ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 380 - 384 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

An Efficient Reversible Data Hiding Technique using Reserving Room before Encryption for Data Hiding in Encrypted Images

[1]**P.SHAKIRA**, [2]**Dr.P.HARINI**
[1]II year M.Tech, St.Ann's College of Engineering & Technology,India,shakiravunissa@gmail.com
[2]Professor and HOD dept. of CSE, St.Ann's College of Engineering & Technology, India, hpogadadanda@gmail.com

ABSTRACT*:* From the time when few years, the safety of multimedia data is becoming very important. The safety of this multimedia data can be done with encryption or data hiding algorithms. To decrease the transmission time, where data compression is necessary. Since few years, a very new problem is trying to combine into a single step that is compression, encryption and data hiding. So far, a few solutions have been proposed to combine image encryption and compression for example. Currently, a novel test consists to embed data in encrypted images. Since the entropy of the encrypted image is maximal, also the embedding step, considered like noise, is not possible by using the standard data hiding algorithms. A latest idea is to affect reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. Recently more and more awareness is paid to reversible data hiding (RDH) in encrypted images, since it maintains the good property that the original cover can be lossless recovered after embedded data is extracted while protecting the image content's privacy. All previous methods embed data by reversibly vacating room from the encrypted images, which may leads to subject for some errors on data extract ion and/or image restoration In this paper, we propose a new method by reserving room before encryption with a conventional RDH algorithm, and thus it is very easy and popular for the data hider to reversibly embed data in the encrypted image.

Key words: Reversible data hiding, keyless image encryption, privacy protection, data extraction.

INTRODUCTION

The amount of digital images has increased rapidly on the Internet. Where Image security becomes increasingly important for many applications, e.g., for confidential transmission, for video surveillance, military and also for medical applications. Consider an example that, the necessity of fast and secure analysis is vital in the medical world. In these days, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over networks. To reduce the transmission time, the data compression is necessary. The security of this multimedia data can be done with encryption or data hiding algorithms. Since few years, where a problem is to try to combine compression, encryption and data hiding into a single step.

Nowadays, a new challenge consists to embed data in encrypted images. Previous works have proposed to embed data in an encrypted image by using a data hiding's irreversible approach. The challenge was to find an encryption method robust to noise. Since here the entropy of encrypted image is maximal, and the embedding step, considered like noise, is not absolutely possible by using standard data hiding algorithms. Here a new idea is to apply reversible data hiding algorithms on encrypted images by taking forward to remove the embedded data before the image decryption. Recently reversible data hiding (RDH) methods have been proposed with high capacity, but these methods are not at all applicable on encrypted images.

There are also a number of efforts on data hiding in the encrypted domain. Which the reversible data hiding in encrypted image is to be investigated in. Mostly the work on the reversible data hiding focuses on the data embedding/extracting on the plain spatial domain. This method by reserving room before encryption with a traditional RDH algorithm, and thus it is the easiest part for the data hider to reversibly embed data in the encrypted image.

Where the proposed method can achieve real reversibility, that is the data extraction and the image recovery are of free of any error. Thus the data hider can be benefited from the extra space Emptied out in previous stage to make data hiding process as effortless. This proposed method can take advantage of all regular and traditional RDH techniques for plain images and achieve excellent performance without any loss of perfect secrecy.

Reversible data hiding (RDH) is a technique in image processing area for encryption, by which the original cover can be losslessly recovered after the embedded message is extracted. The RDH approach is widely used in medical science, defense field and forensic lab, where there is no degradation of the original content is allowed. Since more research RDH method in recently. In theoretical aspect rate-distortion model for RDH Kalker and Willems, 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. 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, where it establishes the equivalence between data compression and RDH for binary covers

A various RDH method is more popular is based on difference expansion (DE), in which the difference of

each pixel group is expanded by various method or technique. Example, multiplied by 2, and thus the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages Another reliable strategy for RDH is histogram shift (HS), in which space is saved for data embedding by shifting the bins of histogram of gray values.
With respective to providing confidentiality for images, the encryption is an effective and also popular which means as it converts the original and meaningful content to non-readable one. Although there are few RDH techniques in encrypted images have been published yet, where there are some promising applications if RDH can be applied to encrypted images. To separate the data extraction from image decryption, it emptied out space for the data embedding following the idea of compressing encrypted images, where Compression of encrypted data can then be formulated as source coding with side information at the decoder, in which the typical method is to be generated for the compressed data in lossless manner by exploiting the syndromes of parity -check matrix of channel codes. Hereafter the method in compressed the encrypted LSBs to vacate room for additional data.

Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a reversible manner with which that the original cover content can be perfectly restored after extraction of the hidden message. As an effective and popular means for a privacy protection, then the encryption converts the ordinary signal into incomprehensible data, so that the very general signal processing typically takes place before encryption or after decryption However, in some circumstances that a content owner does not trust the service provider, with the ability to manipulate the encrypted data when keeping the plain content secret is desired. When the high secret data to be transmitted are encrypted, then a channel provider without any knowledge of the cryptographic key may compress the encrypted data due to the limited channel resource.

RELATED WORK

1. In the existing System more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent and good property that the original cover can be lossless Recovered after embedded data is extracted while protecting the image content's confidentiality.

2. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some of the errors on data extraction and/or image.
3. . Previous methods implement RDH in encrypted images by vacating room after encryption, as it was opposed to which we proposed by reserving room before encryption. Thus the data hider can be benefited from the extra space emptied out in previous stage to make data hiding process effortless.

The architecture of the existing system will contain 3 modules. They are Content owner, Data Hider, Receiver.

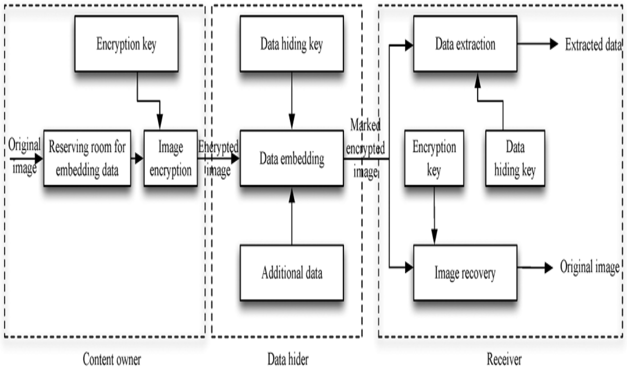


Fig:1.Architecture of existing system i.e Reserving room before encryption key.

DISADVANTAGES

1. The attackers recover the embedding data in original image because the data placed in particular bit position.
2. Previous methods embed data by reversibly vacating room from the encrypted images, which may leads for being subject to some errors on data extraction and/or image restoration.
3. To attack the hidden data using original image because referred the key value.

In all methods of, the encrypted 8-bit gray-scale images are generated by encrypting every bit-plane with a stream cipher. The method in which it segments the encrypted image into a number of no overlapping blocks size x*x each block is used to carry one additional bit.

PROPOSED METHOD

Vacating room from the encrypted images losslessly is relatively difficult and also sometimes inefficient. Thus, we reverse the order of encryption and vacating room, i.e. reserving room is to be prior to image encryption at content owner side, then the RDH tasks in encrypted images would be more natural and are much easier which leads us to this framework,

"The Reserving Room Before keyless Encryption". Which was shown in Fig. 2, the content owner first reserves enough space on original image and then converts the image into its encrypted version with the encryption key. The data embedding process in encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space previous emptied out. The P LSB-planes of each and every group are being compressed with the parity-check matrix and then the vacated room is used to embed the data.

For an instance, denoting the pixels of one group by $X_1 \ldots X_*$, and its encrypted answer LSB-planes by that which consists of P. Actually we are giving an original image which can reserve room for embed data then the data embed in the form of secret data(decode form),where the image encryption need not use any key for that of encrypting the image this is the module for transmitter and coming to the receiver, he can decrypt the image with keyless decode and then image extracts later data recover will be done by this proposed system.

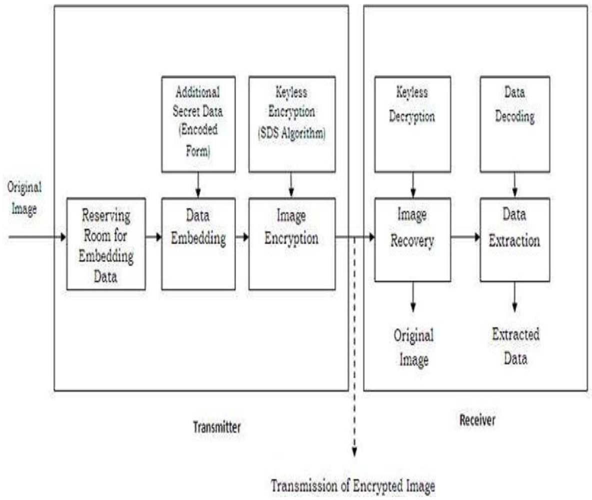


Fig:2.Architecture of reserving room for embedding with additional secure data before encryption.

Where the data extraction and image recovery are an identical to the Framework VRAE.

Where standard RDH algorithms are the ideal operator for reserving room before encryption and can be easily applied to Framework RRBE to provide better performance as compared with techniques from Framework VRAE. This is because for this new framework, we are following the customary idea that which first losslessly compresses the redundant image content (e.g., using excellent RDH techniques) and encrypts it with respect to protecting the privacy. Next, we elaborate a practical method based

on the Framework "RRBE", which primarily consists of four stages: generation of encrypted image, and data hiding in encrypted image, data extraction by keys and image recovery. Note that the reserving operation that we adopt in the proposed method is nothing but a traditional RDH approach.

IMPLEMENTATION ISSUES

The proposed approach can be tested on the public available Standard images, which of that will include "1st image 1.image", "2nd image 2.image", "3rd is 3.image", "4th is 4.image", "5th is 5.image" and "6th is 6.image". Here the sizes of all images are 512 X 512 X 8. Where the objective criteria PSNR is to be employed to evaluate the image quality of marked decrypted image quantitatively

The new idea about reversible data hiding in encrypted image without loss can be achieved by proposed system. Reserving room before encryption in this we first losslessly compress the redundant image and then encrypts it with respect to maintain privacy the implementation is carried ways.

A) Reserving room,
B) Encryption key,
C) Data hiding key.

The following shows the different ways/modules of Reversible data hiding Technique using Reserving Room before Encryption for Data Hiding in Encrypted Images is

A. **Reserving Room**

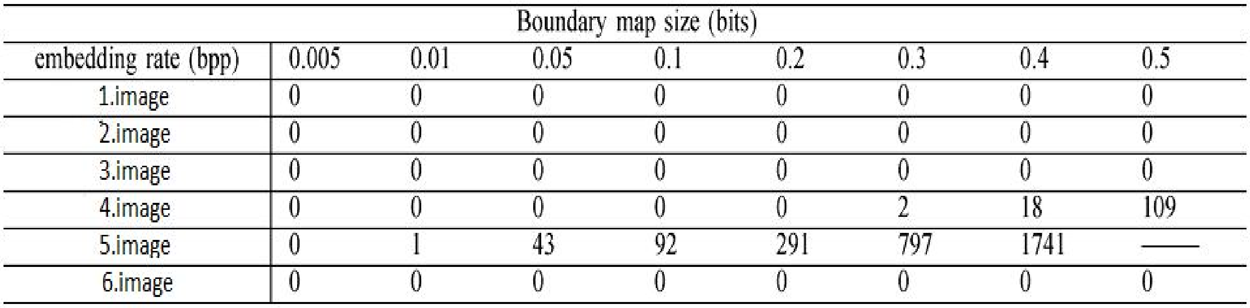
In this we first empty out room i.e. creating space in the image before encryption of image the RDH task in encrypted image would be more natural and much easier and real reversibility is realized this can be achieved by first losslessly compress the redundant data of image in this way space is created for embedding data and then encrypts the image by different encryption technique.

B. **Encryption Key**

This key is present at the content owner side. where the content owner firstly reserves enough space on original image and then encrypts the original image using standard cipher with an encryption key and then after producing the encrypted image the content owner hands over to database manager or any third party.

Table:I

Length of boundary maps under different data embedding rates



	Boundary map size (bits)							
embedding rate (bpp)	0.005	0.01	0.05	0.1	0.2	0.3	0.4	0.5
1.image	0	0	0	0	0	0	0	0
2.image	0	0	0	0	0	0	0	0
3.image	0	0	0	0	0	0	0	0
4.image	0	0	0	0	0	2	18	109
5.image	0	1	43	92	291	797	1741	——
6.image	0	0	0	0	0	0	0	0

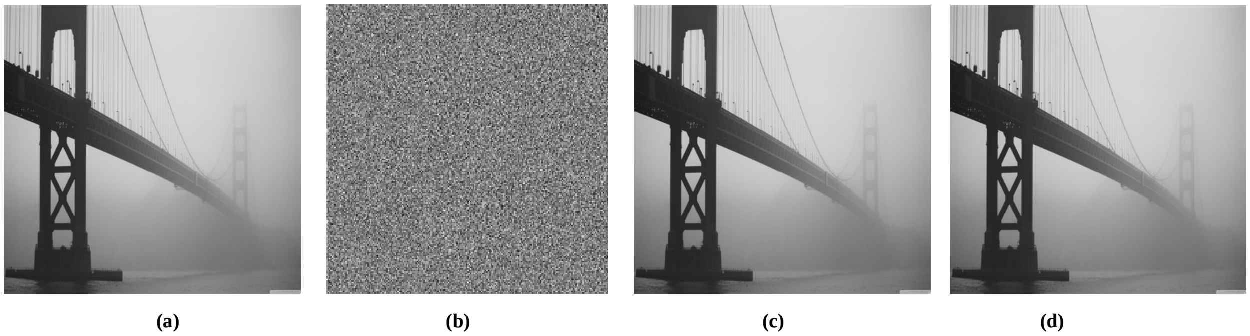

(a) **(b)** **(c)** **(d)**

Fig. 3. (a.) Original image, (b.) Encrypted image with embed data, (c.) Decrypted image containing messages, (d.) Recovery version.

C. **Data Hiding Key**

This key is present at the data hiding center as well as receiver side the data hider can embed some auxiliary data into the encrypted image according to the data hiding key. The receiver maybe the content owner himself or can be an authorized party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to encryption key

The proposed scheme is made up of 4 phases: image encryption phase, data embedding phase and data extraction phase, image-recovery phase. The owner of the content encrypts the original uncompressed image using an encryption key to produce an encrypted image. Where, the data-hider will compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the data provided additionally. At the receiver side, the data is embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding which only affects the LSB, a decryption with which the encryption key can result in an image similar to the original version. By using both of the encryption and data-hiding keys, the embedded and also additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image.

When having an encrypted image containing the embedded data, then the receiver firstly generates the ri, j, k according to the encryption key, and then calculates the exclusive-or of the received data and here ri, j, k to decrypt the image. We denote that the decrypted bits as bri j and k. Clearly, the original five most significant bits (MSB) are retrieved correctly.

Here in this Table I: the boundary maps under different data embedding rates are to be shown which shows that some pics like 1.image, 2.image and so on, which we are just taking for our reference where coming to boundary mapping it is used for differentiating between natural and also pseudo boundary pixels well and its size is critical for practical applicability of proposed approach. Table I which shows the boundary map size for six standard images. In this the most cases, no boundary map is to be needed. Even for 5.image, the largest size will be 1741 bits (with a large embedding data rate 0.4 bpp by adopting these embedding scheme 4 rounds) and then the marginal area (bits.) is large enough for accommodating it.

For a certain pixel, if the embedded bit in the block including the pixel is zero and the pixel belongs to the S1, or if the embedded bit is to be 1 and the pixel belongs to S0, the data-hiding does not effect on any encrypted bits of the pixel. So, then the three decrypted LSB must be same as the original LSB, which is implying that the decrypted gray value of the pixel is correct. On the other side, if the embedded bit in the pixel's block is 0 and the pixel belong to S0, or the embedded bit is 1 and the pixel belongs to S1which is decrypted LSB.

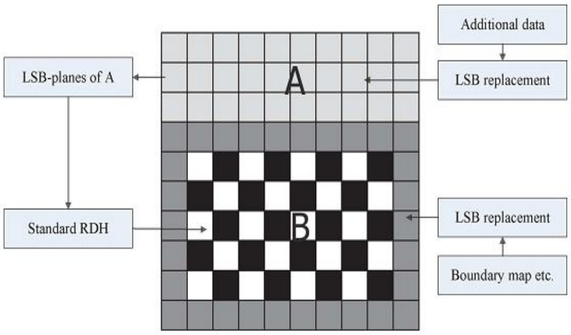


Fig 4.Image partitioning and embedding process using RDH.

The above discussion which implicitly relies on the fact of that only single LSB-plane of **A** is recorded. It is straight forward that the content owner can also embed two or more LSB-planes of **A** into **B**, which leads to half, or more than that of half, reduction in the Size of **A**. However, the better performance of **A**, in terms of the PSNR.

After data embedding in the second stage decreases significantly with growing bit-planes exploited. Therefore, in this paper, we investigate situations that at most three LSB-planes of are employed and determine the number of bit-plane with regard to different payloads experimentally in the next section.

This project proposes a novel scheme for separable reversible data hiding in encrypted image. In the proposed scheme, where the original image is encrypted using an encryption key and the additional data are embedded into the encrypted image using a data-hiding key. And with an encrypted image containing additional data, if the receiver having only the data-hiding key, then he can extract the additional data though he does not know the image content. If he contains only the encryption key, then he can decrypt the received data to obtain an image similar to the original one, but they cannot extract the embedded additional data. If the receiver having both the data-hiding keys and then also the encryption keys, where he can then extract the additional data into image and finally can recover the original image without any error when the amount of additional data is not too large.

EXPERIMENTS AND COMPARISONS

We have taken standard image shown in Fig. 3(a), to Demonstrate the feasibility of our proposed method. Fig. 3(b) is considered that the encrypted image containing embedded messages and the image was also partitioned and where the decrypted version of 3(a) with messages is illustrated in Fig. 3(c). And Fig. 3(d) depicts the recovery version of image which is very identical to original image with no loss.

In fact, where the proposed method can also embed more than 10 times per as large as payloads for that of the same acceptable PSNR. (e.g., PSNR=40 dB) as the models in [16]–[18], which implies a better potentiality for the practical applications.

CONCLUSION

Finally the Reversible data hiding based on reserving room before encryption is a novel method for hiding the data in image using encryption and data hiding keys to secure transfer of original data from the content owner to the receiver. For improving the security level, using a password in this phase of data hiding and data taking out processes. Based on the single password protocol.

The future implementation is to add support to hide all file formats. This will always allow for a much broader spectrum of usage: one would be able to encode .exe, .doc, .pdf, .mp3, etc. The system would be more versatile because often hiding text just isn't enough.

REFERENCES

[1] 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. 2992-3006, Oct. 2004.

[2] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354-362, Mar.2006.

[3] C.-C. Chang, C.-C.Lin, and Y.-H. Chen, "Reversible data-embedding scheme using differences between original and predicted pixel values, "IET Inform. Security, vol. 2, no. 2, pp.35-46, 2008.

[4] T. Bianchi, A. Piva and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inform. Forensics Security, vol. 4, no. 1, pp. 86-97, Feb. 2009.

[5] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted gray scale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097-1102, Apr. 2010.

AUTHORS:

Patan Shakira received the B.Tech degree in Information Technology from JNTU Kakinada, in 2012.She is currently working toward the Master Degree at the JNTU Kakinada. Her research interests include Image processing, Data hiding, and also networking.

Dr. P. Harini is presently working as a professor and HOD, Dept. of Computer Science and engineering, in St. Ann's College of Engineering and Technology, Chirala. She obtained Ph.D. in distributed and Mobile Computing from JNTUA, Ananthapur. She Guided Many UG and PG Students. She has More than 18 Years of Excellence in Teaching and 2 Years of Industry Experience. She published more than 20 International Journals and 25 Research Oriented Papers in Various Areas. She was awarded Certificate of Merit by JNTUK, Kakinada on the University Formation Day on 21 - August - 2012.