National Conference on Engineering Innovations and Solutions (NCEIS – 2018)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 6 | ISSN : 2456-3307

Key Modulation Technique for Secure Data Transfer Using Image Encryption

Kavya M N, Sudha M[1],Vaishnavi S[1],Chaya P [2]

[1]Student, Department of information science and engineering, GSSSIETW, Mysuru, Karnataka, India
[2]Assistant professor, Department of information science and engineering,GSSSIETW, Mysuru, Karnataka, India

ABSTRACT

This work proposes a reversible image data hiding (RIDH) scheme over the encrypted domain. The confidential or important information, which sent in non-encrypted form, there might be a chance of misuse cases. To avoid this, secret data has to be encrypted while sending over network and hiding secret data into carrier so that the existence of encrypted data has to be invisible in order to convey secret message confidentially. The data embedding is achieved through a public key modulation mechanism. At the decoder side, a powerful two-class SVM classifier is designed to distinguish encrypted and non-encrypted image blocks, allowing us to jointly decode the embedded message and the original image signal. Compared with the state-of-the-art, the proposed approach provides higher embedding capacity and is able to perfectly reconstruct the original image as well as the embedded message.

Keywords: Reversible image data hiding (RIDH), Support Vector Machine(SVM) and Least Significant Bit (LSB).

I. INTRODUCTION

The image is an electronic medium for copying, playback, broadcasting, and display of moving visual media. Image security has gained importance over time in numerous applications wherein, information in the form of the image is to be secured from an unauthorized user.

The use of internet has increased tremendously over the years and the concept of data security is gaining momentum. The word steganography combines the Greek words steganos meaning "covered" and graphein meaning "writing"[6]. The art and science of hiding information by embedding messages within other is steganography. It works by replacing bits of useless or unused data. Steganography is an Encryption technique that can be used along with cryptography as an extra-secure method in which to protect data. It can be applied to images, an image file or an audio file. Steganography is used to supplement encryption[7].An encrypted file may hide information, by using steganography even if the encrypted file is deciphered; the hidden message is not seen.

Cryptography involves creating, written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data. Cryptography is the study of hiding information, While Steganography deals with composing hidden messages so that only the sender and the receiver know that the existence of message. In Steganography, only the sender and the receiver know the existence of the message, whereas in cryptography the existence of the encrypted message is visible to the world [8]. Due to this, Steganography removes the unwanted attention coming to the hidden message. Cryptographic methods try to protect the content of a message, while Steganography uses methods that would hide both themessage as well as protect the content. By combining Steganography and Cryptography one can achieve better security.The proposed systemmakes use of least significant bit (LSB) insertion technique to hide the information. In Least significant bit (LSB) insertion technique, for hiding information, LSB of the image file is replaced with the information bits [3].LSB insertion is the simplest technique for implementing Image Steganography. The LSB method substitutes the LSBs of the hidden message with the LSB of cover image frames. Substituting data in the LSBs of any cover media is not detectable by human eyes (Human Visual System) i.e. very less change in the color[4]. Here the bits of the image from the image are directly embedded into the least significant bit plane of the cover frame in the deterministic sequence.

AES (Advanced Encryption Standard) is asymmetric encryption algorithm. The algorithm was developed by two Belgian cryptographers Joan Daemen and Vincent Rijmen.AES was designed to be efficient in both hardware and software and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits[2].AES is more secure than its predecessors DES and TripleDES as the algorithm is stronger and uses longer key lengths. It also enables faster encryption than DES and TripleDES, making it ideal for software applications, firmware, and hardware that require either low latency or high throughput. We use 128 bit key for an AES algorithm which specifies the number of repetitions should be 10 cycles' transformation rounds that convert the input called plain text into final output called ciphertext. Each round consists of several processing steps that depend on the encryption key [5].

II. EXISTING SYSTEM

The majority of the existing RIDH algorithms are designed over the plaintext domain, namely, the message bits are embedded into the original, un-encrypted images. Histogram Shifting (HS)-based technique, initially designed by Zhicheng Ni *et al.*, has been achieving better embedding performance through shifting the histogram of some image features. The latest Difference Expansion (DE)-based schemes and the improved Prediction Error Expansion (PEE)-based strategies were shown to be able to offer the state-of-the-art capacity distortion performance. As the source coding with side information at the decoder requires a feedback channel, this scheme would face severe challenges in many practical scenarios, e.g., secure remote sensing, where the feedback channel could be very costly. The embedding capacity of this type of method is rather limited and the incurred distortion on the watermarked image is severe.

III. LITERATURE SURVEY

Every Software development requires the survey process. The Survey process is needed to get the requirement for the software. The Survey also consists of studying the present system. A proper understanding of the tools is very much essential. Following is an extract of the information of the material collected during literature survey.

In this paper [1], information hiding techniques and historical details is discussed. Several methods for hiding data in audio, the image is described with appropriate to the environment of each medium as well as strength and weakness of each medium. The information about the secret key, transmission protocol, computer file system, hiding techniques is discussed.

In this paper [2], the different types of steganographic methods its pros and cons are discussed in detail. It gives information about the efficient method for sending safely to this destination.

The use of steganography application is to hide different types of data within the cover file. This is done according to the embedding algorithm and a secret key that performs the actions of the embedding process.

In this paper [3], the image data embedding scheme is proposed. We can replace one or more LSB of each pixel in the image frame. It becomes very difficult for the intruder to guess the data hidden in a frame. An advanced data hiding method by using a different bit with help of LSB substitution is proposed and analysed.

In this paper [4], it explains the prime need of hiding data from eavesdroppers is accomplished by the use of steganography. It explains about the wide researches that have been carried out on image steganography due to the high capacity of information be stored in the image file.This paper presented using LSB insertion which is very efficient method to embed data into a cover medium. It has explained the LSB insertion method for image steganography and its application.

In this paper [5], the focus on the data security approachwith combined encryption and steganographic techniques for secret communication by hiding it inside a multimedia file is done. The file such as images, audio, the image contains a collection of bits that can be further translated into same. The files composed of insignificant bits or unused areas which can be used for overwriting of other data. This paper explains the proposed algorithm using image steganography for enhancing data security.

In this paper [6], the explanation on a combination of cryptography and steganography is used for data hiding in image clips. A random frame selection, pixel swapping and encryption of message have been done to enhance the security of secret information which goes under the cover of image clips. Image steganography method has been developed to transfer secret data.

In this paper [7], the modern secure image steganography presents a challenging task of transferring embedded information to destination without being detected. Here, a simple approach for embedding a message into an image or the image from the pixel of carrier image is replaced with message information so that it cannot be observed by the human visual system, therefore exploits some limitations of the human visual system.

IV. ARCHITECTURE

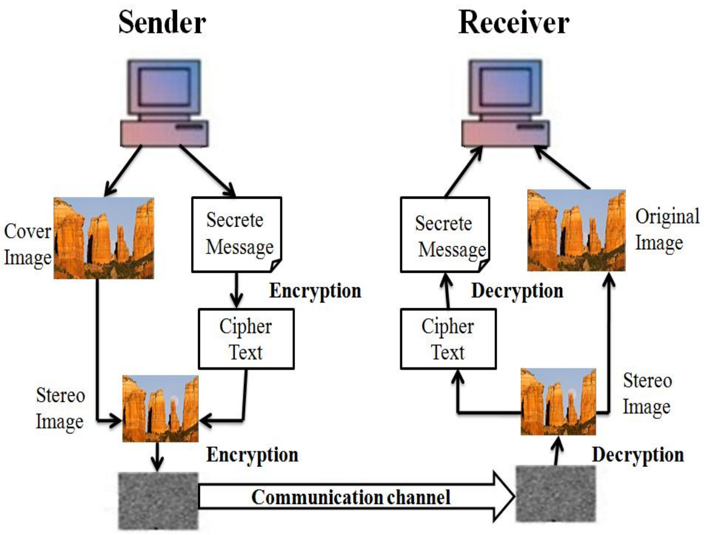


Figure 1. structure of secure transmission system.

As illustrated in Fig 1, the overall process is divided into two parts i.e. sender and receiver. When a sender wants to send the secret data, he will register for the access and extract the image file along with the secret data. The secret data will be encrypted using AES Algorithm while sending an image i.e. stego/stereo image. The Encryption key will be generated at the time of sending. The authorized receiver can only access the image file with the help of an encrypted key.

V. METHODOLOGY

An Image can be viewed as a sequence of still images. After embedding the data inside the image this image is referred as stegano image and this stegano image seems very similar to original images. However, there are many differences between data hiding within image and image encryption, where the first important difference is the size of the host media since images contain more sample number of pixels, an image has a higher capacity than a still image and more data can be embedded in the image. After the data encryption the encrypted data is divided into a number of chunks, these chunks will be given to the LSB technique, by this technique the chunks will be placed in the marked frame.

AES is based on a design principle known as a substitution-permutation network and is fast in both software and hardware. AES operates on a 4×4 column-major order matrix of bytes, termed the state. We use 128 bit key for an AES cipher which specifies the number of repetitions should be 10 cycles' transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext.

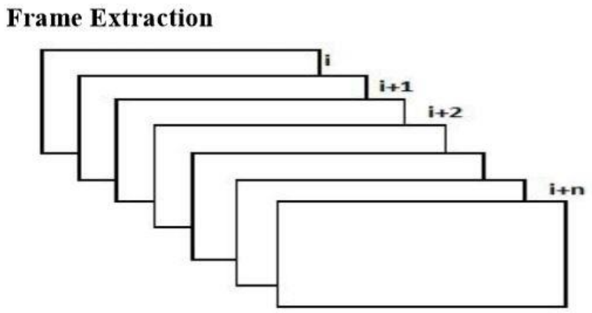


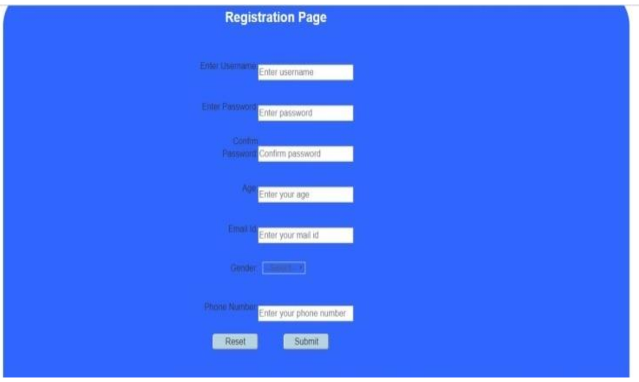
Figure 2. Frame extraction process for the image.

Least Significant Bit (LSB) insertion is a common, simple approach for embedding information in a cover image. As illustrated in Fig 2, Image is converted into a number of frames and then converts each frame into an image. Here, the bits of the image are directly embedded into least significant bit plane of the cover-frame in a deterministic sequence.

VI. RESULTS AND SCREENSHOTS

Lossless and Reversible Data Hiding in Encrypted Image with Public Key Cryptography

Figure 3. Homepage



Registration Page

Enter Username: Enter username

Enter Password: Enter password

Confirm Password: Confirm password

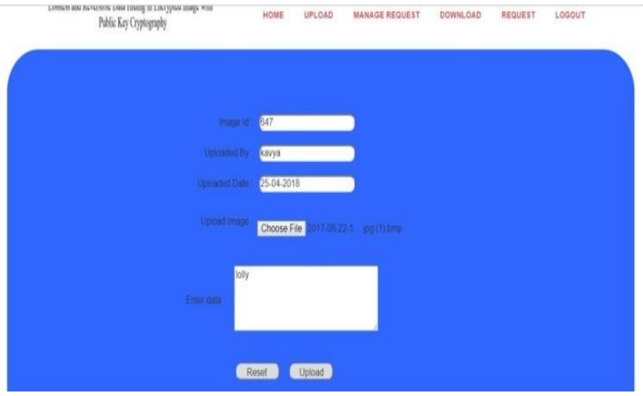
Age: Enter your age

Email Id: Enter your mail id

Gender:

Phone Number: Enter your phone number

Figure 4. User Registration Page



Lossless and Reversible Data Hiding in Encrypted Image with Public Key Cryptography

Image id: 647

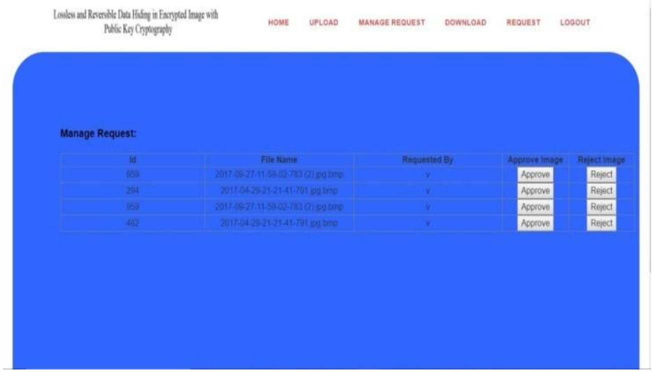
Uploaded By: kavya

Uploaded Date: 25-04-2018

Upload Image: Choose File 2017-06-22-1 .jpg (1).bmp

Enter data: lolly

Figure 5. sender uploading the image and inserting the data.

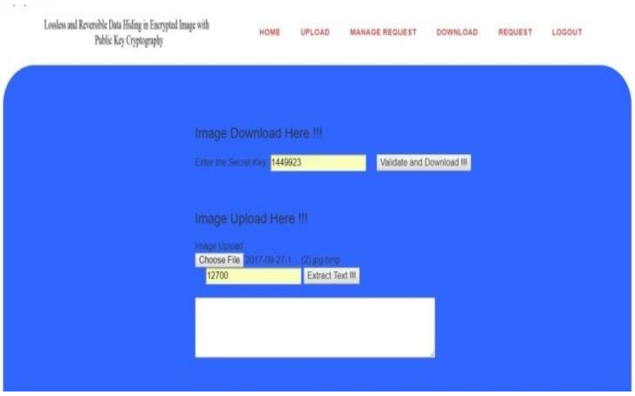


Lossless and Reversible Data Hiding in Encrypted Image with Public Key Cryptography

Manage Request:

Id	File Name	Requested By	Approve Image	Reject Image
959	2017-09-27-11-59-02-783 (2).jpg.bmp	v	Approve	Reject
294	2017-04-29-21-21-41-791.jpg.bmp	v	Approve	Reject
959	2017-09-27-11-59-02-783 (2).jpg.bmp	v	Approve	Reject
482	2017-04-29-21-21-41-791.jpg.bmp	v	Approve	Reject

Figure 6. sender accepting/rejecting the receiver's request



Lossless and Reversible Data Hiding in Encrypted Image with Public Key Cryptography

Image Download Here !!!

Enter the Secret Key: 1449923

Image Upload Here !!!

Image Upload: 2017-09-27-1 (2).jpg.bmp

12700

Figure 7. Receiver downloading page.

VII. CONCLUSION

This paper presents a comprehensive review ofimage steganographic technique. The proposedmechanism for secure data transfer using public key modulationallows embedding the data via LSB technique. Furthermore, popular image and image quality metrics available in the literature were discussed. Finally, steganalysis was surveyed from the point of view that improves the design of good steganographic systems.

The scope of the proposed technique can be further enhanced technique by embedding the secret data inside the audio files and video files. Based on this review, the following recommendations may help interested researchers in image steganography and also by considering two images as input and can embed secret message in both.

VIII. REFERENCES

1. "Separable Reversible Data Hiding in Encrypted Images Based on Two-Dimensional Histogram Modification", Dawn Xu, Kai Chen, Ranging Wang, and Shubing Su.
2. "Techniques for Secure Data Transfer", Jeffery Gardner, Jr.
3. "Efficient LSB Substitution for Interpolation based Reversible Data Hiding Scheme", Md. Abdul Waheed,HussainNyeem.
4. "Improved Reversible Data Hiding in Encrypted Images using Histogram Modification", Shuang Yi, Yicong Zhou.
5. "A New Method of Reversible on Compressed Gray-Level Histogram Shifting", TanwiBiswas, Md. Mehdi Hasan, TanoyDebnath.
6. "Image Steganography on Color Image using SVD and RSA with 2-1-4-LSB Technique", Sanjay Yadav, Prof.Anand. K.Tripathi, Pradeep Yadav.
7. "Comparative Study of Different Reversible Image Data Hiding Techniques", Anisha Jose, Mary Mareena, Saritha K.
8. "Substitution Steganography with Security Improved By Chaotic Image Encryption", Jakub Oravec and Jan Turan.
9. "An Imperceptible LSB Image Hiding on Edge Region Using DES Encryption", JakubEdi Jaya Kusuma, Oktaviana Rena Indriani, Christy Atika Sari, EkoHariRachmawan.
10. "Improvisation of security in image Steganography using DWT, Huffman Encoding & RC4 based LSB Embedding", PalakMahajanand Heena Gupta.
11. "High-Security Data Hiding Using Image Cropping and LSB Least Significant Bit Steganography", Khalid A. Al-Afandy, El-Sayed M. EL-Rabaie, Osama S. Faragallah, Ahmed ELmhalawy, Gh. M. El-Banby.
12. "An Advanced Diffie-Hellman Approach to image steganography", Shreyank N Gowda.
13. "Secure Reversible Data Hiding with Image Encryption", KB BiniAnd R. Sreejith.

14. “Advancement In Reversible Data Hiding Techniques: Review”, NamitaTiwariAnd Abha Singh Sardar.
15. “Automatic attendance management system using face detection”, TanwiBiswas, Md. Mehdi Hasan, TanoyDebnath.
16. “Secure Reversible Data Hiding Over Encrypted Domain via Key Modulation", Jiantao Zhou, Xiaoming Liu, Li Dong and Oscar C. Au.
17. “Reversible Data Hiding for Security Applications”, BaijFirdous and S Bhavani.
18. “Data Security Using Image Steganography and Weighing its Techniques", Pritam Kumar, Chetna Kumar, Prieeyanshi and Jaya Bhushan.
19. “A Novel Compressed Domain Technique of Reversible Steganography”, Mahmud Hasan, Kamuruddin Md. Nour, Tanzeem Bin Noor, and Monotosh Roy.
20. “Reversible Data Hiding In Encrypted Image”, Xinpeng Zhang.