Separeable Reversible Data Hiding In Encrypted Image

Ronak Bhatia, Pawan Jagtap, Ashish Gupta, Professor Deepti Lawand
Information Technology, Pillai’s Institute of Information Technology, New Mumbai, India

Abstract—The field steganography is a very popular technique for sending secret messages and a lot of researches are going on it. The project on separable reversible data hiding in encrypted image uses Rijndael algorithm which is an iterated block cipher algorithm that uses encryption or decryption of a block of data that is accomplished by the iteration of a specific transformation. As input, Rijndael accepts 1-D 8-bit byte arrays that create data blocks. The plaintext is input and then mapped onto state bytes. The design of Rijndael is based on easily understandable mathematical concepts including finite field mathematics and linear algebra and matrix manipulation. Using an encryption key, the person which has information to send encrypts the original image. With an encrypted image containing data, if a receiver has the data-hiding key, he can extract the data without knowing the content of the image. The receiver cannot extract the data by just having an encryption key, but by having this key, he can decrypt to obtain an image similar to the original one. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data to recover the original content without any error by exploiting the spatial correlation in natural image when the amount of additional data is not too large.

Keywords— Rijndael, AES, encryption, decryption, spatial correlation, steganography

I. INTRODUCTION

In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. There are many possible ways to transmit data using the internet: via emails, chats, etc. The data transmission is made very simple, fast and accurate using the internet. However, one of the main problems with sending data over the internet is the security threat it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring. Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data modification. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet. In order to improve the security features in data transfers over the internet, many techniques have been developed like: Cryptography, Steganography. While Cryptography is a method to conceal information by encrypting it to cipher texts and transmitting it to the intended receiver using an unknown key, Steganography provides further security by hiding the cipher text into a seemingly invisible image or other formats.

SCOPE

It can be used in banking sector where ATM pin is hidden inside image and the image is encrypted with credentials along with password to decrypt the image and retrieve the relevant data from it and send to the user through mail. At the user side, user decrypt the image with the appropriate password provided by the Bank and also decrypt the File in which they provide additional password to extract the ATM pin from image. If users provide a valid data hiding key then he get the relevant ATM pin from the image.

PROBLEM STATEMENT

The previous existing system deals with transmission of a message or data without allowing unauthorized access over the internet but with lesser security using the basic approach of steganography technique. In that approach data was revealed to the receiver only by applying both the keys. 1. If any one of the key (that is either data hiding key or encryption key) is lost while the transmission of key from sender to receiver then the receiver can’t extract the data. 2. If the mail from the sender doesn’t reach the expected client due to many reasons such as poor availability of network, poor availability of internet or loss of internet, improper mail id entered by the sender. 3. If the mail used is corporate mail ID.

II. PREVIOUS ARTS

In the existing system reversible data hiding technique the image is compressed and encrypted by using the encryption key and the data to hide is embedded in to the image by using the data hiding key [4]. At the receiver side he first need to extract the image using the encryption key in order to extract the data and after that he’ll use data hiding key to
extract the embedded data. It is a serial process and is not a separable process.

**Image Encryption**
The sender selects the file and applies his encryption algorithm to encrypt the image. Encryption is the method of applying or changing some of the attributes of the original image to form every different image. Nobody can read the exact image if he is unknown of the changed done by the content owner.

**Data Embedding**
After encrypting the image the sender embed some additional data behind the selected part of the image before transmission. Any type of image can be selected for the encryption like JPEG, PNG or BMP.

**Data Extraction**
This is the action performed at the receiver side. After receiving the data the main task of the receiver is to extract the original data hide behind the image. This technique is known as data extraction.

**Image Recovery**
Image recovery is the technique of decrypting the received image. The main task is to generate the image same as the original image. And this is done by the reversibly performing

The encryption action i.e., by using the decryption key.

![Image Recovery Diagram](image)

**Fig 3.1 Sketch of Non separable reversible data hiding in encrypted image.**

**Limitations**
Principle content of the image is revealed before data extraction. If someone has the data hiding key but not the encryption key he cannot extract any information from the encrypted image containing additional data.

**Figures and Tables**

<table>
<thead>
<tr>
<th>SR No.</th>
<th>List of Figures</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Sketch of Non separable reversible data hiding in encrypted image.</td>
<td>02</td>
</tr>
</tbody>
</table>

**III. PROPOSED SCHEME**
The proposed scheme is made up of image encryption, data embedding and data-extraction/image-recovery phases. The content owner encrypts the original image using an encryption key to produce an encrypted image [2]. The plaintext is input and then mapped onto state bytes. With an encrypted image containing data, if a receiver has the data-hiding key, he can extract the data without knowing the content of the image. The receiver cannot extract the data by just having an encryption key, but by having this key, he can decrypt to obtain an image similar to the original one. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data to recover the original content without any error by exploiting the spatial correlation in natural image when the amount of additional data is not too large, the embedded additional data can be successfully extracted and the original image can be perfectly recovered.

**IV. CONCLUSION**
Separable Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy-preserving requirements from cloud data management. Previous methods implement LSB in encrypted images by vacating room before encryption, as opposed to which we proposed by first embedding data, protecting it with a data hiding key and then encrypting the entire image. Thus the data hider is assure that data in image is protected with a key and the entire image is encrypted and that encrypted image can be decrypted only by the key know to the receiver. The proposed method can take advantage of all traditional techniques for plain images and achieve excellent performance without loss of perfect secrecy. Furthermore, this novel method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images.

**ACKNOWLEDGMENT**
Dedication, determination plays a key role in success of human life as well as inspiration and motivation plays a key role in success of any venture. At this level of understanding it is difficult to understand the wide spectrum of knowledge without proper guidance and advice. We would like to take this opportunity to express our sincere thanks to, dr. Madhumita chatterjee (h.o.d) and our project guide prof. Deepitlawand who have shown us the way all throughout the venture. Their kind co-operation & encouragement has helped us in doing the project. We are indebted to them for spending their valuable time in guiding us with minute details of our project. We would like to express our gratitude and appreciation to all those who gave us the possibility to complete this report. A special thanks to our final
year project coordinators, prof. Madhunashipudi, and prof. Sushoptigawade whose help, stimulating suggestions helped us especially in writing this report. Also this is the best opportunity to thank our principal dr. R. I. K. Moorthy for his timely help and guidance.

Our special thanks to the college faculty members, without their guidance our embarking on this project would not have been successful. We would take this opportunity to thank the staff of the IT department for providing us guidance.

REFERENCES


[2] Separable Reversible Data Hiding In Encrypted Image accessed on 15 July 2015 available online https://www.youtube.com/watch?v=BK_StE54pMs


