INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

RDH in Encrypted Images by Reserving Room before Encryption

Deepak Godse
Student (BE), Department of Computer, Shatabdi Institute of Engineering & Research, Nashik, Maharashtra, India
Suvarna Lokhande
Student (BE), Department of Computer, Shatabdi Institute of Engineering & Research, Nashik, Maharashtra, India
Madhuri Bhagwat
Student (BE), Department of Computer, Shatabdi Institute of Engineering & Research, Nashik, Maharashtra, India
Suyog Kandekar
Student (BE), Department of Computer, Shatabdi Institute of Engineering & Research, Nashik, Maharashtra, India

Abstract:
For several years, the protection of multimedia data is becoming very important. The protection of this multimedia data can be done with encryption or data hiding algorithms. To decrease the transmission time, the data compression is necessary. Recently, more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be Loss lessly recovered after embedded data is extracted while protecting the image contents confidentiality.
All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration.
In this project, we propose a novel method of reserving room 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 extraction and image recovery are free of any error.

Keywords: *Reversible data hiding, image encryption, privacy protection*

1. Introduction

In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. There are many possible ways to transmit data using the internet: via emails, chats, etc. The data transition is made very simple, fast and accurate using the internet. However, one of the main problems with sending data over the internet is the security threat it poses, i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore, it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring. Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data modification. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet In order to improve the security features in data transfers over the internet, many techniques have been developed like: Cryptography, Steganography. While Cryptography is a method to conceal information by encrypting it to cipher texts and transmitting it to the intended receiver using an unknown key, Steganography provides further security by hiding the cipher text into a seemingly invisible image or other formats.

1.1. Basic Concept

Since losslessly vacating room from the encrypted images is relatively difficult and sometimes inefficient, why are we still so obsessed with novel RDH techniques, working directly for encrypted images? If we reverse the order of encryption and vacating room, i.e., reserving room prior to image encryption on the content owner side, the RDH tasks on encrypted images would be more natural and much easier which leads us to the novel framework, reserving room before encryption (RRBE). The content owner first reserves enough space on the original image and then converts the image into its encrypted version with the encryption key. Now, the data embedding process in encrypted images are inherently reversible for the data hider only needs to accommodate data into the spare space previous emptied out. The data extraction and image recovery are identical to that of Framework VRAE. Obviously, standard RDH algorithms are the ideal operator for reserving room before encryption and can be easily applied to Framework RRBE to achieve

better performance compared with techniques from Framework VRAE. This is because in this new framework, we follow the customary idea that first losslessly compresses the redundant image content (e.g., using excellent RDH techniques) and then encrypts it with respect to protecting privacy. Next, we elaborate a practical method based on the Framework RRBE, which primarily consists of four stages: generation of encrypted image, data hiding in encrypted image, data extraction and image recovery. Note that the reserving operation, we adopt in the proposed method is a traditional RDH approach.
The data extraction and image recovery are identical to that of Framework VRAE.

1.2. Modules

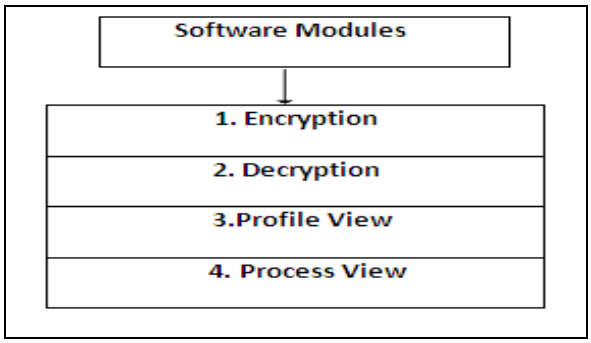

Figure 1: Modules

1.3. Applications

1. In Deductive Agencies
2. Consultancies
3. Bank Information Sharing's
4. Military purpose

2. Overview

Reversible Data hiding (RDH) in images is a technique, by which the original cover can be losslessly recovered after the embedded message is extracted. This important technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed. Since first introduced, RDH has attracted considerable research interest. In theoretical aspect, Kalker and Willems established a
rate-distortion model for RDH, through which they proved the rate-distortion bounds of RDH, for memory less covers and proposed a recursive code construction which, however, does not approach the bound. Zhang et al. improved the recursive code construction for binary covers and proved that this construction can achieve the rate-distortion bound as long as the compression algorithm reaches entropy, which establishes methods mentioned
above rely on spatial correlation of original image to extract data. That is, the encrypted image should be decrypted first before data extraction. To separate the data extraction from image decryption ,out space for data embedding. 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 a lossless manner by exploiting the syndromes of parity-check matrix of channel codes. The method in compressed the encrypted LSBs to vacate room for additional data by finding syndromes of a parity-check matrix, and the side information used on the receiver side is also the spatial correlation of decrypted images. All the three methods try to vacate room from the encrypted images directly.
We propose a novel method for RDH in encrypted images, for which we do not vacate the room after encryption but reserve room before encryption.

2.1. Existing System

In the existing system reversible data hiding technique the image is compressed and encrypted by using the encryption key and the data to hide is embedded into the image by using the data hiding key. On the receiver side, he first need to extract the image using the encryption key in order to extract the data and after that hell use data hiding key to extract the embedded data. It is a serial process and is not a separable process.

2.1.1. Limitation

1. Principal content of the image is revealed before data extraction.
2. If someone has the data hiding key, but not the encryption key he cannot extract any information from the encrypted image containing additional data.

3. Proposed System

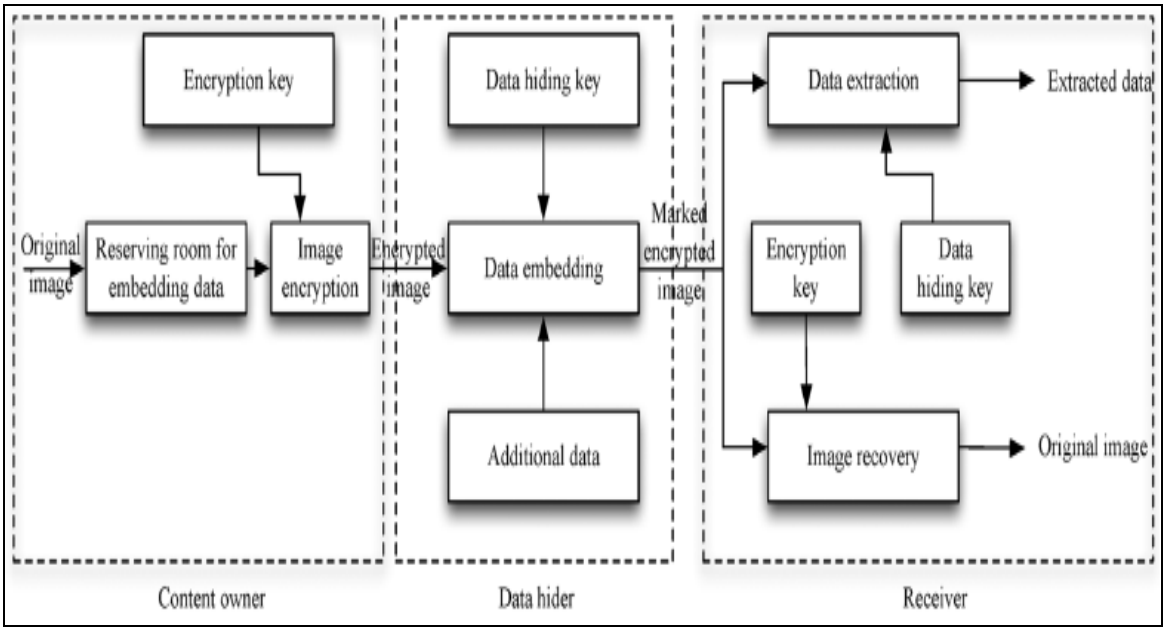

Figure 2: Proposed System Architecture

We elaborate a practical method based on the Framework RRBE, which primarily consists of four stages: generation of encrypted image, data hiding in encrypted image, data extraction and image recovery. Note that the reserving operation, we adopt in the proposed method is a traditional RDH approach.

3.1. If the Receiver Has Only the Data-Hiding Key, He Can Extract the Additional Data, though He Does Not Know the Image Content

Once the data hider acquires the encrypted image, he can embed some data into it, although he does not get access to the original image. The embedding process starts with locating the encrypted version of, denoted by. Since has been rearranged to the top of, it is effortless for the data hider to read 10 bits information in LSBs first 10 encrypted pixels. After knowing how many bit-planes and rows of pixels he can modify, the data hider simply adopts LSB replacement to substitute the available bit-planes with additional data. Finally, the data hider sets a label following to point out the end position of embedding process and further encrypts according to the data hiding key to formulate marked encrypted image denoted by. Anyone who does not possess the data hiding key could not extract the additional data.

3.2. If He Has Only the Encryption Key, He Can Decrypt the Received Data to Obtain an Image Similar to the Original One, but Cannot Extract the Embedded Additional Data

Both embedding and extraction of the data is manipulated in encrypted domain. On the other hand, there is a different situation that the user wants to decrypt the image first and extracts the data from the decrypted image when it is needed. The following example is an application for such scenario. Assume Alice outsourced her images to a cloud server, and the images are encrypted to protect their contents. Into the encrypted images, the cloud server marks the images by embedding some notation, including the identity of the images owner, the identity of the cloud server and time stamps, to manage the encrypted images. Note that the cloud server has no right to do any permanent damage to the images. Now an authorized user, Bob who has been shared the encryption key and the data hiding key, downloaded and decrypted the images. Bob hoped to get marked decrypted images, i.e., decrypted images still including the notation, which can be used to trace the source and history of the data. The order of image decryption before/without data extraction is perfectly suitable for this case.

4. Conclusion

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 emptied out in previous stage to make data hiding process effortless. 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.

5. Acknowledgement

With all respect and gratitude, we would like to thank all people who have helped us directly or indirectly for the completion of this project work.

We express our heartily gratitude towards Prof. S. G. Chordiya, for guiding us to understand the work conceptually and also for his constant encouragement to complete this Project work on "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption".

We also express our thanks to Prof. C.N.Patki Head of department of Computer Engineering for providing necessary information and required resources. With deep sense of gratitude we thank to our Principal Dr. D. P. Joshi and management of the SIER, Agaskhind for providing all necessary facilities and their constant encouragement and support.

6. References

1. T. Kalker and F.M.Willems, Capacity bounds and code constructions for reversible data-hiding, in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp.7176.
2. W. Zhang, B. Chen, and N. Yu, Capacity-approaching codes for reversible data hiding, in Proc 13th Information Hiding (IH2011), LNCS 6958, 2011, pp. 255269, Springer Verlag
3. K. Hwang and D. Li, Trusted cloud computing with secure resources and data coloring, IEEE Internet Comput., vol. 14, no. 5, pp. 1422, Sep./Oct. 2010.
4. L. Luo et al., Reversible imagewatermarking using interpolation technique, IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187193, Mar. 2010.
5. P. Tsai, Y. C. Hu, and H. L. Yeh, Reversible image hiding scheme using predictive coding and histogram shifting, Signal Process., vol.89, pp. 11291143, 2009.
6. X. L. Li, B. Yang, and T. Y. Zeng, E_cient reversible watermarking based on adaptive prediction-error expansion and pixel selection,IEEE Trans. Image Process., vol.20, no. 12, pp. 35243533, Dec.2011.
7. Application Notes[Online], Available: http://www.maxim-ic.com/an1490
8. D.M. Thodi and J. J. Rodriguez, Expansion embedding techniques for reversible watermarking, IEEE Trans. Image Process., vol. 16, no. 3,pp. 721730, Mar. 2007.
9. W. Hong, T. Chen, and H.Wu, An improved reversible data hiding in encrypted images using side match, IEEE Signal Process. Lett., vol.19, no. 4, pp. 199202, Apr. 2012.
10. M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K.Ramchandran, On compressing encrypted data, IEEE Trans. Signal Process., vol. 52, no. 10, pp.29923006, Oct. 2004.