IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

Reversible Data Hiding In Encrypted Images- An Overview

Mr. Dipak R Pardhi[1], Miss. Harshali Phalak[2]

HOD and Assistant Prof, Dept of Computer Engineering, Godavari College of Engineering and Technology, Jalgaon, Maharashtra, India[1]

Dept of Computer Engineering, Godavari College of Engineering and Technology, Jalgaon, Maharashtra, India[2]

Abstract: Reversible data hiding (RDH) has captured most of the attention in the field of encrypted images, RDH has ability to maintain the strong property that the original cover can be easily be recovered after embedded data is extracted while protecting the image content's confidentiality. Available methods embed data by reversibly vacating room from the encrypted images that leads to some errors on data retrieval and/or image recreation. In this paper, we propose a novel method by reserving image space before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility, that is, data retrieval and image recreation are free of any error. Experiments show that this novel method can embed more than 10 times as large payloads for the same image quality as the previous methods, such as for PSNR dB.

Keywords: Reversible data hiding, image encryption, privacy protection, histogram shift.

I. INTRODUCTION

Proposed is a method for image Steganography an area that deals with hiding some important message within the image so as to keep it safe while delivering to the another person. Image Steganography is a scientific methodology in which apart from sender and intended receiver no one knows about the existence of message. The message transmission from one person to another person has taken a huge step in the internet and cloud computing era. Some extra efforts has been made to make the communication more and more secured. The researcher are putting a lot of efforts in making the communication more simple while more secure so that unauthorized user does not get the access to the private messages. Reversible data hiding (RDH) in images is a technique, by which the original cover can be lossless recovered after the embedded message is extracted. One such method with novel approach has been proposed in this paper. The existing method that uses reversible data hiding in Image Steganography has some disadvantages as data extraction and recovery of image are free of errors. The PSNR will be improved to get original cover back. In future it may possible that memory space can be reserved before encryption which requires less amount of time for data extraction & image recovery. The existing system is achieving error because of division by 2 and due to bit replacement visual quality degrades. The existing system does not consider grey scale for designing recursive codes. The existing system has single level of security that can be improved in the proposed system. The method begins with the encryption of individual characters in the message to be send using the Morse methodology. The generated code then be used by reversible data hiding technique to generate the image to be mailed or given to the intended user and then the reverse decryption process starts in which the message first shall be extracted from image and then applying Morse decryption technique to regenerate the original message. This approach gives us several advantages one of which is proposed methodology cab be considered one of the most secured methodology for the message communication.

Fig 1: Text Contents in Image

II. RELATED WORK

The topic is one of the most favorite topics amongst the researchers and considered as most important as far as the security is concern while transmitting the data from one place to another using the digital media transfers. There has been already some work done in this regards. Few references are listed as below.

A] Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEE, Nenghai Yu, and Fenghua Li has published a paper

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

in titled "Reversible Data Hiding in encrypted Images by reversing room before encryption"[1] in IEEE Transactions and information forensics and security published in March 2013 stated about the important property that the original cover can losslessly removed after the embedded data is extracted while protecting the images's content security. This paper describes the elimination of errors caused due to vacating the room from the encrypted images. The paper simply modifies the approach for the traditional RDH algorithm to make it more secured and easy for the message retrieval while decrypting the images.

B] T Margaret of Satyabhama University Chennai India writes in his paper titled "Reversible Data Hiding In encrypted Images by XOR ciphering technique"[2] published in International Journal of Advanced Research in Electrical Electronics and Instrumental Engineer Vol 3 Isuue 2 of Feb 2014 about germinal concal can be losseslessly recovered after data is extracted from while keeping the original images security concerns as it is.

C] Dr. J Jagagadeesan, Mr. Balika Chelliha and Nichila Nyapathy in their paper "Reversible Data Hiding In Encrypted Images Using AES Data Encryption Technique"[3]
Reversible data hiding in images is a technique by which the original cover can losslossely recovered after the embedded messages are extracted .This important technique is widely used in medical imaginary ,military imaginary and law forensics ,where no distortion of original cover is allowed .since first introduced , RDH has attracted considerable research interest. In practical aspects, many RDH techniques have emerged in recent years. A more popular method is based on difference expansion (DE)[5],in which the difference of each pixel group is expanded and the least significant bit (LSBs)of the differences are all 0s and can be used for embedding messages.
To separate the data extraction from image decryption, emptied out space for data embedding following the idea of compressing encrypted images, Compression of encrypted data can be formulated as source coding with side information at the decoder, in which the typical method is to generate the compressed data in lossless manner by exploiting the syndromes of parity-check matrix of channel codes.

A. Notations And Definations

Morse Methodology:
Morse code is a method of sending text messages by keying in a series of electronic pulses, usually represented as a short pulse (called a "dot") and a long pulse (a "dash"). The code was devised by Samuel F. B. Morse in the 1840s to work with his invention of the telegraph, the first invention to effectively exploit electromagnetism for long-distance communication. The early telegrapher, often one who was at a railroad station interconnected with others along miles of telegraph pole lines, would tap a key up and down to send a succession of characters that the receiving telegrapher could read from tape (later operators learned to read the transmissions simply by listening). In the original version, the key down separated by a pause (key up) from the next letter was a dot (or, as it sounded to the telegrapher, a "dit") and the key down quickly twice in succession was a dash (a "dah" or "dit-dit"). Each text character was represented by a dot, dash, or some combination.
Morse code offers a slow but reliable means of transmitting and receiving wireless text messages through conditions involving noise, fading, or interference. This is primarily because its simple binary code (key down or key up) allows for an extremely narrow bandwidth. In addition, the human ear and brain make a remarkably good digital receiving device. Nowadays, Morse code is used to a limited extent by amateur radio operators, landline telegraphers, and military radio operators.

B. Digital Image Steganography

Hiding secret messages inside what seem to be harmless messages is nothing new. The word steganography itself originated in Greece and means "covered writing". During important historic events of our past, steganography was often used to trade personal secrets, plan covert operations and send political espionage information. For example, during World War II, the French Résistance used invisible ink on couriers' backs to send messages between Résistance cells. In Greece, people wrote secret messages on plain wood tablets and covered it with wax. Since wax tablets were popular reusable writing surfaces, the Greeks would simply carve an inconspicuous message into the wax and pass the tablet along. The moment the tablet reached its destination, the wax was melted to reveal the hidden message. Fortunately for all of us, steganography has gotten a lot easier to achieve and a lot harder to reveal: Enter digital Steganography

III. IMPLEMENTATION METHODOLOGY

Morse code is a method of transmitting text information as a series of on-off tones, lights, or clicks. Each character (letter or numeral) is represented by a unique sequence of dots and dashes. The duration of a dash is three times the duration of a dot. Each dot or dash is followed by a short silence, equal to the dot duration. The letters of a word are separated by a space equal to three dots (one dash), and the words are separated by a space equal to seven dots.

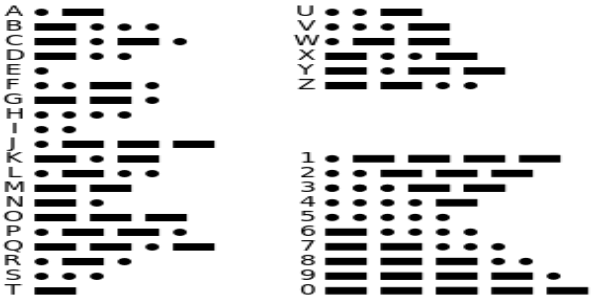

Fig 2: Character Representation in Morse Method

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

The method can be used to construct a set of code to be used to create a code for each and every individual character in the message. The encoding can be done in form of 8 bit value using binary representation. Following example shows the encryption in morse code that can be used in our technology as

11 111 010 000 0	**1010 111 100 1**	**By our method**
‒‒ ‒‒‒ ·‒· ··· ·	‒·‒· ‒‒‒ ‒·· ·	By Morse Code

M O R S E C O D E

Algorithm used in the proposed system

1. Generate Color Code for Each Character to be used inside the message using **Morse Code Message**
2. Input Text
3. Encrypt text using Encryption key and data hiding key with the help of PRIVATE KEY
4. For each of the character in encrypted text prepare a color band use of **Color Codes** defined in step 1
5. Generate new image with proposed color bands
6. Send mail or share it with new password inside it
7. Reverse way for decryption

PROJECT FLOW

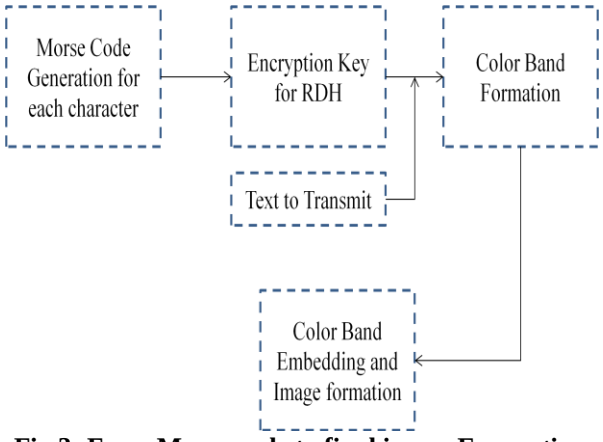

Fig 3: From Morse code to final image Encryption

The proposed method receives text information to be embedded inside the image as Steganography. The input text will be provided to morse code algorithm and digital code is generated for this digital code the an encryption key for reversible data hiding algorithm will be generated and this key will be used with the morse code generated digital data. The generated value will be provided to a color band generator the color band will then be embedded inside the original image. And the time of decryption first the color band from the image is extracted from color band an encrypted message will be extracted from this message the digital message will be extracted using the morse code decryption technique the original message shall be extracted.

IV. PROPOSED RESULTS

Message to Encrypted is Morse Code

(a) (b) (c) (d)

(a) Original Image
(b) Encrypted Image
(c) Encrypted Image Containing Message
(d) Recovery Vision of Image

The message I am encrypted is embedded inside the image will be embedded inside an image (a). The encryption will take place and a new image with color band will be generated (b). Newly created image data will be reversibly hidden inside the original image (c). A final image with data merged represents recovery image to be utilized to decrypt the original data.

V. CONCLUSION

With help of Morse code and the data encryption we can certainly secure the data to be sent over mail and allows user to communicate more secured way. The proposed technology shall only be helpful to the user to in many ways as to save the time and space within the image so that larger data can be stored within the images in most secured manner.

REFERENCES

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

[2] Reversible Data Hiding In Encrypted Images by XOR Ciphering Technique by T. Margaret PG Student [Embedded System], Dept of ECE, Sathyabama University, Chennai, Tamil Nadu, India1 published in International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 3, Issue 2, February 2014

[3] Reversible Data Hiding In Encrypted Images Using AES Data Encryption Technique by Dr. J Jagagadeesan, Mr. Balika Chelliha and Nichila Nyapathy in International Journal of Emerging Research in Management &Technology April 2014

[4] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.

[5] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896,Aug. 2003.

[6] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[7] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," IEEE Trans. Image Process., vol. 16, no. 3.