An Automatic System for Separable Reversible Data Hiding Using an Encrypted Image

[1]Lakshmi K V,[2]Viji C Babu, [3]Ms.Nisha Peter, [4]Dr.Sr.Lissy Anto
[1]Computer Science
[1]St.Joseph's College, Thrissur,India

Abstract—**The paper proposes a secure and authenticated discrete reversible data hiding method in cipher images, which consists of image encryption, data embedding and data-extraction/image-recovery phases. In the first phase, the content owner encrypts the original uncompressed image using the encryption keys which is the public key and secret key so as to provide more security to the system. The image is firstly divided into 8 bit blocks. Then the data is embedded into them and data is hidden in these blocks at random positions. After hiding all the small blocks are combined and then the message is sent. In the receiver side the image is decrypted using public key and their own secret key and then the message is extracted. SHA-1 algorithm is used for achieving authentication and DH - Diffie-Hellman Key Agreement is used for generating encryption and decryption key for achieving high security.**

***Index Terms*— Image encryption, image recovery, reversible data hiding.**

I. INTRODUCTION

Separable reversible data hiding using an encrypted image is software which provides high security while transferring data. Here data is send through an encrypted image. So hackers cannot easily hack the message. Mainly this software is used for sending sensitive secret data. Separable Reversible data hiding using an images is a technique, by which the original image can be lossless recovered and the embedded message can be extracted. Image security becomes increasingly important for many applications, e.g., confidential transmission, video surveillance, military and medical applications. For example, the necessity of fast and secure diagnosis is vital in the medical world. Nowadays, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over networks [1]. A number of reversible data hiding techniques were proposed in the recent years, but on analysis, all lacks in providing the security and authentication. This project proposes a novel reversible data hiding technique which work is separable, the receiver can extract the original image or extra embedded data or both according to the keys hold by the receiver [2].

In this system user can register and only the registered user can login to the system. And login user can select an image and encrypt the image using public and their own secret key and data embedded into this encrypted image. And send this encrypted image which contain data, so receiver can decrypt the image using pubic and their own secret key and can extract the data. Now a days we face so many security problems. So this system mainly aims on provide high security while sending secret data. By this system user can not need to worry about the security. Any efficient hacker cannot hack the message sending by this software. Because here message is embedding into encrypted image only after the encrypted image splits into small 8 bit of blocks and data hide in this blocks in random positions. After hiding combine this small blocks and then only send the message.

II. EXISTING SYSTEM

In the existing system, the date embedded into a normal image and data stored in the continuous positions in the image. Because of hiding data in continuous blocks user or hacker can easily identify the position where data hided and can extract the data.

III. PROPOSED SYSTEM

The proposed scheme is consist of image encryption, data embedding and data extraction and image-recovery phases. First of all encrypt the image, then message is embedding into encrypted image only after the encrypted image splits into small 8 bit of blocks and data hidden in this blocks in random positions. After hiding combine this small blocks and then send the message. In order to achieve authentication SHA-1 algorithm is being used[3].

IV. SYSTEM ARCHITECTURE

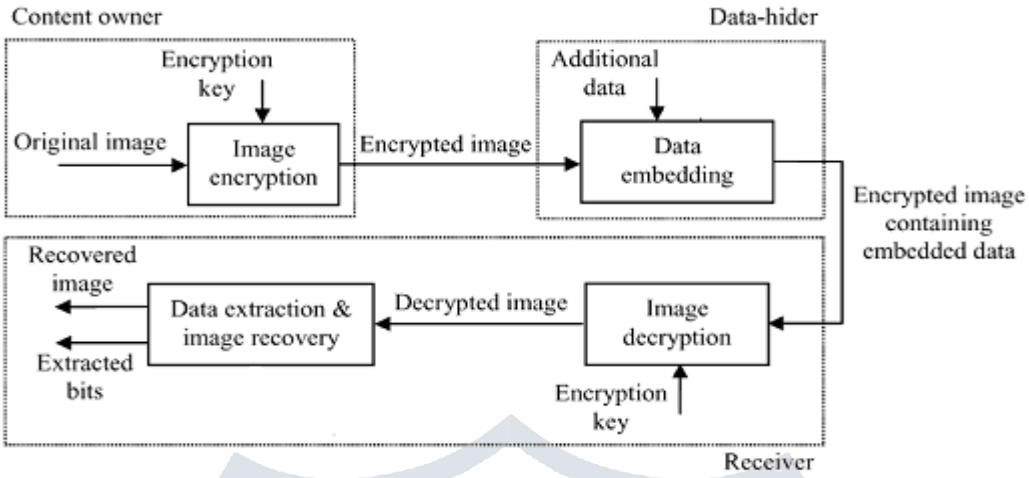

Figure 1. System Architecture

The system architecture is shown in figure 1.This module allows to pick the image from the gallery and then encrypt the image using a public key which is the exchange key between the sender and the receiver and use a secret key of their own side is used as encryption keys and SHA-1 algorithm is used for encryption .The encryption is done on a gray scale image using SHA-1 encryption algorithm. Data embedding is done in the encrypted image. First of all, split the whole encrypted image into 8 bit blocks and make a sparse space. A sparse space attempts to use space more efficiently even when it is mostly empty. Data is then hidden in the random position of each blocks. Decrypt the image using a public key which is the exchanging key between the sender and the receiver and a secret key of their own side is used for decryption. Like encryption split the whole image into small 8 bit blocks. And extract the data hidden in the random position of each blocks.

V. IMPLEMENTATION

Sender side

Figure 2. Sender side home page

Figure 3

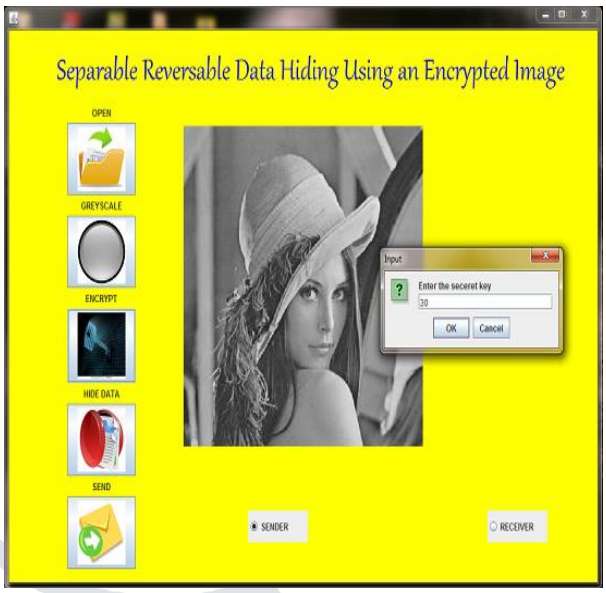

Figure 4

Figure 5

Figure 6

Receiver side

Figure 7 Receiver side Window

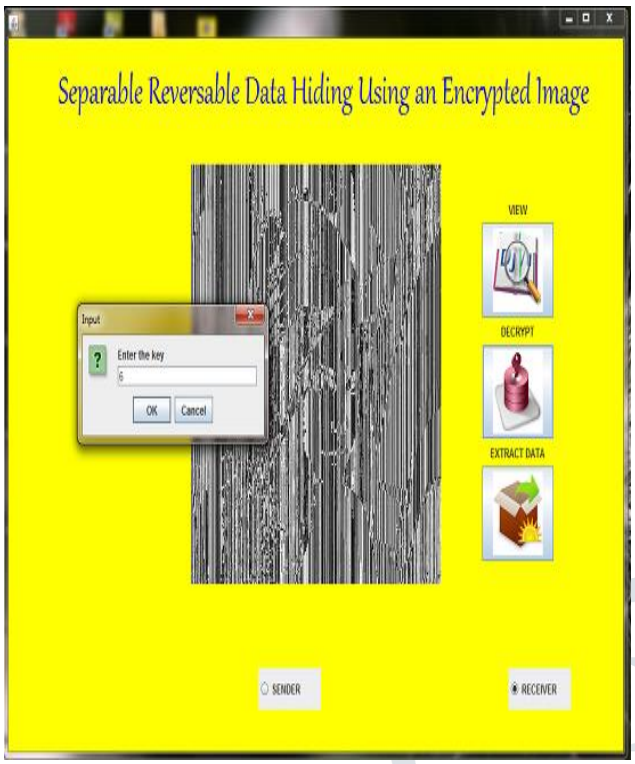

Figure 8

Figure 9

Figure 10

Figure 3 shows the sender side window and here we can open a folder from the system of user presently using and another option is for converting the original image into gray scale.And next button is for encrypt the image, when we click the button a dialogue box appear to enter the public key which is exchanged by the receiver and there after to enter the secret key , like shown in the figure 3 & 4.Then an encrypted image will form like the figure 5. Next button is for hiding the data ,when we click the button a dialogue box will appear to enter the data like figure 6 and there after click the send button to send the data.Figure 7 shows the receiver side window. In the receiver side there are 3 buttons one for viewing the encrypted image which is send by the sender and next button is for decrypt the image ,when we click the button, like sender side here also appear a dialogue box for entering public key which is exchanged by the sender and there after the secret key ,like shows in the figure 8 & 9.And next button is for extract the data which is send by the user,when we click the button a dialogue box will appear like in the figure 10 and yes or no option is there to save or don't save the data,when we click yes button we can save the data in our system with extension .txt.

VI. CONCLUSION

This work proposes a novel scheme for separable reversible data hiding in encrypted images [5]. This consists of image encryption, data embedding and data-extraction/image-recovery phases. In the first phase, the content owner encrypts the original uncompressed image using encryption keys that is public and secret keys so system provide more security. And message is embedding into encrypted image only after the encrypted image splits into small 8 bit of blocks and data hide in this blocks, in random positions. After hiding, combine these small blocks and then send the message. In the receiver side, the image is decrypted by public and their own secret key and the message is extracted. Our study helps constructing secure transmission of secrete file preventing any third party access and security level of data is increased by encrypting data [4]. In future we can use audio, video in case of image as cover for hiding the data.

VII. ACKNOWLEDGMENT

First of all, I am grateful to The Almighty God for establishing me to complete this project. I am especially thankful to my guide, Ms. Nisha Peter, and all other faculty members from the Department of Computer Science and my friends, for giving me their sole co-operation and encouragement and critical inputs in the preparation of this report. Finally I express my heartfelt thanks to our Lab Instructors, colleagues, friends and my dear Parents for giving me valuable advice and support throughout my project work.

REFERENCES

[1]. Rini.J , " Study on Separable Reversible Data Hiding in Encrypted Images", International Journal of Advancements in Research & Technology, Volume 2, Issue 12, December-2013

[2]. Dr.V.Khanaa, Dr.Krishna Mohanta , "Secure And Authenticated Reversible Data Hiding In Encrypted Images" ,International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 3 March 2013 Page No. 558-568

[3]. C.Anuradha, S.Lavanya," Secure and Authenticated Reversible Data Hiding in Encrypted Image", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 4, April 2013 ISSN: 2277 128X

[4]. Lalit Dhande, Priya Khune, Vinod Deore, Dnyaneshwar Gawade, "Hide Inside-Separable Reversible Data Hiding in Encrypted Image" , International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-3, Issue-9, February 2014

[5]. Xinpeng Zhang, ," Separable Reversible Data Hiding in Encrypted Image" , IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012