ISSN 2395-1621

Steganography of Encrypted Images by Reserving Room Before Encryption

[#1]Mr.Mitesh Kumar Rath, [#2]Mr.Saurabh Kumar Rai, [#3]Mr.Punit Kumar Mishra,
[#4]Miss.Snhehal Adagale, [#5]Prof.S.R.Todmal

[1]punit72mishra@gmail.com
[2]saurabhkumarrai3@gmail.com

[#1234]Department Of Information Technology
[#5]Prof. Department Of Information Technology

Jspm's Imperial College Of Engineering & Research, Wagholi,Pune-412207

ABSTRACT

The data owner deals with the transmission of immense data. Data owner encrypts the original uncompressed image by using the encryption key. Then the LSB (least significant bit) of the image is compressed to create thinly dispersed or scattered space to adjust data. Receiver uses the data hiding key to retrieve the accommodated data while the receiver is unaware of the original image's content. Receiver uses decryption key to retrieve data to obtain similar to uncompressed image, receiver will not be able to retrieve the accommodated data .The receiver requires data hiding and encryption key to retrieve the data from the image and obtain the original uncompressed image without any loss.

Keywords: Reversible data hiding, Encryption, Data hiding and extraction.

ARTICLE INFO

Article History

Received :22nd April 2016

Received in revised form :

23rd April 2016

Accepted : 25th April 2016

Published online :

28th April 2016

I. INTRODUCTION

1.1 Encryption

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating ciphertext that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors.

Types of Encryption

Symmetric key encryption

In symmetric-key schemes the encryption and decryption keys are the same. Communicating parties must have the same key before they can achieve secure communication.

Public key encryption

In public-key encryption schemes, the encryption key is published for anyone to use and encrypt message. However, only the receiving party has access to the decryption that enables message to be read. Public-key encryption was first described in a secret document in 1973 before then all encryption schemes were symmetric-key (also called private-key).

A publicly available public key encryption application called Pretty Good Privacy (PGP) was written in 1991 by Phil Zimmermann, and distributed free of charge with source code, it was purchased by Symantec in 2010 and is regularly updated.

Use of encryption

Encryption has long been used by military and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. For example, the Computer Security Institute reported that in 2007, 71% of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage. Encryption can be used to protect data "at rest", such as information stored on computers and storage devices (e.g. USB flash drives). In recent years there have been numerous reports of confidential data such as customer's personal records being exposed through loss or theft of laptops or backup drives. Encrypting such files at rest helps protect them should physical security measures fail. Digital rights management systems, which prevent unauthorized use or reproduction of copyrighted material and protect software against reverse engineering (see also copy protection), is another somewhat different example of using encryption on data at rest.

Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, microphones, wireless systems, Bluetooth devices and bank automatic teller machines. There have been numerous reports of data in transit being intercepted in recent years. Data should also be encrypted when transmitted across networks in order to protect against eavesdropping of network traffic by unauthorized users.

Message verification

Encryption, by itself, can protect the confidentiality of messages, but other techniques are still needed to protect the integrity and authenticity of a message, for example, verification of a message authentication code (MAC) or a digital signature. Standards for cryptographic software and hardware to perform encryption are widely available, but successfully using encryption to ensure security may be a challenging problem. A single error in system design or execution can allow successful attacks. Sometimes an adversary can obtain unencrypted information without directly undoing the encryption. See, e.g., traffic analysis, TEMPEST, or Trojan horse.

Digital signature and encryption must be applied to the ciphertext when it is created (typically on the same device used to compose the message) to avoid tampering, otherwise any node between the sender and the encryption agent could potentially tamper with it. Encrypting at the time of creation is only secure if the encryption device itself has not been tampered with.

Steganography

Steganography is the science of hiding information Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Steganography can be said to protect both messages and communicating parties.

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganography coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganography transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the colour of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

II. LITERATURE SURVEY

A Steganography Algorithm for Hiding Image in Image Improved LSB by Minimize Detection

In [5] Vijay kumar Sharma etc. all, explains the practice of protecting a file, image, or video with another file, image, or video. In recent years, steganography has great importance in data hiding, but stegananalysis identify the encoded data into other data and if possible it recovers that data.
So, to overcome this problem the paper presents a new algorithm based on 8-bit (greyscale) or 24- bit (colour images). This algorithm encapsulates MSB of secret image into LSB of colour image and by using computational complexity it also maintains the quality of stego image.

A Reversible Data Hiding Method for Encrypted Images

In [3] William Puech etc. all, explains the paper tells that over, the time it has become more essential to secure multimedia data and for that new data hiding algorithm and encrypting algorithms are found.

The steps that are followed are as follows:

- The multimedia data is compressed. Now there is challenge of encryption and compression.
- RDH removes embedded data before decryption.
- in this paper algorithms to embed data during decryption are applied.
- hence, the data is embedded in encrypted images and removed the data out of the encrypted images and restored the original image.

A Reserving Room Approach for Reversible Data Hiding Algorithm before Encryption on Encrypted Digital Images

In [6] Nimse Madhuri S etc. all, explains the RDH method had a great success in recovery of image with great success with minimal loss. Since, the method has high accuracy the resulting image has great accuracy and it is better than applying any other previously proposed methods. Not only it provides great accuracy it also provides great payloads i.e. It can support higher resolution of images and also larger amount of data for encryption.

Reversible Data Hiding in Encrypted Images by Reserving Room before Encryption with LSB Method

In [4] Sabeena O.M. etc. all, explains RDH provides a technique to restore or recover original cover image after data extraction. Unlike the previous methods which used to vacate the room after encryption the RDH technique reserves room before encryption .i.e. it provides encryption of both data and image before combining them and a layer of encryption again after combining them. This in a way provides multiple layer of encryption on the data and makes it extremely rigid .Image restored is free of errors and is as per desired or it is same as the sent data. The use of L.S.B gives more space to accommodate data into the image.

III. OBJECTIVE AND SCOPE

OBJECTIVE

The objective of this project is to provide an efficient data hiding technique and image Encryption in which the data and the image can be retrieved independently. The aim or objective of the project is to implement a reversible data hiding (RDH) technique in encrypted images. The proposed technique or method can achieve real reversibility, that is, data extraction and image recovery with minimum data loss.

SCOPE

RC4 is a stream cipher, symmetric key algorithm. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent of the plaintext used. It uses a variable length key from 1 to 256 bit to initialize 256-bit state table. The state table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream which is XORed with the plaintext to give the cipher text.

IV. PROPOSED SYSTEM

A system architecture or subsystem architecture is a conceptual model that defines the structural behaviour and more views of a system.

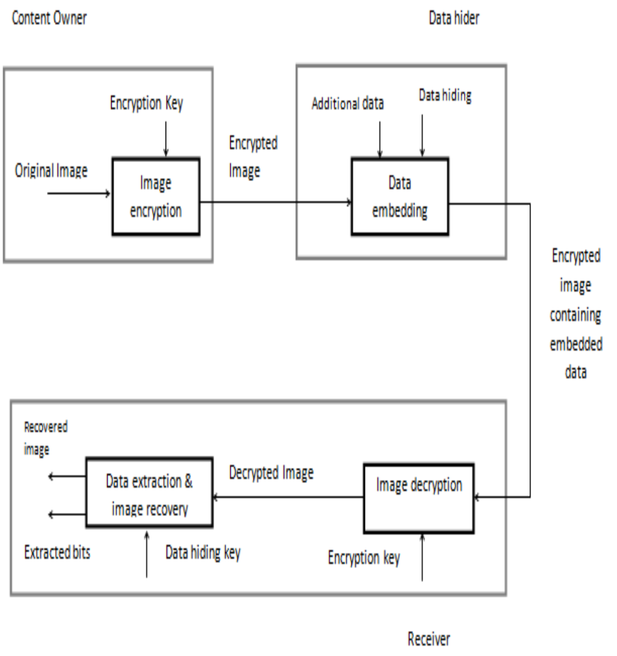


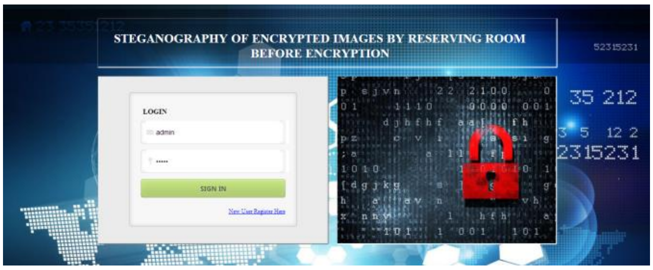
Fig 1. System Architecture

Proposed system will achieve real reversibility, that is, data extraction and image recovery with minimal error.

If we are 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 innovative framework Initially the data to be sent is selected along with the image used as a medium for transferring the data. The image and the data is encrypted separately followed by embedding of data into the image here by steganography takes place and the embedded data is encrypted as a whole. This encrypted data is then stored at the database of the server. The sender sends the decryption key of data and image.

The receiver on the other end uses the credentials provided by the sender to download the image .This image is decrypted and original data is retrieved along with the image.

V. RESULT

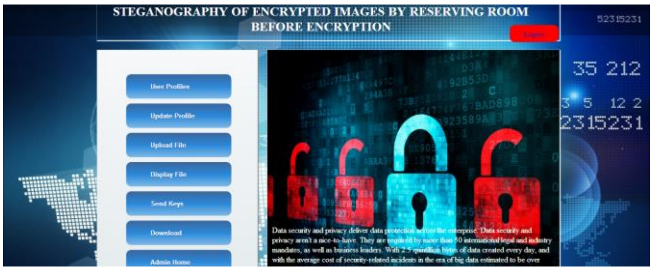

STEGANOGRAPHY OF ENCRYPTED IMAGES BY RESERVING ROOM BEFORE ENCRYPTION

LOGIN

admin

•••••

Fig 1. Login page


STEGANOGRAPHY OF ENCRYPTED IMAGES BY RESERVING ROOM BEFORE ENCRYPTION

Data security and privacy deliver data protection across the enterprise. Data security and privacy aren't a nice-to-have. They are required by more than 50 international legal and industry mandates, as well as business leaders. With 2.5 quintillion bytes of data created every day, and with the average cost of security-related incidents in the era of big data estimated to be over

Fig 2. Home page

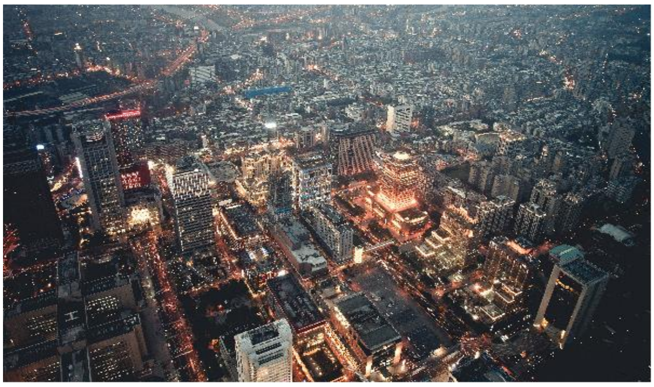


Fig 3. Embedded Image

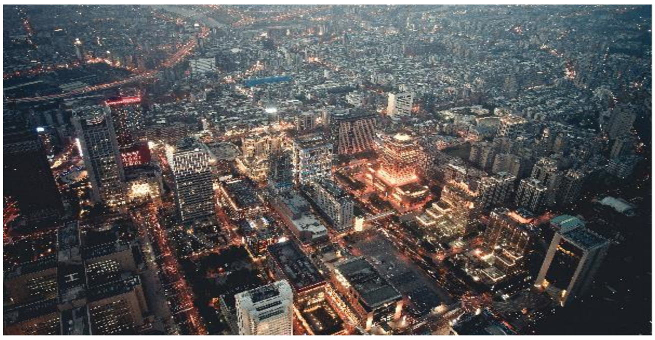


Fig 4. Decrypted Image

V. CONCLUSION

Pseudo random sequence consists of random bits generated using the encryption key. In our system, RC-4 algorithm is used to create the pseudo-random sequence using the 128-bitencryption key. The additional data inserted to encrypted image using the parameters. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain animate similar to the original one using only the encryption key. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the Spatial correlation in natural image. Compared with the other algorithms, the proposed system will give better accuracy in recovering the original images.

REFERENCES

[1]. N.Nagaraja Kumar, M.Sucharitha "Image Encryption and Iterative Reconstruction of an Encrypted Image," IJSR, vol. 2, Issue 12, December 2013.

[2]. Prasanth P.S. ,Anusree L "Lossy compression and Reconstruction of encrypted images," IJSCMC, ISSN 2320-088Xno. 4, , Dec 13-17 2013.

[3].William Puech, Marc Chaumont, Olivier Strauss. "A Reversible Data Hiding Method for Encrypted Images." IS&T/SPIE Electronic Imaging 2008 - Security, Forensics, Steganography , and Watermarking of Multimedia Contents, San Jose, CA, United States. SPIE/IS&T, 6819, pp.N/A, 2008.

[4]. Sabeena O.M., Rosna P. Haroon "Reversible Data Hiding in Encrypted Images by Reserving Room before Encryption with LSB Method" , IJCER ,vol 4, Issue 10, October 2014.

[5]Vijay Kumar Sharma , Vishal Srivastava in "A Steganography Algorithm For Hiding Image in Image Improved LSB by Minimize Detection" JATIT, vol.36,No.1,15th feb 2012.

[6] Nimse Madhuri S , Prof. D.D Ahire , Prof. P.M. Mahajan in "A Reserving Room Approach for Reversible Data Hiding Algorithm Before Encryption on Encrypted Digital Images" IJIRAE, vol 1,Issue 10,November 2014.

[7]Vimal, Mahendra Kumar Patil in "Reversible Data Hiding in Encrypted Images Using DCT", IJES, vol 3, Issue 3, June 2013.