Volume 5, Issue 2, February 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Approach for Extracting of Hidden Data from Encrypted Images Using Reserving Room before Encryption

Ashwini B. Gadge, Naresh Thoutam
Computer Engineering, Pune University
Maharashtra, India

Abstract*— The Technology named Reversible data hiding (RDH) .It maintains the property even after processing on the image. The original cover image remains the same. After encryption and processing is done on the data the original data is obtained. The image is used to embed additional information in the encrypted images. It is applicable in many fields of security which can be recoverable with original media and the hidden data without loss. Many reversible data hiding techniques are present but on analysis all fail to provide security and authentication. This system proposes a reversible data hiding technique which work is separable, the receiver can extract both original and extra embedded data if he knows the keys and the receiver can verify the data hidden by the data hider, such that the work proposes both security and authentication. This proposed has a reversible data hiding technique with both security and authentication for additional data stored in the encrypted images.

***Keywords*— Data Hiding, Encrypted Images, Reversible data hiding.**

I. INTRODUCTION

Reversible data hiding technique which hides data behind the image and an original data is retrieved after the processing on the encrypted image. It was found that [1]; a lot of research done on signal processing of encrypted images. It is very useful for hiding the data and maintaining the privacy of the data. However, in some scenarios a content owner does not trust the processing service provider, it is thus able to keep the data unrevealed but in encrypted form. For instance, when the secret data to be transmitted are encrypted, a channel provider without knowing anything of the cryptographic key may try to compress the encrypted data due to the limited resources.[8] Image security has become increasingly important for many applications mostly related to internet e.g. confidential transmission, military and medical application purpose. The protection of multimedia data can be done with encryption or data hiding algorithms. There was a problem faced to try to combine compression, encryption and data hiding in a single step. For example, solutions were proposed to combine image encryption and compression. Two groups of technologies have been developed to solve. First technique is based on content protection through encryption. There are several methods to encrypt binary images or gray level images. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. Recent reversible data hiding methods have been proposed with high capacity, but these methods are not applicable on encrypted images.

A. What is reversible data hiding?

Data hiding is a process of hiding data behind the cover media. That is, the data hiding process has two sets of data, one set of the embedded data and another set of the cover media data.[2] The relationship between these two sets of data characterizes different applications. For instances, in covert communications the hidden data may often be relevant to the cover media. In authentication however the embedded data are closely related to the cover media. [3]In most cases of data hiding the cover media experiences some distortion due to data hiding and inverting back to the original media is not possible. That is some permanent distortion has occurred to the cover media even after the hidden data has been extracted out. It is used in medical and law forensics where data secrecy has to maintain.

B. What is reserving room before encryption?

Lossless vacating room from the encrypted images is relatively difficult and inefficient, so reverse 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] The data extraction and image recovery are identical to that of Framework VRAE. Standard RDH algorithms are ideal for reserving room before encryption and can be easily applied to Framework RRBE to achieve better performance compared with techniques from Framework VRAE. [1] This is because in this new framework, follow the customary idea that first lossless compresses the redundant image content (e.g., using excellent

RDH techniques) and then encrypts it with respect to protecting privacy. Next 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. [4] The reserving operation adopt in the proposed method is a traditional RDH approach.

II. LITERATURE SURVEY

1. Difference Expansion:

A common approach of high capacity reversible data embedding is to select an embedding area (for example, the least significant bits of some pixels) in an image, and embed both the payload and the original values in this area (needed for exact recovery of the original image) into such area. As the amount of information needed to be embedded (payload and original values in the embedding area) is larger than that of the embedding area, techniques rely on lossless data compression on the original values in the embedding area and the space saved from compression will be used for embedding the payload. DE technique, which discovers extra storage space by exploring the redundancy in the image content. The DE technique to reversibly embed a payload into digital images. Both the payload capacity limit and the visual quality of embedded images of the DE method are among the best in the literature, along with a low computational complexity. But is does not have more payload capacity.

2. Histogram Shifting:

Another promising strategy for RDH is histogram shift (HS), in which space is saved for data embedding by shifting the bins of histogram of gray values.[1] The state-of-art methods usually combined DE or HS to residuals of the image, e.g., the predicted errors, to achieve better performance.

III. PROPSED-FRAMEWORK

- Lifting Wavelet Transformer
- Chaos based image encryption
- Asymmetric key algorithm based text encryption
- Adaptive LSB Replacement
- Data Recovery by decryption
- Parameter Analysis(MSE, PSNR, Correlation, Elapsed time)

The diagram below explains all the flow of the system. The input is the image i.e. the gray scale image and the data have to be hidden behind the image so the data is attached and the methods are applied to it and send to encryption. While encryption the original data is recovered without ant distortion a nd finally the output image is achieved. After the retrieval the final image is looks same as the original image. It achieves lossless data with original cover image.

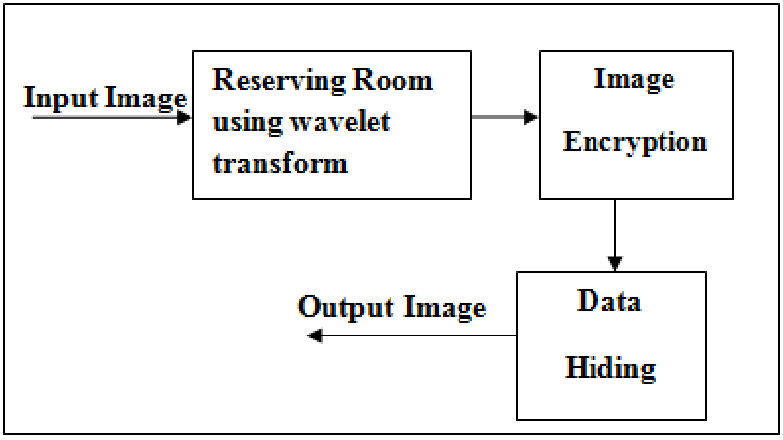

Fig .1. Block Diagram of the system.

A. Lifting Wavelet Transformer

- 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 contain 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.
- It is one of the advanced encryption standard to encrypt the image for secure transmission.
- Encryption is done with the original image pixel values with encryption key value generated from chaotic sequence with threshold function by bit xor operation.
- Logistic map is used for generation of chaotic map sequence.
- It is very necessary to transmit the secret image through unsecure channel securely which prevents data hacking.

B. Image Encryption Flow

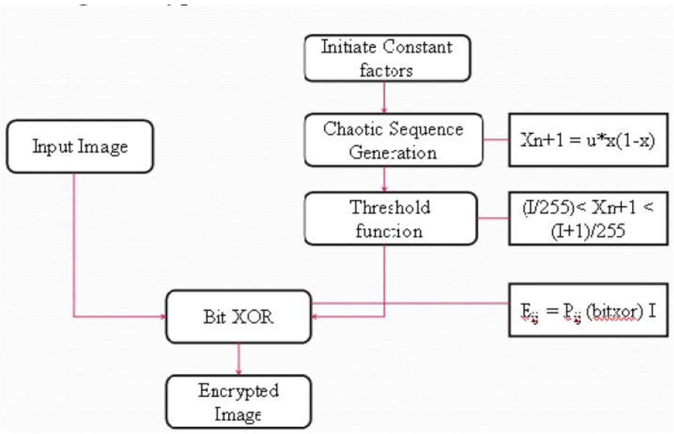

Fig .2.Image Encryption flow Diagram.

C. Asymmetric Key Cryptography

- Cryptography allows secure transmission of private information over insecure channels (for example Packet-switched networks).
- As cryptography allows secure storage of sensitive data on any computer.
- **RSA** – Public Key Cryptography
- **Public key (E)** and Modulus *N* are known to all users
- **Private key (D)** (secret key)
- Provides Authentication/Encryption
- Signing/Decryption operation
- Verifying/Encryption operation
- Data encryption will be done by,
  Cipher text = C. ^E mod N
  Where, C – Each Character of Input text message
  N = p * q; N – modulus parameter, p & q – two largest prime number obtained from user given 8-bit key.
- Data decryption will be done by,
  Plaintext = Cipher. ^D mod N.

D. Adaptive Lsb Embedding

- Consider an 8-bit gray scale image matrix consisting m × 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 soon.
- The resultant Stego-image which holds the secret message is also a 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.

E. Data Recovery

Since data extraction is completely independent from image decryption, the order of them implies different practical applications.

Extracting Data from Encrypted Images: Managing and update ting personal information of images which are encrypted for protecting clients' privacy, an inferior database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. The order of data extraction before image decryption guarantees the feasibility of our work in this case. When the database manager gets the data hiding key, he can decrypt the LSB-planes of and extract the additional data by directly reading the decrypted version. When requesting for updating information of encrypted images, the database manager, then, updates information through LSB replacement and encrypts updated information according to the data hiding key all over again. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.

IV. MATHEMATICAL MODEL

Actually, to construct the encrypted image, the first stage can be divided into three steps: image partition, self reversible embedding followed by image encryption. At the beginning, image partition step divides original image into two parts A and B ;then, the LSBs of A are reversibly embedded into B with a standard RDH algorithm so that LSBs of A can be used for accommodating messages; at last, encrypt the rearrangement of image to generate its final version.

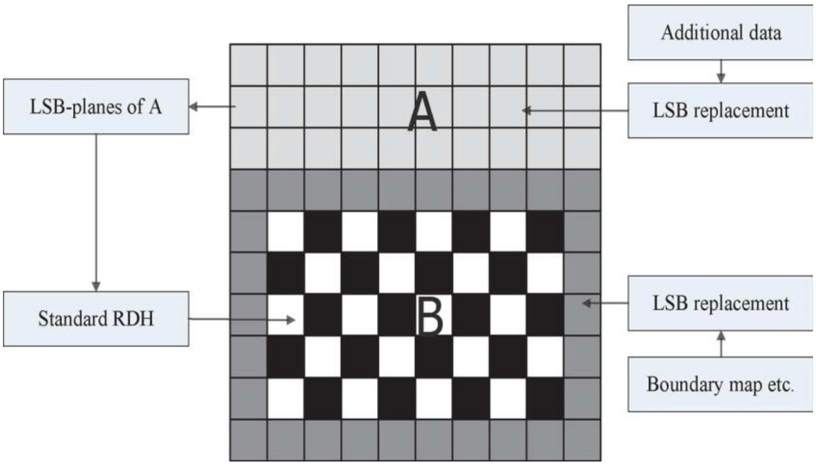

Fig .3. Illustration of image partition and embedding process.

Image Partition: The operator here is a standard RDH technique, so the goal of image partition is to construct a smoother area B, on which standard RDH algorithms such as [10], [11] can achieve better performance. To do that, without loss of generality, assume the original image C is an 8 bits gray-scale image with its size D*E and pixels Ci,j €[0,255],1≤ i≤ D,1≤j≤E. First, the content owner extracts from the original image, along the rows.

$$f=\sum_{u=2}^{m}\sum_{v=2}^{N-1}\left|\mathbf{C}_{u,v}-\frac{\mathbf{C}_{u-1,v}+\mathbf{C}_{u+1,v}+\mathbf{C}_{u,v-1}+\mathbf{C}_{u,v+1}}{4}\right|. \qquad (1)$$

V. EXPERIMENTAL ANALYSIS

The experiment carried out are analyzed and compared with the similar systems here existing system like Reversible Data Hiding in Encrypted Images by Reserving room before Encryption for the performance. The further section describes the dataset used in the data extraction from multiple data sources .Further section gives the brief idea about which input data is used and how input data is used to get the result and analyze the data extraction with the similar system. The another method used is graphical representation view for the analysis. Further section explains the applications of the Extracting Hidden Data from Encrypted Images Using Reserving Room before Encryption system.

1. Dataset

The dataset used is plain image like leena, Barbara, baboon, etc .A specified amount of data is worked upon to get the psnr value greater to existing system.

2. Result set and graphs

The tables give statistics of the trial data that is given as the input dataset. My evaluation is based on lsb plane values. I divide this into lsb plane 1 and lsb plane 2 according to embedding rates is the system I implemented i.e. the proposed system. Lsb plane means the image corresponding to the contribution of the LSB to the stego-image also contains the secret information.LSB Plane of the Image either represent the hidden information or the LSB Component of the total Image.

Lsb plane 1 for leena

As shown in table the embedding rate i.e how much amount of data is behind the image. According comparision of Existing system and Proposed System.

Table I Result set for psnr value

Embedding Rate	RDH Method	IWT Method
0.005 lsb1	67.16	67.88
0.01 lsb1	63.44	64.25
0.05 lsb1	55.46	55.25
0.1 lsb1	52.33	53.23

3. Graphicl View for lsb plane 1

How existing and Extracting Hidden Data from Encrypted Images Using Reserving Room before Encryption system respond to different input is represented graphically. Graphs plotted below gives the brief idea about the system's response for individual dataset.

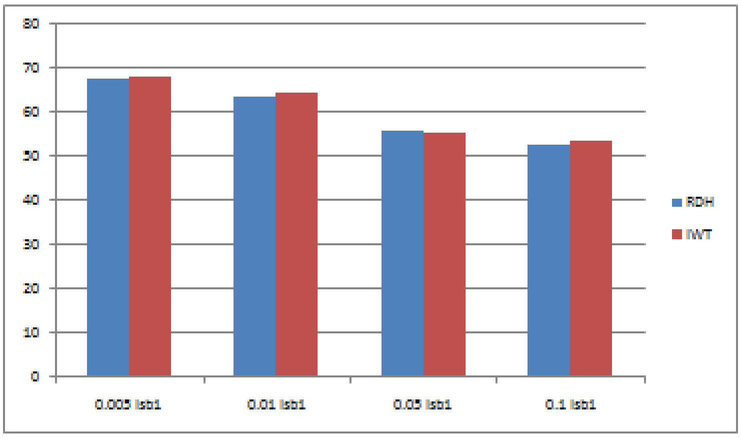

Fig 4: Evaluation of lsb1 for leena

4. Result Set for airplane lsb 2 plane

As shown in table the embedding rate i.e. how much amount of data is behind the image .According comparision of Existing system and Proposed System.

Table II Result set for psnr value

Embedding Rate	RDH Method	IWT Method
0.005 lsb2	65.48	65.63
0.01 lsb2	62.33	62.45
0.05 lsb2	55.91	56.32
0.1 lsb2	53.05	54.21

5. Graphicl View for lsb plane 2

How existing and Extracting Hidden Data from Encrypted Images Using Reserving Room before Encryption system respond to different input is represented graphically. Graphs plotted below gives the brief idea about the system's response for individual dataset.

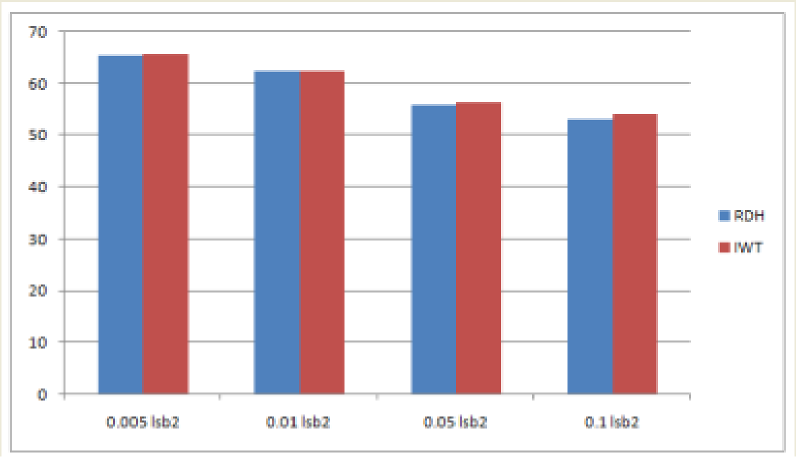

Fig5: Evaluation of lsb 2 plane for airplane

VI. CONCLUSIONS

Reversible data hiding method that has achieved more payload capacity. I have done reversible data hiding by using Integer Wavelet Transform. It ensures the correct data extraction and the perfect image recovery prevention of image from external attacks less computational time for image encryption. It achieves more security than previous method. Data hiding capacity is high. Less degradation in Image quality during Recovery. The method compress the data and then it is send. No access without key to the original image.

ACKNOWLEDGMENT

I would like to acknowledge all the people who have been helpful and assisted me throughout my project work.

First of all I would like to thank respected Principal Prof.DR.S.T.Gandhe and my respected H.O.D.Prof. R.D.Kadu and specially Thank to my guide Prof.N.C.Thoutam of Computer Engineering for introducing me throughout features needed. The time-to-time guidance, encouragement, and valuable suggestions received from him are unforgettable in my life. This work would not have been possible without the enthusiastic response, insight, and new ideas from him.I would also like to thank my friends for their valuable support and encouragement.

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. 71-76.

[2] W. Zhang, B. Chen, and N. Yu, \Capacity-approaching codes for reversible data hiding," in Proc 13th Information Hiding (IH'2011), LNCS 6958, 2011, pp. 255-269, Springer-Verlag.

[3] W. Zhang, B. Chen, and N. Yu, \Improving various reversible data hiding schemes via optimal codes for binary covers," IEEE Trans. Image Process., vol. 21, no. 6, pp. 2991-3003, Jun. 2012.

[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 di_erence 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. Circuit 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, pp. 721-730, Mar. 2007.

[8] 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. 3524-3533, Dec. 2011.

[9] P. Tsai, Y. C. Hu, and H. L. Yeh, \Reversible image hiding scheme using predictive coding and histogram shifting," Signal Process., vol. 89, pp. 1129-1143, 2009.

[10] L. Luo et al., \Reversible imagewatermarking using interpolation technique," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187-193, Mar. 2010.

[11] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, \Reversible watermarking algorithm using sorting and prediction," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989-999, Jul. 2009.

[12] 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.

[13] W. Liu, W. Zeng, L. Dong, and Q. Yao, \E_cient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097-1102, Apr. 2010.

[14] X. Zhang, \Reversible data hiding in encrypted images," IEEE Signal Process. Lett.,vol. 18, no. 4, pp. 255-258, Apr. 2011.

[15] 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. 199-202, Apr. 2012.

[16] X. Zhang, \Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826-832, Apr. 2012.

[17] Masaaki FUJIYOSHI, \A Dual Permutation-Based Separable Reversible Information Hiding Scheme in Encrypted Images", Department of Information and Communication Systems, Tokyo Metropolitan University. Hino, Tokyo, Japan. IEEE 17th International Symposium on Consumer Electronics (ISCE)2013

[18] C.Anuradha, S.Lavanya , \Secure and Authenticated Reversible Data Hiding in Encrypted Image." Volume 3, Issue 4, April 2013 ISSN: 2277 128X

[19] vinit Agham and Tareek Pattewar, \A Survey on separable reversible data hiding technique."vol4,may 2013

[20] w.Puench and J.M.Rodrigues, \A new fast reversible method for images safe transfer.

[21] M.Nosrati and R.Karimi, \Reversible data hiding:Principles,Techniques and recent studies"vol2,Issue(5),May 2012.