International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Reversible Encrypted Data Concealment in Encrypted Images by Reserving Room approach for Data Protection System

Sunayana A. Sutar[1], Ashish A. Zanjade[2]

[1]Master Student, Electronics and Telecommunication, YTIET, Karjat, India

[2]Professor, Electronics and Telecommunication, YTIET, Karjat, India

Abstract: ***The reversible encrypted data concealment in encrypted images is used to hide encrypted data in encrypted images for secret communication which has very high security. The project proposes the enhancement of protection system for secret data communication through encrypted data concealment in encrypted images. The image is then separated into number of blocks locally and lifting wavelet transform will be used to detect approximation and detailed coefficients. Then approximation part is encrypted using chaos encryption. After image encryption, the data hider will hide the secret data into the detailed coefficient which are reserved before encryption. The data hiding technique uses the adaptive LSB replacement algorithm for concealing the secret message bits into encrypted image. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of errors.***

Keywords: Reversible, Data Concealment, Image Encryption

1. Introduction

Reversible data hiding in images is a technique, by which the original cover can be lossless, recovered after the embedded message is extracted. This important technique is used drastically in medical imagery, military imagery and law forensics, where no disturbance of the original cover is to be achieved. Regarding providing confidentiality for images, encrypting the data is an effective and familiar means as it converts the original and significant to inexplicable one. Although few reversible data hiding (RDH) techniques in encrypted images have been introduced yet, there are some promising applications if RDH can be applied to encrypted images. A reversible data coloring technique based on encrypted data is preferred. Suppose a medical image data-base is stored in a data centre, and a server in the data centre can embed notations into an encrypted version of a medical image through a RDH technique. A person, who is having the decrypting key, can relocate the image in a reversible manner for the purpose of further diagnosing by using the process in the reversible manner.

The project proposes the enhancement of protection system for secret data communication through encrypted data concealment in encrypted images. The image is then separated into number of blocks locally and lifting wavelet will be used to detect approximation and detailed coefficients. Then approximation part is encrypted using chaos encryption method. The proposed encryption technique uses the key to encrypt an image and not only enhances the safety of secret carrier information by making the information inaccessible to any intruder having a random method. After image encryption, the data hider will conceal the secret data into the detailed coefficients which are reserved before encryption. Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural or meaningless. This system is still enhanced with encrypt messages using an asymmetric key method. This is the reason a new security approach called reversible data hiding arises. It is the art of hiding the existence of data in another transmission medium to achieve secret communication. The data hiding technique uses the adaptive LSB replacement algorithm for concealing the secret message bits into the encrypted image. In the data extraction module, the secret data will be extracted by using relevant key for choosing the encrypted pixels to extract the data. By using the decryption keys, the image and extracted text data will be extracted from encryption to get the original information. Finally the performance of this proposal in encryption and data hiding will be analyzed based on image and data recovery.

2. Proposed System

The proposed novel method for RDH in encrypted image is encryption after allocating some space. In the proposed method, we first empty out room by embedding LSBs of some pixels into other pixels with a traditional RDH method and then embed the image with some data, so the positions of the bits in the encrypted image can be used to embed data. Real data hiding with data concealment is realized, that is, data extraction and image recovery are free of any error. For given embedding rates, the PSNR so encrypted image containing the embedded data can be improved and for the satisfactory error occurrences, the range of embedding rate is greatly enlarged.

The method in segments the encrypted image into a number of non-overlapping blocks sized by each block is used to carry one additional bit. To do this, pixels in each block are gathered and divided into two sets and according to a data hiding key. For data extraction and image recovery, the receiver alters the pixels in to a new decrypted block. One of them will be decrypted to the original block. Due to spatial correlation in natural images, original block is presumed to

be much smoother than interfered block and embedded bit can be extracted correspondingly. Moreover, there is a problem in bit extraction and image recovery when divided block is relatively small or has much detailed textures.

The new framework "Reserving room before encryption" Since losslessly vacating room from the encrypted images is relatively difficult and sometimes inefficient, 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)" [1].

In order to effectively realize digital image encryption and decryption, two one-dimensional discrete Chebyshev chaotic sequences are used for row and column scrambling of the pixels of original and encrypted digital images. Experiment results shows that the encrypting algorithm is reasonably feasible and effective, and can ensure encrypted images sufficient security in their storage and transmitting processes.

3. Ideas of the Proposed Method

The proposed method uses Data Protection system for secret data transmission based on, Reversible encrypted data concealment in encrypted images using chaos encryption, Asymmetric key encryption and adaptive least significant bit replacement technique. The basic steps of the proposed algorithm are shown in the following figure 4.1 and figure 4.2.

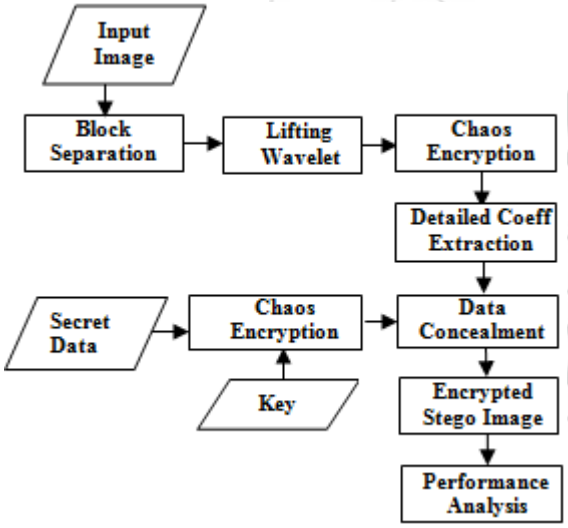

Figure 1: A block diagram of Encryption and Embedding system.

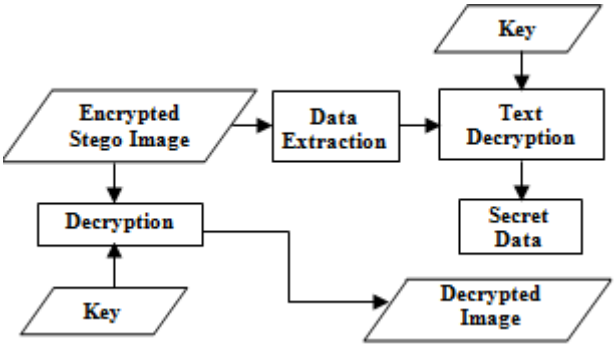

Figure 2: A block diagram of Decryption and Data Extraction system.

3.1 Reversible Data Hiding

Data hiding is referred to as a process to hide data (representing some information) into cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data. The relationship between these two sets of data characterizes different applications. For instance, in covert communications, the hidden data may often be irrelevant to the cover media. In authentication; however, the embedded data are closely related to the cover media .In these two types of applications, invisibility of hidden data is an important requirement. In most cases of data hiding, the cover media will experience some distortion due to data hiding and cannot be inverted back to the original media. That is, some permanent distortion has occurred to the cover media even after the hidden data have been extracted out. In some applications, such as medical diagnosis and law forcement it's critical to reverse the marked media back to the original cover media after the hidden data are retrieved for some legal considerations. In other applications, such as remote sensing and high-energy particle physical experimental investigation, it is also desired that the original cover media can be recovered because of the required high-precision nature. The marking techniques satisfying this requirement are referred to as reversible, lossless, distortion-free, or invertible data hiding techniques. Reversible data hiding facilitates immense possibility of applications to link two sets of data in such a way that the cover media can be losslessly recovered after the hidden data have been extracted out, thus providing an additional avenue of handling two different sets of data.

3.2 Lifting Wavelet Transform

This technique is used to reserve the space for hiding data with minimum distortion. LWT decomposes the image into different sub-band images, namely, LL, LH, HL, and HH for embedding the messages in the pixel coefficients of sub-bands. Lifting scheme is a technique to convert DWT coefficients to Integer coefficients without losing information .LL sub-bands contains the significant part of the spatial domain image. High-frequency sub-band contains the edge information of input image. These coefficients are selected as reserved space foe hiding the text data. The secret text data is embedded into the wavelet coefficients of high frequency sub-bands because it is non sensitive to human visual system.

Basically we use Wavelet Transform (WT) to analyze non-stationary signals, i.e., signals whose frequency response varies in time, as Fourier Transform (FT) is not suitable for such signals

2-D wavelet transforms

The 1-D DWT can be extended to 2-D transform using separable wavelet filters. With separable filters, applying a 1-D transform to all the rows of the input and then repeating on all of the columns can compute the 2-D transform. When one-level 2-D DWT is applied to an image, four transform coefficient sets are created. As depicted in figure 4.3(c), the four sets are LL, HL, LH, and HH, where the first letter corresponds to applying either a low pass or high pass filter

to the rows, and the second letter refers to the filter applied to the columns.

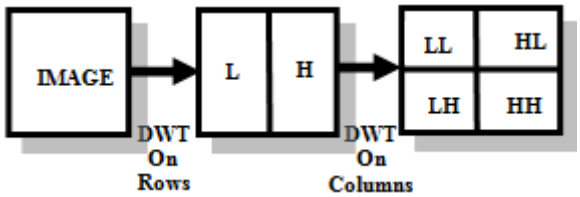

Figure 3: Block Diagram of DWT (a) Original Image (b) Output image after the 1-D applied on Row input (c) Output image after the second 1-D applied on row input.

The Two-Dimensional DWT (2D-DWT) converts images from spatial domain to frequency domain. At each level of the wavelet decomposition, each column of an image is first transformed using a 1D vertical analysis filter-bank. The same filter-bank is then applied horizontally to each row of the filtered and sub sampled data. One-level of wavelet decomposition produces four filtered and sub sampled images, referred to as sub bands. The upper and lower areas of figure 3(b), respectively, represent the low pass and high pass coefficients after vertical 1D-DWT and sub sampling. The result of the horizontal 1D-DWT and sub sampling to form a 2D-DWT output image is shown in figure 3(c).

3.3 Image Encryption

In proposed system for encryption of data and image we have used Chaos Crypto system

- This method is one of the advanced encryption standard to encrypt the image for secure transmission.
- It encrypts the original image pixel values with encryption key value generated from chaotic sequence with threshold function by bit-XOR operation
- Here logistic map is used for generation of chaotic map sequence.
- It is very useful to transmit the secret image through unsecure channel securely which prevents data hacking.
- The chaotic systems are defined on a complex or real number space called as boundary continuous space.
- Chaos theory generally aims that to recognize the asymptotic activities of the iterative progression.
- The properties essential for chaotic systems designed for cryptography is sensible to an initial condition with topology transitivity.

3.4 Adaptive LSB Embedding

The least-significant-bit (LSB) is the most widely used spatial domain data hiding technique. It generally embeds the same amount of data as the LSB pixels. Least significant bit (LSB) is one of the simplest techniques that hide a secret message in the LSBs of pixel values without introducing many perceptible distortions.

An 8 - bit gray scale image matrix consisting m x n pixels and a secret message consisting of k bits. The first bit of message is embedded into the LSB of the first pixel and the second bit of message is embedded into the second pixel and so on. The resultant Stego-image which holds the secret message is also 8-bit gray scale image and difference between the cover image and the Stego-image is not visually perceptible.

The quality of the image however degrades with the increase in number of LSBs. This hiding process will introduce the error between input and output image and it is determined by mean square error and Peak signal to noise ratio determines the image quality.

LSB substitution replaces the least significant bit with a secret bit stream. Least significant bit (LSB) insertion is a simple approach for embedding information in a cover image. The least significant bit (i.e. the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. In 24-bit image, a bit of each of the green, red and blue color components can be used,
Performance Parameters Evaluation:

To retain the image quality and provide a stronger robustness and security of a dual image steganography scheme, the statistical parameters are further considered. The value of statistical parameters not only reduces the image perceptibility but also enhances the robustness to resist attacks. We used PSNR and MSE to measure the distortion between the original cover image and the steganographic image.

3.5 Performance Parameters

1. Mean Square Error (MSE): The distortion in the image can be measured using MSE and is calculated using Equation MSE can be defined as the measure of average of the squares of the difference between the intensities of the steganographic image and the cover image. It is popularly used because of the mathematical tractability it offers.

2. Peak Signal to Noise Ratio (PSNR): It is the measure of the quality of the image by comparing the cover image with the stego image, i.e., it measures the statistical difference between the cover and Stego image. The PSNR depicts the measure of reconstruction of the transformed image. This metric is used for discriminating between the cover and stegno image.

3. Capacity: It is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image. The steganography embedding operation needs to preserve the statistical properties of the cover image in addition to its perceptual quality. Therefore capacity depends on total number of bits per pixel & number of bits embedded in each pixel. Capacity is represented by bits per pixel (bpp) and the Maximum Hiding Capacity (MHC) in terms of percentage.

4. Algorithm of the Proposed Method

Based on the proposed method, the algorithms for reversible data concealment of encrypted data in encrypted image and decrypted data extraction from decrypted image may describe respectively as Algorithm 1 and 2.

Algorithm 1: Reversible data concealment of encrypted data in encrypted image.

Input: A cover image i, text file f, and encryption key K.
Output: A stego encrypted image.

Steps:

Stage 1. **Reserving Coefficients for concealing text messages**
Step1: Read input image.
Read the cover image and resize the selected cover image in standard resolution. After resizing the image read the region in modified image.
Step2: Panel separation.
In panel separation R, G & B Panels are separated. B panel is selected for data hiding.
Step3: Apply transform for B Chanel.
Before encryption of the image Lifting wavelet transform will be applied. We segments image into multiple blocks and each are of 8 X 8 matrixes. Lifting wavelet transform will be applied on each block variable. After successful transformation we get four components LL, LH, HL, and HH.
Step4: Apply Encryption on LL, HL, and HH sub-band.
LH sub-band is reserved for data hiding. Chaos encryption is used to scramble an image except reserved space to make protection of image details during transmission.
For encryption chaotic sequence generator is used with formula,

$$X_{n+1} = u^* x(1-x) \quad (1)$$

Stage 2. Encryption of secret data and Image.

Step5: Select the secret data.
The secret data that we want to hide in cover image is selected from text file.
Step6: Encrypt the secret data.
The selected secret data is encrypted using chaotic encryption algorithm.
Step7: Encrypt the cover Image.
The cover image is encrypted using chaotic encryption algorithm.

Stage3. Concealing the encrypted in the reserved area
Step8: Hide or conceal the encrypted data into the reserved coefficients

After an encryption, the data hider will conceal the encrypted secret data into the reserved coefficients using adaptive LSB insertion method. After hiding the data we get stego encrypted image.

Algorithm 2: Decrypted data extraction from stego encrypted image.

Input: A stego encrypted image and decryption key K2.
Output: Original Image, Text file.

Steps:

Stage 4. Inverse transformation of Image.
Step9: Apply inverse transform and panel reconstruction.
The lifting wavelet transformation will be performed to stego image to find reserved space to select coefficients which are used at embedding side.

Stage 5. Extraction of data and decryption of image and data
Step 10: Validation, same reverse process for extraction.
The secret data can be extracted from the embedded image with help of key matrix.
Step 11: Decryption of an image and data.
Image and data are decrypted using chaos decryption method to recover the image and data.

Stage 6: Recovery of original Image.
Step 12: Panel suppression
All R, G and B panels are suppressed together to get original cover image. Finally, image and hidden text will be recovered without any loss based same methods which are used at embedding stage.

5. Experimental Results

The proposed reversible data concealment algorithm with reserving room approach is applied to the various typical colour images. The examples of the experimental results. Figure 4(a) Input cover image, Figure 4(b) B-Panel image , Figure 4(c) Transformation image , Figure 4(d) Encrypted stego image, Figure 4(e) recovered original image.

- The input image is used for cover image to hide the secret data.
- B-Panel of image is chosen for the data hiding.
- Image transformation is done by using wavelet transform for reserving coefficient for the data hiding.
- Image with hidden data is encrypted for more security. So figure shown is stego encrypted image.
- Original image is recovered with reverse lossless transformation.

Figure 4(a): Input image

Figure 4(b): B Panel image

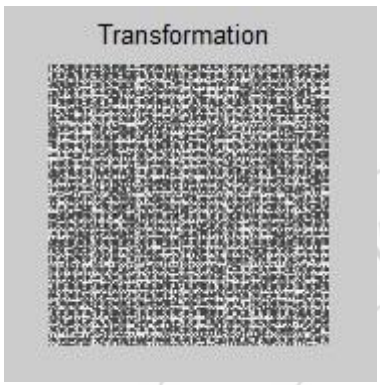

Figure 4(c): Transformation image

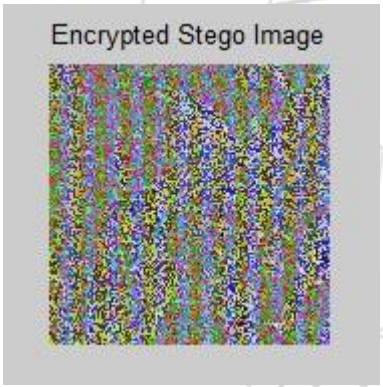

Figure 4(d): Encrypted Stego Image

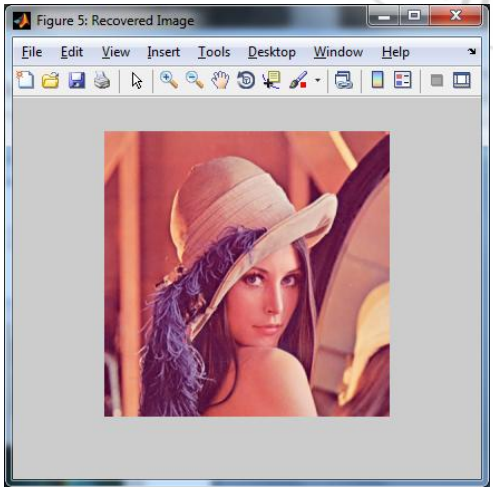

Figure 4(e): Recovered Original images

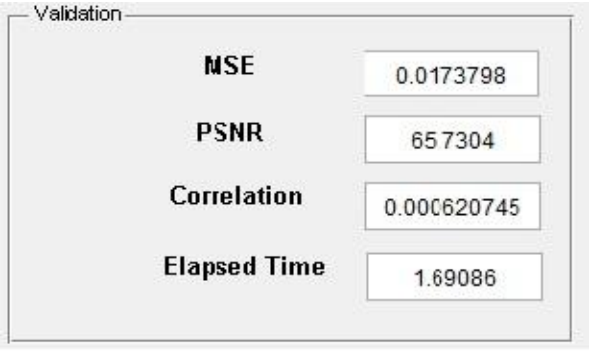

Figure 4(f): MSE, PSNR, Correlation and elapsed time calculation of recovered Original image.

It can be seen from Figure.5 that the Original image is recovered by the proposed method, has smaller MSE value, which implies that image is more similar to the input cover image in appearance. PSNR is significantly high. Another advantage of proposed method is that; it can embed much wider range of data with acceptable PSNR value. The proposed method can embed more than 10 times larger payload for same acceptable PSNR, which implies very good potential for practical applications. The other results of the experiments show the same conclusion.

6. 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. This project proposes less computational time for image encryption. More security than previous method. Data hiding capacity is high and Less degradation in Image quality during recovery

7. Future Scope

In our previous paper we have given the detail survey of various reversible data hiding schemes and also presented the comparative analysis of those schemes. In this paper details of algorithms used in proposed scheme has been explained. For proving the performance of the method the PSNR value of an original image and data hided image is considered and to prove the performance of reconstruction of image scheme the PSNR of original image and reconstructed image is considered. The PSNR of the original image and data hided image should be maintained >40db and to prove that after the data is retrieved, the reconstructed image is same as original image, the PSNR should be infinity. This can be proved with proper implementation of the algorithm.

8. Acknowledgment

The authors would like to thank the reviewers for many useful comments and suggestions which can improve the presentation of the paper.

References

[1] Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li,"Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption", IEEE Transactions On Information Forensics And Security, March 2013.
[2] W.Zhang, B.Chen, and N.Yu, "Capacity-approaching codes for reversible data hiding,"in Proc 13th Information Hiding (IH'2011), Springer-Verlag.
[3] W. Hong, T. Chen, and H.Wu, An improved reversible data hiding in encrypted images using side match,‖ IEEE Signal Process. Lett., vol.
[4] J.Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol.,Aug.2003.
[5] Wen Chung Kuo, Po Yu Lai, Lih Chyau Wuu,"Adaptive Reversible Data Hiding Based on Histogram", 10th International Conference on Intelligent Systems Design and Application, © IEEE 2010 (2002).
[6] Kuo-Ming Hung, Wen-Kai Su, Ting-Wen Chen, Li-Ming Chen, "Reversible Data Hiding Base on VQ and Half toning Technique", (ICMiCR-2013).
[7] Jose, R.; Abraham, G, "A separable reversible data hiding in encrypted image with improved performance", Emerging Research Areas and 2013 International Conference on Microelectronics, annual International Conference ©IEEE 2013.
[8] Moni Naor, Adi Shamir," Visual Cryptography", in Proc. EUROCRYPT'94, Berlin, Germany, 1995, vol. 950, pp. 1-12,Springer-Verlag, LNCS.
[9] Siddharth Malik, Anjali Sardana, Jaya, "A Keyless Approach to Image Encryption",2012 international conference on Communication systems and Network Technologies ©2012 IEEE.
[10] InKoo Kang, Gonzalo R. Arce , Heung-Kyu Lee, " Color Extended visual cryptography using error diffusion", ICASSP 2009 © IEEE 2009.
[11] Wei Qiao, Hongdong Huaqing Liang, "A kind of Visual Cryptography Scheme For color Images based on halftone technique", International Conference on Measuring Technology and Mechatronics automation © 2009 IEEE .
[12] Yi-Hui Chen, Ci-Wei lan and Chiao Chih Huang, " A verifiable Visual Cryptography Scheme", Fifth International Conference and Evolutionary Computing © IEEE 2011
[13] Alice Blessie, J. Nalini and S. C. Ramesh "Image Compression Using Wavelet Transform Based on the Lifting Scheme and its Implementation", IJCSI ,Vol. 8, Issue 3, No. 1, May 2011.