retrieving the message, the reverse algorithm involving file conversion of the distorted message and get back the original message by subjecting it to the reversal of distortion process.

A. Hiding The Message

1) Hiding Mechanism:

Hiding mechanism deals with enclosing the actual image within the cover image. The larger the cover message, the easier it is to hide the information. For this purpose in the proposed scheme we make use of digital images. The least significant bits of the image pixels can be used to carry the message. In our proposed scheme we first convert the image and the message and the length of the message to bytes consisting of 8 bits, to let know how much bits needs to be extracted. Using AND and OR operations, the bits are inserted one by one into the LSB starting with the length occupying the first 3 to 4 bytes.

2) Stego Module:

Stego module applies the following steps on the cipher text (Refer **Fig.1**).

-The Cipher text in Byte form along with cover image also in Byte form is served as input to stego module.
- Length of the message is calculated and inserted at the beginning of the image making it easy during extraction.
- Following the length, the actual message in form of bytes is inserted into the least significant bit of the cover image.
- Leads to the formation of Stego Image.

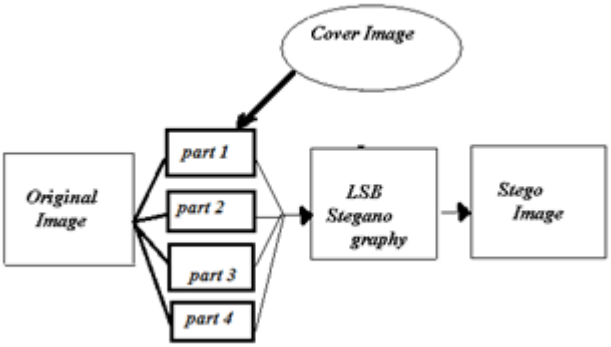

Fig. 1 Stego Module.

3) Crypto Module:

Crypto module applies the following steps on the Stego Image (Refer **Fig.2**).

-Chaotic Encryption is applied on the Stego Image by changing the value of the pixels using Key 1.
- Cipher Image is formed which entirely differs from the original cover image.

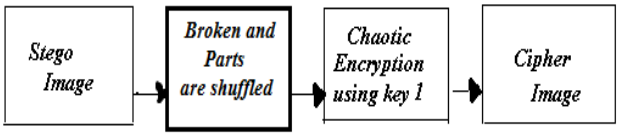

Fig. 2 Crypto Module.

B. Retrieving The Message

1) Retrieving Mechanism:

Retrieving mechanism includes two main steps.Firstly, the length of the message to be extracted is pulled out and then the LSB of the image pixels are singled out using AND and OR operations with the involvement of LEFT and RIGHT operations. The bits are collected into the resultant byte array.

*2) Crypto Module (**Reverse Process**):*

Crypto module includes the following steps for retrieving from the cipher image (Refer **Fig.3**).

-Cipher Image is received to decipher and get back the Stego Image used for hiding the message.

- Reverse of Chaotic Encryption is applied on the Cipher Image using **reverse of Key 1**.
- Stego Image is got back.

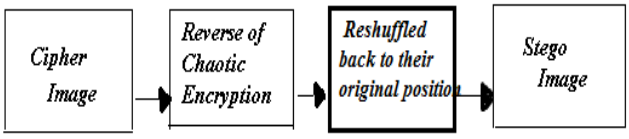

Fig. 3 Crypto Module (Reverse Process).

*3) Stego Module (**Reverse Process**):*

Stego module includes the following steps for retrieving from the Stego image (Refer **Fig.4**).

-Get the Stego Image and first read up to 32 bits to get the length of the message which tells us till how much length, the LSB of the image should be read.

- Followed by reading the least significant bits up to the desired length as Bytes.

-Cipher text is obtained in the form of bytes.

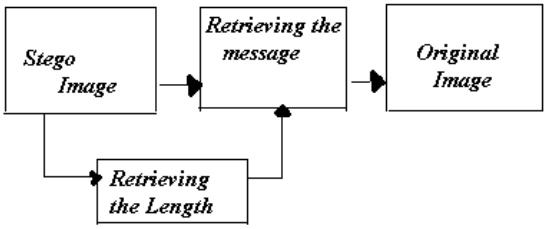

Fig. 4 Stego Module (Reverse Process).

C. File Conversion Technique

Here is the walk through of step by step procedure involved in the file conversion module (Refer **Fig.5**).

1. Get the cover image.
2. Convert it to other file format such that the original data gets displayed in a totally unrelated format.
3. For example, .jpeg to .txt (or) .bmp to .doc thus passes through unnoticed over the network.

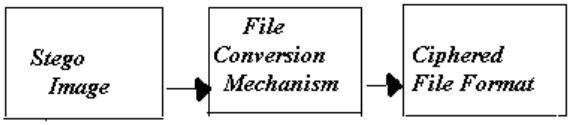

Fig. 5 File Conversion module.

D. Split And Insert

The proposed scheme also applies the split and insert technique during steganography (Refer **Fig.6**).

Splitting the original as well as the cover image based on the length of the key and inserting each piece into the other, say, O1 into C1 and so forth to ensure the additional protection.

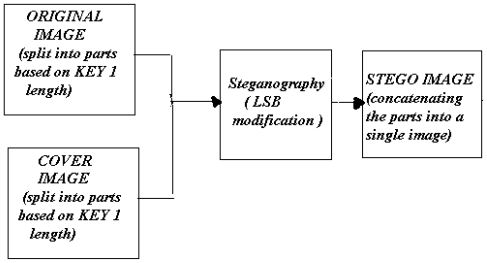

Fig. 6 Split and Insert.

IV. Procedure For The Proposed Encryption Scheme

A. Encryption Mechanism

In the newly proposed scheme, we make use of Steganography followed by Cryptography. The plain text is first Encrypted using Key 1 and is hidden inside a cover image which is later Encrypted using Key 2 with the additional technique of converting the image file to any other file format (Refer **Fig.7**).

Step 1: Cover Image To Stego Image
The selected image is inserted into the least significant bits of the cover image using LSB STEGANOGRAPHY with split and insert extension mechanism to form stego image.

Step 2: Stego Image To Cipher Image
The Stego image is then converted to a cipher image by breaking the image into parts and shuffling the parts following which they are encrypted using CHAOTIC ENCRYPTION using KEY 2.

Step 3: Cipher Image To Ciphered File Format
Cipher image is then transformed to completely unrelated file format.

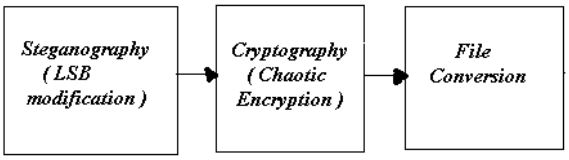

Fig. 7 Proposed Scheme for Encryption

B. Decryption Mechanism
The original image is got back from the ciphered file by applying the following steps (Refer **Fig.8**).

Step 1: Ciphered File Format To Cipher Image
The original image is then got back from the file in new format by applying the file conversion technique.

Step 2: Cipher Image To Stego Image
Reverse of Chaotic Encryption using REVERSE of KEY 2 is applied on the cipher image after which the broken parts are reshuffled to get the stego image.

Step 3: Stego Image To Cover Image
The information bits are retrieved from the stego image LSBs to extract the original image as well as cover image and extract parts of original image finally concatenating it to produce fully retrieved Original image.

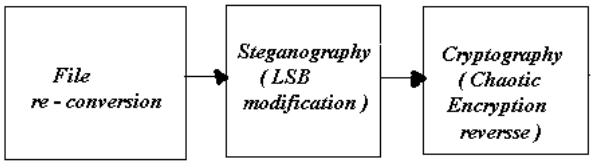

Fig. 8 Decryption (Reverse of Encryption).

V. Security Of The Proposed System

The proposed system is highly secure on account of the following:
-Combination of highly secure techniques using Chaotic Encryption for Cryptography and LSB modification for Steganography.
-Splitting before inserting extension provides more challenges while retrieval of the image.

VI. Conclusion

The work accomplished can be summarized with the following points:
-In this project, we have presented a new system which makes use of cryptography as well as steganography.
-The proposed method produces image which is much close to the original image with little or no distortion.
-Crypto/Stegano/Crypto system is more secure because of the use of the methods used in Encryption, Chaotic Encryption is very secure and the LSB steganography cannot be detected easily.
-File Conversion and Split and Insert extension ensures that the message is far better secured.

References

[1] Dipti Kapoor Sarmah, Neha Bajpai, *Proposed System for Data Hiding Using Cryptography and Steganograph,* October 2010
[2] Jun He, Jun Zheng, Zhi-bin Li, Hai-feng Qian, *An improved colour image encryption based on chaotic map and OCML model.*
[3] B.Schneier, *Description of a New Variable-Length key, 64-bit block cipher(Blowfish),* 1994.
[4] Robert Krenn, *Steganography and steganalysis.* Internet Publication, March 2004.
[5] Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay, Sugata Sanyal, *Steganography and Steganalysis: Different Approaches.*

