International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

Reserving Room Approach on Reversible Data Hiding before Encryption

Prof. Sagar Rajebhosale[1] Mr. Gaurav Suryawanshi[2], Mr. Kalpesh Gharte[3], Mr. Amey Jadhav[4], Mr. Jeewan Kale[5]

Assistant Professor, Dept. of Information Technology, PVG's COE Nashik, Maharashtra, India[1]
UG Student, Dept. of Information Technology, PVG's COE Nashik, Maharashtra, India[2,3,4,5]

ABSTRACT

Now-a-days peoples give more attention while transmitting secure data. For that Reversible Data Hiding algorithm is mostly preferred since it maintains the property that the original image is recovered from encrypted image and embedded data without analysis into it. But the existing method embeds data by reversibly vacating room from encrypted images, which will further leads to the loss of data at the receiver end. Hence authors propose the method which reserves the room for transmission of data from sender to receiver with existing RDH (Reversible Data Hiding) algorithm and therefore it is very easy for data hider to embed data reversibly in encrypted image. Thus in proposed method data extraction an image recovery parts are free from any errors. Also analysis shows that the proposed method can embed data 10 times as large payloads for same quality image than the previous method can embed.

KEYWORDS: Reversible data hiding, image encryption, security, histogram shift.

INTRODUCTION

For transmitting any confidential data over the network many issues like hacking, stealing this data may arise. So techniques which prevents this attacks on such on confidential data is known as Encryption In encryption original data is transformed into some secure format so that it will be very hard to understand by third party person. Information embedding and data hiding systems play a key role in addressing couple of major challenges that have arisen from the widespread distribution of multimedia content over digital communication networks. In particular, these systems are enabling technologies for enforcing and protecting copyrights, authenticating and detecting tampering of multimedia signals images. This significant system is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is acceptable. Since first introduced, RDH has attracted considerable research interest In existing system there were some problems like, while transferring data from sender to receiver some additional data is added to encrypted image which we don't want. While transferring image, the image quality gets degraded at receiver end, and additional data gets added which is not required. Hence we proposed a novel method which reserves the room (bandwidth) before the actual encryption between sender and receiver. In proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. If we reverse the order of encryption and vacating room, i.e., reserving room prior to image encryption at content owner side, the RDH tasks in encrypted images would be more natural and much easier which leads us to the novel Reserving Room Approach on Reversible Data Hiding before Encryption. Framework, reserving room before encryption (RRBE)

There are few technique by which we are vacating the room after encryption.

1.Framework for RDH for vacating room in encrypted image. By first extracting compressible features of original image and then compressing them lossless. In this way space can be created for embedding data [5].

2. Another method is based on difference expansion, for vacating room in encrypted image in which the difference of each pixel group is expanded, e.g., multiplied by and thus the least significant bits (LSBs) of the difference are all-zero and the space created can be used for embedding data.

3. Another method is histogram shift (HS)[3], for vacating room in encrypted image in which space is saved for data embedding by shifting the bins of histogram ofgrey values. And the space created can be used for embedding data

RELATED WORKS

The proposed architecture consists of a Reserving Room before Encryption (RRBE)method for the data hiding in colour images and also allows the reversible extraction of cover image. VRAE images are sometimes inefficient and difficult to extract data; we like to reverse the order of encryption and vacating room, i.e., reserving room before image

Encryption at content owner side becomes a novel framework reserving room before encryption (RRBE) which leads to the more natural and much easier Reversible data hiding tasks in encrypted images. Here the content owner first reserves enough space on original image and then converts the image into its encrypted version with the encryption

Key. Now, the data hiding process in encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space previously reserved. The data extraction and image recovery are identical to VRAE. Using colour images as the cover images, more data can become hidden. We can reserve more space from three

channels of colour image. Reserving Room Approach on Reversible Data Hiding before Encryption. In proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. If we reverse the order of encryption and vacating room, i.e., reserving room prior to image encryption at content owner side, the RDH

tasks in encrypted images would be more natural and much easier which leads us to the novel framework, reserving room before encryption (RRBE).

SYSTEM ARCHITECTURE

In this system, firstly after getting the image as input we reserve the room (bandwidth) for transmitting the data from sender to receiver. After that the actual encryptionis done, and this encrypted image send to the Data hider. The Data hider embed thedata to that encrypted image and apply Data hiding key for more security. This marked encrypted image is then transmitted to the receiver. At the receiver end by using Data hiding key data is extracted and by using encryption (private) key original image is recovered.

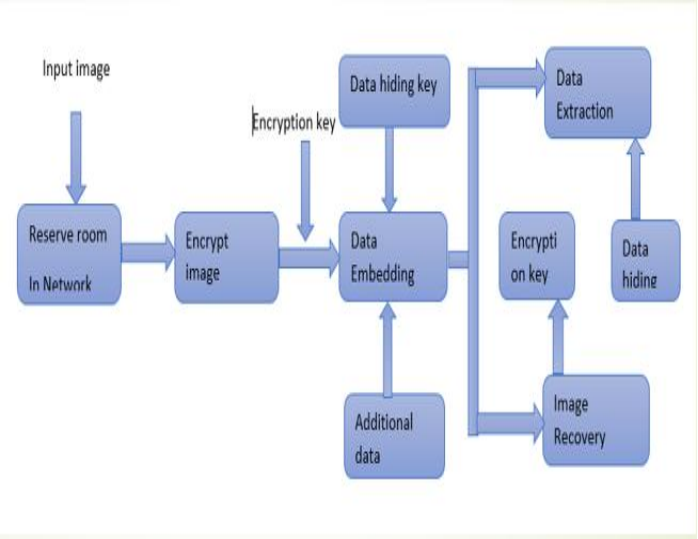

Figure 1: System Architecture

MODULES DESCRIPTION

1 Encryption

Encryption is the process of encoding messages or information is such a way that only authorize person can read it. In an Encryption scheme, the intended communication information or message, referred to as plain text, is encrypted using an encryption algorithm.

2 Room Reserve

Room reserve means finding a appropriate available path to send the data to the receiver, so that data will be send at greater speed to the given destination.

3 Decryption

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its encrypted form. In decryption, the system extracts and converts the garbled data transforms it to text and images that are easily understandable not only by the reader but also by the system.

4 Encrypted Image Generations

In this module, to construct the encrypted image, the next stage can be divided into three steps:

- IMAGE PARTITION
- SELF REVERSIBLE EMBEDDING followed by image encryption.

At the beginning, image partition step divides original image into two parts and then, the LSBs of are reversibly embedded into with a standard RDH algorithm so that LSBs of can be used for accommodating messages; at last, encrypt the rearranged image to generate its version.

5 Image Partition

The operator here for reserving room before encryption is a standard RDH technique, so the goal of image partition.

6 Self Reversible Embedding

The goal of self-reversible embedding is to embed the LSB-planes of into by employing traditional RDH algorithms. We simplify the method in to demonstrate the process of self-embedding.

7 Data Hiding In Encrypted Image

`In this module, a content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider (e.g., a database manager) and the data hider can embed some auxiliary data into the encrypted image by lossless vacating some room according

to a data hiding key.

8 Data Extraction and Image Recovery

In this module, Extracting Data from Encrypted Images to manage and update personal information of images which are encrypted for protecting clients privacy, an inferior database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. When the database manager gets the data hiding key, he can decrypt and extract the additional data by directly reading the decrypted version. When requesting for updating information of encrypted images, the database manager, then, updates information through LSB replacement and encrypts up dated

information according to the data hiding key all over again. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content

9 Data Extraction and Image Restoration

In this module, after generating the marked decrypted image, the content owner can further extract the data and recover original image.

I. SIMULATION RESULTS

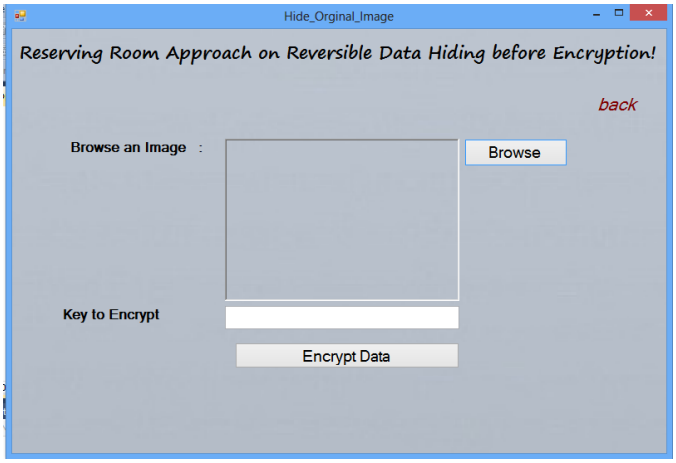

Figure 2 : Encryption

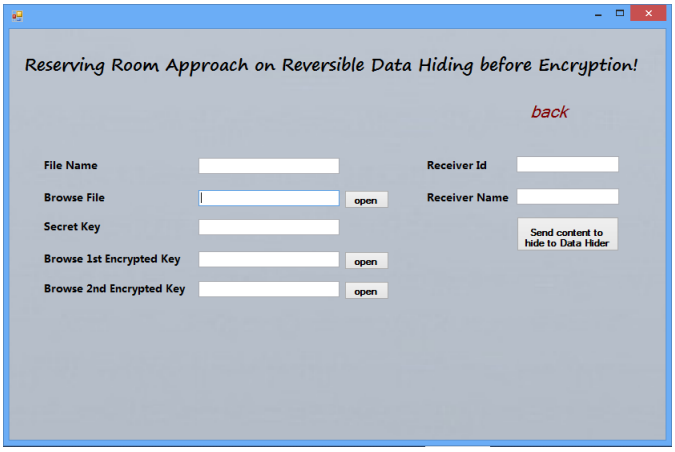

Figure 3 : Encryption

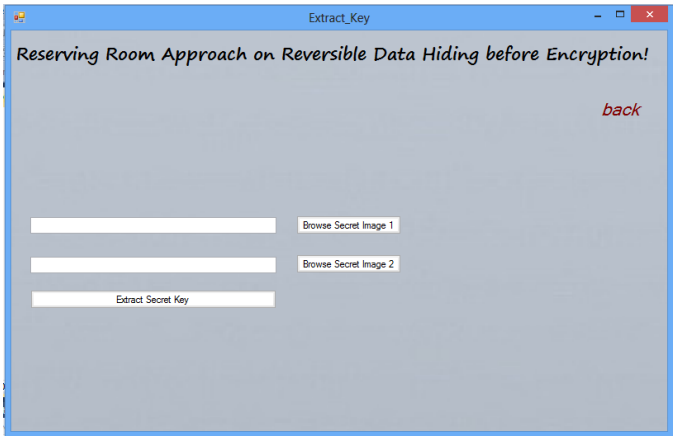

Figure 4 : Decryption

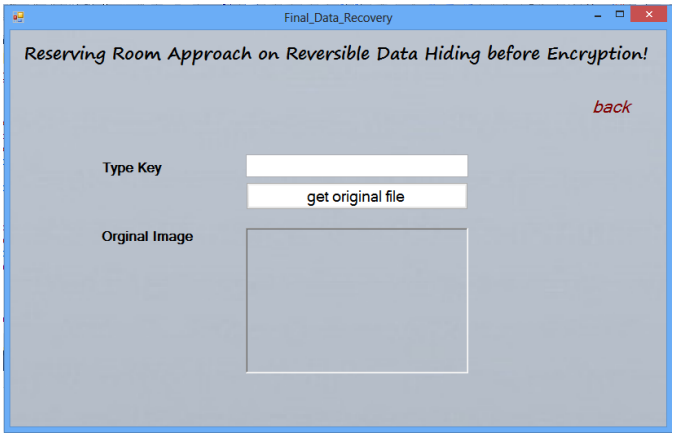

Figure 5 : Decryption

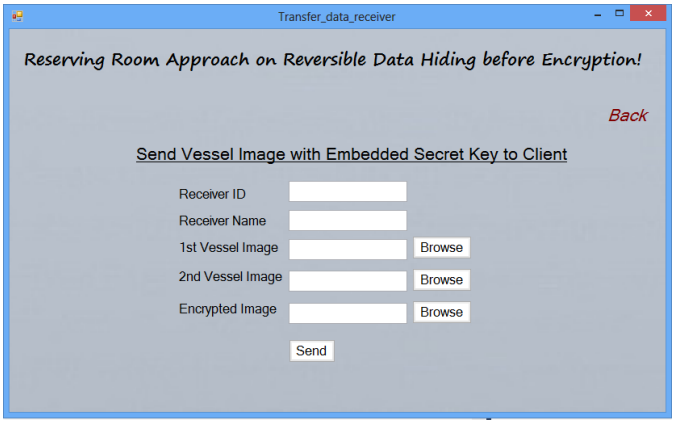

Figure 6 : Receiver

II. CONCLUSION AND FUTURE WORK

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 RDH in encrypted images by vacating room after encryption, as opposed to which we proposed by reserving room before encryption. Thus the data hider can benefit from the extra space emptiedoutin previous stage to make data hiding process effort-less. The proposed method can take advantage of all traditional RDH 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.

REFERENCES

1]Kede Ma, Weiming Zhang, Xianfeng Zhao, *Member, IEEE*, Nenghai Yu, and Fenghua Li" Reversible Data Hiding in Encrypted Images byReserving Room Before Encryption",*IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 3, MARCH 2013*

*2]*DemijanKlinc_, CarmitHazayy, AshishJagmohan, Hugo Krawczykand Tal Rabinz "On Compression of Data Encrypted with Block Ciphers"

3]Diljith M. Thodi and Jeffrey J. Rodríguez, Senior Member" Expansion Embedding Techniques for Reversible Water marking" *IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 16, NO. 3, MARCH 2007*

*4]*P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting." Signal Process. (2009).

5]K. Hwang and D. Li, "Trusted cloud computing with secure resources and data colouring." IEEE Internet Compute (2010).

6]W. Zhang, B. Chen, and N. Yu,"Capacity-approaching codes for reversible data hiding." in Proc 13th Information Hiding (2011).

7]X. L. Li, B. Yang, and T. Y. Zeng, "E_cient reversible watermarking basedon adaptive prediction-error expansion and pixel selection." IEEE Trans.Image Process. (2011).

8]X. L. Li, B. Yang, and T. Y. Zeng, "E_cient reversible watermarking basedon adaptive prediction-error expansion and pixel selection." IEEE Trans.Image Process. (2011).

9]X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans.Inf. Forensics Security.

BIOGRAPHIES

Prof. Sagar S. Rajebhosale.
M.E. (Computer Engg.)
Assistant Professor, Dept. of Information Technology, PVG's COE Nashik, Maharashtra, India

Mr. Jadhav Amey K.
B.E. (Information Technology)
UG Student, Dept. of Information Technology, PVG's COE Nashik, Maharashtra, India

Mr. Gharte Kalpesh S.
B.E. (Information Technology)
UG Student, Dept. of Information Technology, PVG's COE Nashik, Maharashtra, India

Mr. Suryawanshi Gaurav K.
B.E. (Information Technology)
UG Student, Dept. of Information Technology, PVG's COE Nashik, Maharashtra, India

Mr. Kale Jeewan D.
B.E. (Information Technology)
UG Student, Dept. of Information Technology, PVG's COE Nashik, Maharashtra, India