International Journal of communication and computer Technologies, ISSN: 2278-9723

Available at http://www.ijccts.org

Comparing PSNR by using Integer and Haar Wavelet Transform in Reversible Data Hiding Technique

Ms. S. Jeba Pon Elizabeth[1], Mrs.R.Vedhapriya Vadhana[2]

Received: 14-01-2014, **Revised:** 27-03-2014, **Accepted:** 02-05-2014, **Published online:** 19-06-2014

.***Abstract – A novel approach to recover data and cover image was introduced here by using reserve room concept of encryption. Here, data can be extracted without any loss, since reserve room concept of encryption is being used. In the previous methods, data are encrypted and are then being stored. But, in this method, data are stored in a particular place before the process of encryption. This helps in preventing the loss of data occurring in the system. Usually, transformation is a compression technique, takes place in the image to improve its quality. Integer wavelet transform and Haar transform are used here to improve the quality of the image. Comparison of integer wavelet transform and Haar transformation takes place and the PSNR achieved by Haar transform is greater than the PSNR achieved by integer wavelet transform. The mean square error also gets decreases in Haar transformation when compares with the integer wavelet transformation. Experimental results show that this method can embed large amount of data comparing to the previous methods.***

Key words: **Reserve Room concept of encryption, Reversible data hiding, histogram modification, Integer wavelet transform, Haar transform.**

I.INTRODUCTION

Steganography is a wide area which deals with the security systems of various kinds in digital image processing. It plays an important role in technical aspects. It deals with the form of security through obscurity. It hides the message within a particular medium and thus helps the source to send the message to the destination secretly. This method is similar to cryptography. The advantage of steganography over cryptography is that the secret message does not attract attention to itself as an object of scrutiny. N. Johnson has explained the study of steganographic techniques in [1].

Reserve room concept of encryption is being used. Hence, the original cover can be losslessly recovered after the embedded data is extracted. This is widely used in medical field, military and law forensics where distortion is not allowed. Confidentiality is improved here by increasing the quality of the image with the rate distortion model for RDH was established by Kalker and Willems [2], where the rate distortion models for memory less covers are proved and a recursive code construction was being proposed. A recursive code construction for binary covers was proposed by Zhang et al [3], [4] and proves that the code construction reach the rate distortion bound as long as compression reaches entropy which establish the equivalence between data compression and RDH for binary images.

For providing confidentiality, encryption is an effective way as it converts original content into an incomprehensible one. Hence, Reversible Data Hiding technique is being used in the process of encryption. The process of embedding data into the cover image with the help of RDH technique was explained briefly Zhicheng Ni in [5]. A reputation based trust management scheme with data coloring was proposed by Hwang et al [15] and data encryption by watermarking and coloring offers content owners privacy and data integrity. Here, the cloud service provider has no rights to provide data distortion for encrypted images. Thus, a reversible data coloring for encrypted images is preferred.

Zhang [20] is a pseudo randomly permuted method which emptied out the space between data embedding following the idea of compressing the encrypted images [15],[16]. Compression can also be followed by source coding with side information at the decoder. In this paper, we proposed a novel method for RDH by which we do not vacate the room after encryption as don in [16] to [18] but “Reserve room before encryption”. Hence, we first empty out the room by embedding some pixels of LSB and then encrypt the image.

II. PREVIOUS METHODS

There are several methods that are being used to encrypt the data and cover images previously. Fridrich et al construct a general frame work for RDH. In this method, we extract the compressible features of original cover. We then compress them losslessly. Spare spaces can be saved for embedding auxiliary data. In difference expansion, the difference is first expanded. Then, the LSB of the difference are zero. This is used for embedding messages. In histogram shift, space is saved for data embedding by shifting the bins of histogram of gray values. Here, encryption converts the original content into incomprehensible ones.

In data coloring, a medical image is stored in the data center. Server in the data center can embed notation in the encrypted form through RDH techniques. With the notation, the server can manage the image or verify its integrity without the knowledge of the original content. Thus, the patients privacy is protected. The doctor with the help of the cryptographic key can decrypt and restore the image.

In RDH method, the encrypted image is divided into several blocks. By flipping 3 LSB's of half of the pixel in each block, rooms can be vacated. Data extraction and image recovery can be proceed by finding which block can be flipped. This is realized with the help of the spatial correlation in decrypted images. Hong et al exploit the spatial correlation by using different estimation equation and side match technique to achieve much lower error rate. Usually encrypted images must be decrypted before data extraction. To separate the data extraction from image decryption, the space for data embedding is emptied by compressing encrypted images. Compression can takes place with source coding and side information. These techniques achieve smaller payloads by maximizing the entropy.

In previous method, we vacate room after encrypting the data. This may cause error occurring in the system. Here, first the original image is encrypted using the standard cipher with the encryption key. The encryption image is handover to the data hider. The data hider embeds some auxiliary data by vacating some room according to the data hiding key. The receiver extracts the data with the help of the data hiding key. The receiver then recovers the original image with the help of the encryption key.

III. PROPOSED METHOD

A. system model

In the proposed method, reserving room before encryption by using traditional RDH algorithm is being used. This helps to recover the data and the cover image without any loss. The PSNR achieved by this method is high, which helps in producing the good quality of image as the output. Improving the PSNR also helps in increasing the confidentiality. This is achieved by using transformation process in the image before being encrypted. The probability of error occurrence is also low since the value of mean square error obtained is low. This method involves three processing steps such as: 1.Generation of encrypted images 2.Data embedding in encrypted images 3.Data extraction and image recovery.

1. Generation of encrypted images

The generation of encrypted images deals with converting original form of images into another new form. It takes place in two ways. First, by putting digital watermarkings in an image. Here, hidden image can be broken easily by the eaves dropper. Second method is by converting image file into the data file. This method is widely being used.

For example, a gray value $X_{i,i}$ ranging from 0 to 255 can be represented by

8 bits, $X_{i,j}(0)$, $X_{i,j}(1)$,….$X_{i,j}(7)$, such that

$$X_{i,j}(k) = \lfloor X_{i,j}/2^k \rfloor \bmod 2, \quad k = 0, 1, \ldots,7. \qquad \ldots(1)$$

The encrypted bits $E_{i,j}(K)$can be calculated through exclusive- or operation

$$E_{i,j}(k) = X_{i,j}(k) + r_{i,j}(k) \qquad \ldots(2)$$

Where $r_{i,j}$ is generated via a standard stream cipher determined by the encryption key.

2. Data embedding in encrypted images

Data embedding takes place with addition of data into an encrypted image. It can be carried out with and without the use of the key. Embedding with the help of the key increase the robustness. Data hider first finds the no. of bit planes and rows of pixels that it can modify. Data hider adopts LSB to substitute bit planes with additional data M. The symbol M is marked to point out end position of embedding process. Then, M is encrypted according to data hiding key. Hence, additional data cannot be extracted without data hiding key.

3. Data extraction and image recovery

Image recovery takes place with the help of encryption key. Original image can be decrypted with the help of the encryption key. Data extraction takes place in two ways. First, Data extracted from the

encrypted image. Here, the database manager decrypts the LSB with data hiding key. Then, they extract data from the encrypted images. This increases the feasibility.

Secondly, Data is extracted from decrypted images. Here, the encrypted image first gets decrypted with the help of encryption key. The embedded data can be extracted from the decrypted image whenever needed.

With the encryption key, the content owner decrypts the image except the LSB-planes of A_E. The decrypted version of E' containing the embedded data can be calculated by

$$X_{i,j}''(k)=E_{i,j}'(k)+r_{i,j}(k) \quad \ldots.(3)$$

Where $E_{i,j}'(k)$ is the binary bit of $E'_{i,j}$.

B. *Block diagram*

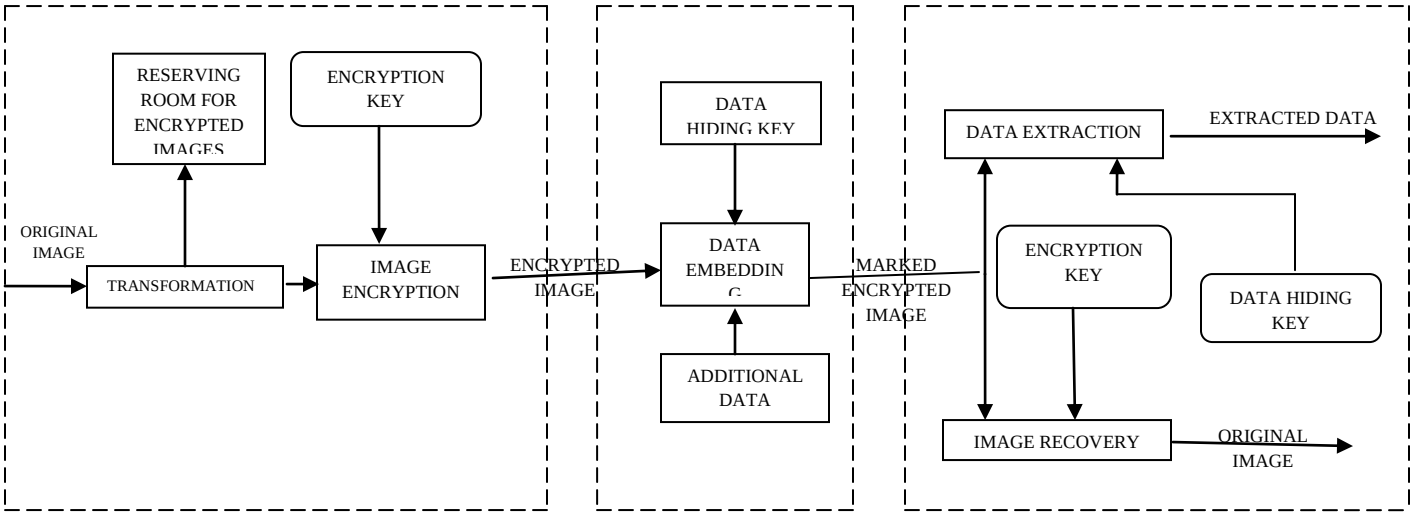


Fig:1 Framework for Reserving Room Before Encryption(RRBE)

C. *Algorithms Used*

Integer wavelet transform and haar transform are the compression techniques used in this process to improve the quality of the image. Generally, when the image gets compressed there will be an increase in the PSNR performance. This helps to improve the quality of the image. The probability of error occurrence is also less due to the transformation used in this process. Haar wavelet function is the function being used in this method. This is generally given by the equation,

$$h_k(t) = \frac{1}{\sqrt{N}} \begin{cases} 2^{p/2} & (q-1)/2^p \le t < \frac{q-0.5}{2^p} \\ -2^{p/2} & (q-0.5)/2^p \le t < q/2^p \\ 0 & \text{otherwise} \end{cases} \quad \ldots.(4)$$

K deals with the index of the Haar function and is generally given by,

$$k = 2^p + q - 1 \quad \ldots..(5)$$

Here, *p* determines the amplitude and width of the non-zero part of the function. and *q* determines the position of the non-zero part of the Haar function.

The encryption of the data and the cover image takes place in the transmitter section while the extraction of the data and the cover image takes place in the receiver section. The transmitter section involves the following steps,

Step1: Read the cover image value into a 2D decimal array.

Step2: Apply histogram modification. Histogram modification helps to set all the values of pixel to maximum or minimum values. This helps to avoid overflow or underflow values of pixels.

Step3: Divide the cover image into 8*8 pixel values

Step4: Transform the 8*8 pixel values into frequency domain with 2D Haar wavelet function.

Step5: calculate the number of bits to hide data of each wavelet coefficient.

Step6: Represent each coefficient as the binary number and replace L LSB of the randomly chosen wavelet coefficient with L bits of data.

Step7: Apply optimum pixel management algorithm to maintain the pixel values.

Step8: Calculate the inverse 2D HIWT to obtain the stego image as the output.

The original data can be extracted and the image can be recovered in the receiver section as follows. This involves the following steps

Step1: Read image file pixel values to a 2d decimal value matrix each represent the pixel value intensity.

Step2: Divide the cover image into (8 pixel * 8 pixel) blocks.

Step3: Transform each (8*8) blocks into frequency domain with 2D HIWT and get 4 sub bands such as LL1, LH1, HL1,

Step4: calculate the number of bits to hide the data of each wavelet co-efficient wc for LL1, LH1, HL1, HH1.

Step5: Use the secret key to generate the selected co-efficient to embed secret data.

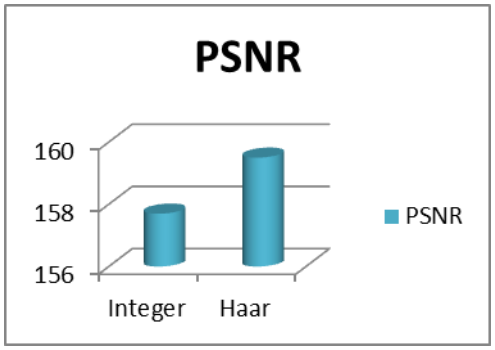
Step6: Extract l bits from each selected co-efficient.

Step7: Gather all l bits to form the secret data in order.

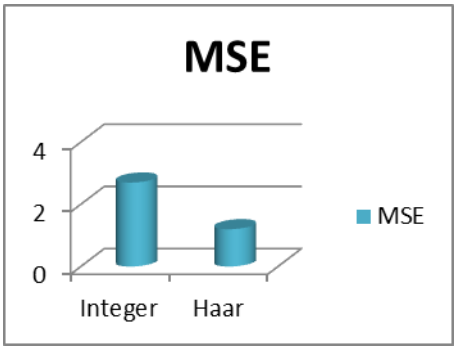
IV. COMPARISON WITH EXISTING SYSTEM

In the existing systems, the encrypted images are stored in a room before the embedding process takes place. This causes some losses in the data. So, in this paper, a reserve room concept of traditional RDH algorithm is being used. This helps in extraction of the data with the original image without any loss. Integer wavelet transform and Haar transform are used here to improve the PSNR performance and decrease the Mean Square Error criteria. This helps in producing the good quality image. The input image first undergoes histogram modification to set all the pixel values either as maximum or minimum. Then, transformation takes place to encrypt the image. In the third step, a secret key is being generated to embed the data and then embedding takes place. Thus, we embed data in the encrypted image. To recover the original image, first optimum pixel management takes place in the embedded image. Then, inverse transform is applied to recover the original image. To extract the data content from the image, transformation takes place with the help of secret keys. Thus, original data is obtained without any error. The quality of the image can be achieved by improving the PSNR performance. The PSNR achieved by using integer wavelet transform is about 157.7dB while through the Haar transform is about 159.5dB. Similarly, the MSE reduced through integer wavelet transformation is 2.61 and through Haar transformation is around 1.22. Hence, better quality of image is obtained through Haar transform than through integer transform.

The bar graph is plotted by comparing the PSNR and MSE value of integer wavelet transform and the Haar transform and is shown below.



(a)



(b)

Fig (a) shows that the PSNR value obtained for Integer wavelet transform is greater than the value obtained for Haar transform. Fig (b) shows that the MSE decreases in HAAR transform than the Integer wavelet transform.

V.RESULTS AND DISCUSSIONS

Here data is being embedded in the cover image using integer wavelet transform and Haar transform algorithm. The PSNR value achieved by Haar transform is greater than the PSNR value achieved by Integer wavelet transform. Here Reserve room concept of RDH algorithm is being used. The data and the cover image are recovered without any loss in this process. Since, the PSNR value achieved is higher, good quality of image is produced as a output and no error performance occur with minimum MSE.

Thus, the original data can be obtained without any error occurring in the system.

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

Fig a) input image b) modified image of the histogram c) Integer transformation takes place in the image d) original image obtained as the output.

In the above example, lenagr figure is considered. First, the input image is modified on the histogram basis. Then integer transformation takes place to encrypt the image. The data file being embedded is chosen and embedded in the encrypted image Finally inverse transformation takes place to obtain the original image and the original data is being extracted from the decrypted image.

Then, Barba is chosen. Here, the input image is modified in the form of histogram basis. Haar transformation takes place here to encrypt the image. Then, the data gets embedded inside the encrypted image. Finally, inverse transformation takes place here to obtain the original image and then the original data gets extracted from the decrypted image.

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

Fig a) input image b) modified image of the histogram c) Haar transformation takes place in the image d) original image obtained as the output.

VI.CONCLUSION

In this work, comparison takes place for the transformation of Integer wavelet transform and Haar transform. Usually, transformation is the compression technique used to improve the quality of the image. Here, transformation is used in Reserve room concept of encryption with the traditional RDH algorithm. Hence, data extraction and image recovery are obtained without any error. But in the existing method, RDH is implemented by vacating room after encryption. This causes loss of data and error occurring in the system. Experimental results shows that the PSNR achieved by the Haar transform is higher than the PSNR value achieved by the integer wavelet transform. Also, the mean square error reduces in Haar transform comparing to the integer wavelet transform. Thus, a good quality of image is obtained as a result. Hence, this can be widely used in modern printers and the media based systems. It provides high confidentiality hence they can used in medical and military applications. No loss of data occurs in the system. Hence they are useful for secret transmission of messages from one source to another.

REFERENCES

[1] N. F. Johnson, S. Katzenbeisser, "A Survey of steganographic techniques", in S. Katzenbeisser and F. Petitco1as (Eds.):Infonnation Hiding, pp. 43- 78. Artech House, Norwood, MA, 2000.

[2] 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.

[3] 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.

[4] 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.

[5] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su, “Reversible Data Hiding” IEEE Trans on circuits and systems for video technology, vol. 16, no. 3, March 2006.

[6] 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.

[7] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[8] Z. Ni, Y. Shi, N. Ansari, and S. Wei, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[9] 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.

[10] X. L. Li, B. Yang, and T. Y. Zeng, “Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,” IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[11] 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.

[12] L. Luo et al., “Reversible image watermarking using interpolation technique,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Mar. 2010.

[13] 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.

[14] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC, 1996.

[16] 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.

[17] W.Liu, W.Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4.

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

[19] 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.

[15] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Comput., vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.

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

[21] Kede Ma, Weiming Zhang, Xianfeng Zhao Member, IEEE, Nenghai Yu, and Fenghua Li's "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption" IEEE transactions on information forensics and security, VOL. 8, NO. 3, MARCH 2013.

AUTHOR(S) PROFILE

Ms.S.Jeba Pon Elizabeth is presently studying M.E second year Communication system Engineering in Francis Xavier Engineering College. She has completed his B.E Electronics and Communication Engineering from Dr.G.U.Pope College of Engineering. Her fields of interests are Digital Image Processing and Wireless communication.

Mrs.R.Vedhapriya Vadhana is presently working as a Assistant Professor, in Department of Electronics and Communication Engineering, Francis Xavier Engineering College, Tirunelveli. She has completed his "Biomedical instrumentation engineering" from Avinashilingam deemed university in the year 2005 and M.Tech in Computer and Information Technology from Manonmaniam Sundaranar University in the year 2009. Her fields of interest are Video processing, Medical image processing.