ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 4, December 2014

Reversible knowledge activity in encrypted pictures by reserving space before cryptography

K. Manoj kumar[1], U. Sheshadri[2]

Department of Computer Science and Engineering, Vaagdevi Institute of Technology and & Science, Proddatur, Kadapa, India[1,2]

Abstract: 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 losslessly recovered after embedded data is extracted while protecting the image content's 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 paper, we propose a novel method by 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. 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

Reversible data hiding (RDH) in images is a technique, by which the original cover can be loss less 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 the equivalence between data compression and RDH for binary covers.

In practical aspect, many RDH techniques have emerged in recent years. Fredric *et al.* [4] Constructed a general framework for RDH. By first extracting compressible features of original cover and then compressing them losslessly, spare space can be saved for embedding auxiliary data. A more popular method is based on difference expansion (DE) [5], in which the difference of each pixel group is expanded, e.g., multiplied by 2, and thus the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages. Another promising strategy for RDH is histogram shift (HS) [6], in which space is saved for data embedding by shifting the bins of histogram of gray values. The state-of-art methods [7]–[11] usually combined DE or HS to residuals of the image, e.g., the predicted errors, to achieve better performance.

Some attempts on RDH in encrypted images have been made. In [16], Zhang divided the encrypted image into Several blocks. By flipping 3 LSBs of the half of pixels in each block, room can be vacated for the embedded bit. The data extraction and image recovery proceed by finding which part has been flipped in one block. This process can be realized with the help of spatial correlation in decrypted image. Hong *et al.* [17] ameliorated Zhang's method at the decoder side by further exploiting the spatial correlation using a different estimation equation and side match technique to achieve much lower error rate.

To separate the data extraction from image decryption, Zhang [18] emptied out space for data embedding following the idea of compressing encrypted images [14], [15]. Compression of encrypted data can be formulated as source coding with side information at the decoder [14], 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. The method in [18] compressed the encrypted LSBs to vacate room for additional data by finding syndromes of a parity-check matrix, and the side information used at the receiver side is also the spatial correlation of decrypted images.

All the three methods try to vacate room from the encrypted images directly. However, since the entropy of encrypted images has been maximized, these techniques can only achieve small payloads [16], [17] or generate marked image with poor quality for large payload [18] and all of them are subject to some error rates on data extraction and/or image restoration. Although the methods in [16], [17] can eliminate errors by error correcting codes, the pure payloads will be further consumed.

Copyright to IARJSET

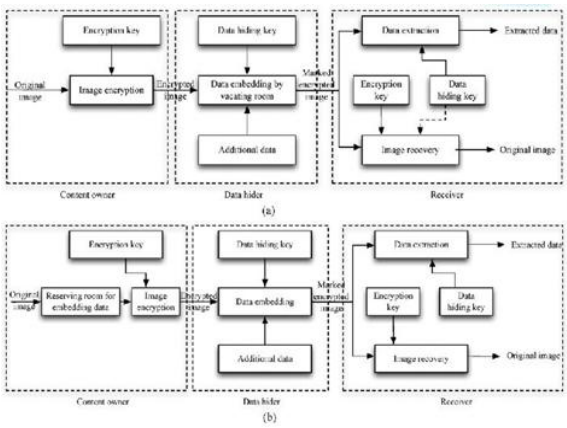
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 4, December 2014

In the present paper, we propose a novel method for RDH in encrypted images, for which we do not "vacate room after encryption" as done in [16]–[18], but "reserve room before encryption". 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 encrypt the image, so the positions of these LSBs in the encrypted image can be used to embed data. Not only does the proposed method separate data extraction from image decryption but also achieves excellent performance in two different prospects:

Real reversibility is realized, that is, data extraction and image recovery are free of any error. • For given embedding rates, the PSNRs of decrypted image containing the embedded data are significantly improved; and for the acceptable PSNR, the range of embedding rates is greatly enlarged.

II. PREVOUS ARTS



As per fig(a), In this framework, a content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider (e.g., a database manager) and the data hider can embed some auxiliary data into the encrypted image by lossless vacating some room according to a data hiding key. Then a receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key.

In all methods of [16]–[18], the encrypted 8-bit gray-scale images are generated by encrypting every bit-planes with a stream cipher. The method in [16] segments the encrypted image into a number of nonoverlapping blocks sized by ; each block is used to carry one additional bit. To do this, pixels in each block are pseudo-randomly divided into two sets and according to a data hiding key. If the additional bit to be embedded is 0, flip the 3 LSBs of each encrypted pixel in , otherwise flip the 3 encrypted LSBs of pixels in . For data extraction and image recovery, the receiver flips all the three LSBs of pixels in to form a new decrypted block, and flips all the three LSBs of pixels in to form another new block; one of them will be decrypted to the original block.

The extraction and recovery of blocks are performed according to the descending order of the absolute smoothness difference between two candidate blocks and recovered blocks can further be used to evaluate the smoothness of unrecovered blocks, which is referred to as side match

III. PROPOSED METHOD

Since losslessly vacating room from the encrypted images is relatively difficult and sometimes inefficient, why are we still so obsessed to find 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 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)".

As shown in Fig. 1(b), the content owner first reserves enough space on original image and then convert the image into its encrypted version with the encryption key. Now, 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 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.

METHODOLOGIES

Lifting Wavelet Transformer

Chaos based image encryption

Asymmetric key algorithm based text encryption

Adaptive LSB Replacement

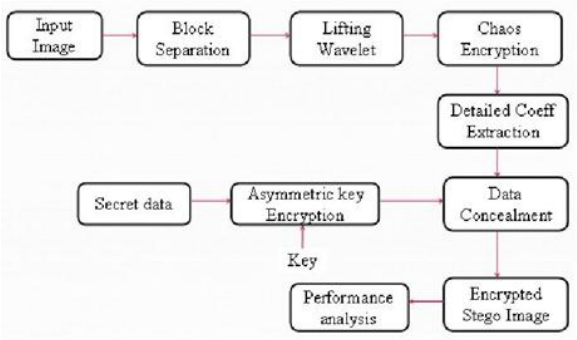
Data Recovery by decryption

Parameter Analysis(MSE, PSNR, Correlation, Elapsed time)

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 4, December 2014

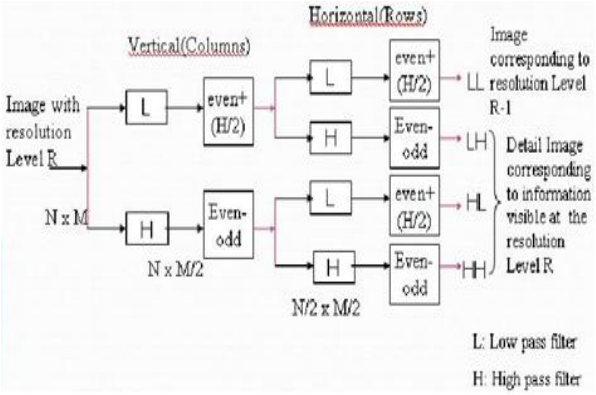
Block Diagram
Image Encryption and Data hiding:



A. LIFTING WAVELET TRANSFORMER

LWT decomposes the image into different subband images, namely, LL, LH, HL, and HH for embedding the messages in the pixel coefficients of subbands.Lifting scheme is a technique to convert DWT coefficients to Integer coefficients without losing information.
LL subbands contains the significant part of thespatial domain image. High-frequency subband 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 subbands because it is non sensitive to human visual system.

Block diagram

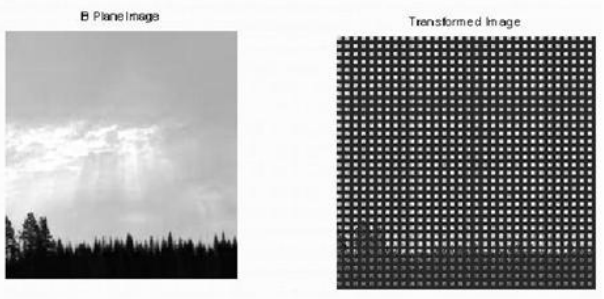


Forward Lifting in IWT
Step1: Column wise processing to get H and L
H = (Co-Ce) and L = (Ce+ [*H/2]*)
Where Co and Ce is the odd column and even column wise pixel values.
Step 2: Row wise processing to get LL,LH,HL and HH, Separate odd and even rows of H and L,
Namely, Hodd – odd row of H, Lodd- odd row of L
Heven- even row of H, Leven- even row of L

LH = Lodd-Leven ,LL = Leven + [*LH / 2]*
HH = Hodd – Heven ,HL = Heven + [*HH / 2]*

Reverse Lifting scheme in IWT
Inverse Integer wavelet transform is formed by Reverse lifting scheme. Procedure is similar to the forward lifting scheme.

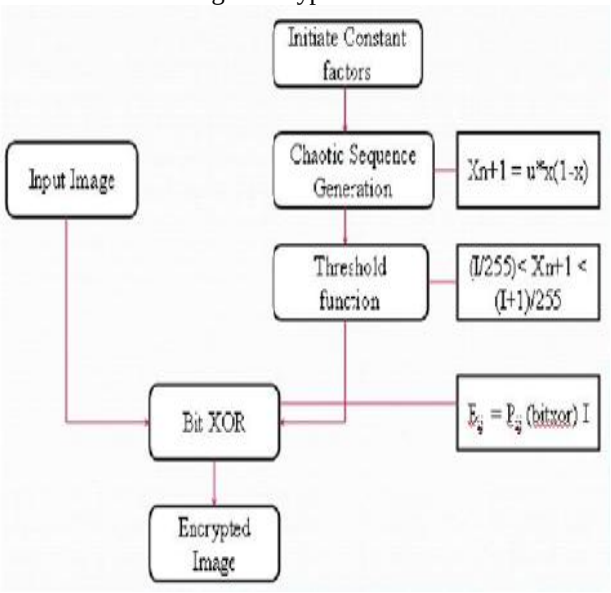
LWT decomposition



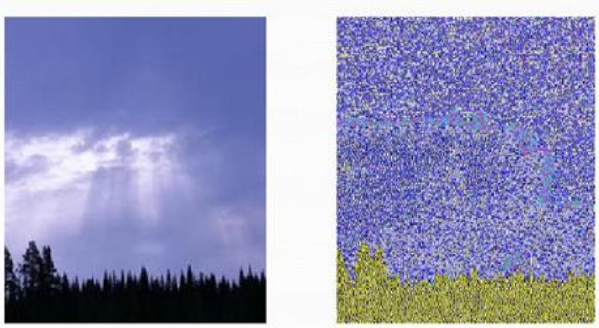
B. CHAOS ENCRYPTION

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 bitxor 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.

Image Encryption Flow



Cover and Encrypted Image



C. ASYMMETRIC KEY CRYPTOGRAPHY

Cryptography allows secure transmission of private information over insecure channels (for example packet-switched networks).
Cryptography also allows secure storage of sensitive data on any computer.

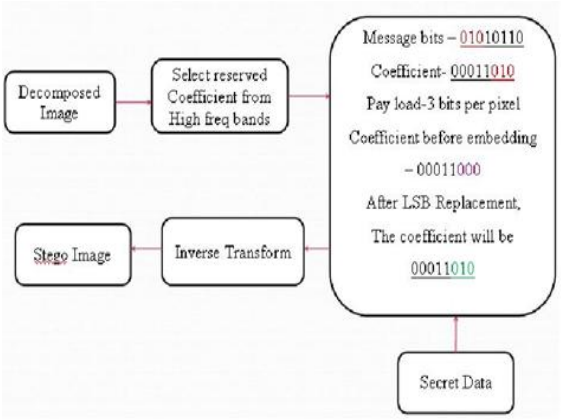
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 4, December 2014

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,
Plain_text = Cipher.^D mod N

D. ADAPTIVE LSB EMBEDDING
A 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 so on.
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.

Algorithm Flow



Advantages
Less computational time for image encryption.
More security than previous method
Data Hiding capacity is high
Less degradation in Image quality during Recovery

Applications
Secret Data Communication in Defense.
Research institute.
Medical information protection.

E. DATA RECOVERY

Since data extraction is completely independent from image decryption, the order of them implies two different practical applications.
Extracting Data From Encrypted Images: To manage and update 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. 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 tomake 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.

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 variousreversible 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 difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

BIOGRAPHY

I am **K. Manoj kumar**, PG scholar. I had attended a National Conference on E-commerce. This is my first publication in a journal.