A System for Separable Reversible Data Hiding using an Encrypted Image

Nisha Peter
Computer Science Department
St. Joseph's College,
Irinjalakuda,Thrissur, India

***Abstract* — The paper highlights a secure and authenticated data hiding method in encode images. The different phases of the system consist of encryption of image, data embedding and data extraction and recovery of image. To provide more security to the system the owner encrypt the uncompressed image using the encryption keys which the public key and the secret key. The encrypted image is thenportioned into eight bit blocks.To provide safety of the data it is embedded in the blocks at random positions in the encrypted message. The message is sent by embedding the data in the encrypted image. At the receiver side using the public key and their own secret key the image is decrypted and then the message is extracted. For Authentication SHA-1 algorithm is used and for obtaining high security DH - Diffie-Hellman Key Agreement is used for generating encryption and decryption.**

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

I INTRODUCTION

Currently, the broadcast of images is a daily routine and it is essential to find a proficient way to transmit them over networks .In modernera there are a diversity of reversible data hiding techniques were projected. But all lack in providing the security and authentication. This project proposes a reversible data hiding technique where work is separable, the receiver can extract the original image and extra embedded data or both according to the keys hold by the receiver. Separable Reversible data hiding using an encrypted image is a software which provides high safety while transferring the data. An encrypted image is used to

send data. So hackers cannot simply hack the message. The software is mainly used for transporting sensitive secret data. It is a technique, in which the original image can be lossless recovered and the embedded message can be extracted. Image security becomes ever moreimportant for many applications. The different fields are confidential transmission, video surveillance, military and medical applications etc.Nowadays, the need of fast and secure diagnosis is critical in the medical world. Thus the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over networks [1].
In this system only the registered users can login to the system. Authenticated user can select an image and encrypt the image using public and their own secret key. Thus it provides more security to the system. Then the image is divided into 8 bit blocks .The data is hidden in the 8 bit block at random positions. Thus the embedded data is send through the encrypted image. The receiver then decrypt the image using pubic and their own secret key and can extract the data. In our time we face so many security problems. Our system will provide high security while sending secret data. By using this system user need not to be anxious about the security. Any proficient hacker cannot hack the message because of the security provided by this software. Because here message is embedding into encrypted imageafter the encrypted image is divided into 8 bit of blocks and data is hidden in the blocks at random positions. Thus the small blocks are combined and send the message. The receiver will decrypt the image and can extract the data.

II EXISTING SYSTEM

In the existing system, the data is embedded into an image and data is stored in the continuous positions in the image. The hacker can easily identify the position because of hiding data in continuous blocks and can easily extract the data.

III PROPOSED SYSTEM

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

IV SYSTEM ARCHITECTURE

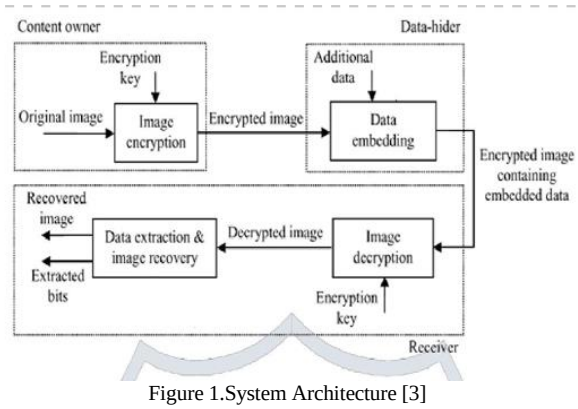

Figure 1.System Architecture [3]

The system architecture is shown in figure1.Image encryption module allows to choose 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.SHA-1 algorithm is used for encryption. The encryption is prepared on a gray scale image using SHA-1 encryption algorithm. Data embedding is done in the encrypted image. Initially divide the whole encrypted image into 8 bit blocks and make a sparse space. A sparse space attempts to use space more proficiently even when it is mostly vacant. Data is then hidden in the random position of each blocks of the image.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. Then split the whole image into 8 bit blocks. And extract the data hidden in the random position of each blocks.

IV IMPLEMENTATION

Sender side

Figure 2 Sender side

Figure 3

Figure 4

Figure 5

FIGURE 6

Receiver side

Figure 7 Receiver side window

Figure 8

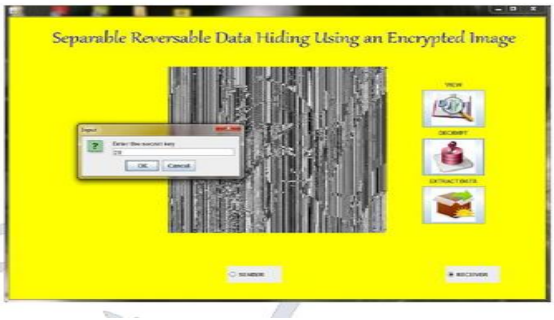

Figure 9

Figure 10

Figure 3 shows the sender side window and the user can open a folder from the system for selecting the image and the user is provided with another option for converting the original image into gray scale. And when we click button for encrypt the image, 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 be displayed as in the figure 5. When we click the button for hiding the data a dialogue box will appear to enter the data as given in figure 6.Then 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 decrypt image 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 to save or don't save the data. When we click yes button we can save the data in our system with extension .txt.

CONCLUSION

This work proposes a novel scheme for separable reversible data hiding in encrypted images [5]. The system consists of image encryption, data embedding into the encrypted images and data-extraction/image-recovery phases. To grant more security to the system , the content owner encrypts the original uncompressed image using encryption keys that is public and secret keys.The message is embedding into encrypted image only after the encrypted image divides into small 8 bit of blocks and data is hidden in the blocks at random positions. After hiding, combine these small blocks into one and then send the message to the receiver. In the receiver side, the image is decrypted using the public and their own secret key. Then 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 also use audio, video instead of images as a wrap for hiding the data.

ACKNOWLEDGMENT

First of all, I would like to thank God, the Almighty, for having made everything possible by giving the strength and courage to do this paper work. Without him, I would not have had the wisdom or the physical ability to accomplish this paper. I also like to express my deep gratitude to all those people who have helped me to carry out this work.A lot of people have directly or indirectly contributed to this project in a variety of ways.

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.KrishnaMohanta , "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]. LalitDhande, PriyaKhune, Vinod Deore, DnyaneshwarGawade, "Hide Inside-Separable Reversible Data Hiding in EncryptedImage" , 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