An Efficient Algorithm for Reversible Data Hiding in Encrypted Images by RRBE

Revathi Nath H A, Jeena R S

Abstract: Recently reversible data hiding in encrypted images is gaining importance as this technique of watermarking can reconstruct the original image after extracting the desired data hidden in the image. In all the previous works, room was reserved for data in the image and the image would be encrypted using a standard stream cipher. This work proposes a technique for reversible data hiding in encrypted images where the data to be hidden is encrypted using Advanced Encryption Standard (AES) that can improve the PSNR. Also the encrypted image holding data would be permuted and transmitted, that can increase the level of security. Experimental results show that this method can achieve a PSNR of more than 60db thereby increasing the embedding rate.

Index Terms: Advanced Encryption Standard, Block merging, Image permutation, Reserving Room before encryption

I. INTRODUCTION

In the technique of Reversible Data Hiding, the original image can be recovered completely after extracting the data hidden in the image. Reversible data hiding is widely used in medical application and military application which do not allow distortion of image after extraction. This work proposes a technique for reversible data hiding in encrypted images where the data to be hidden is encrypted using Advanced Encryption Standard (AES) that can improve the PSNR. The image holding data is also encrypted and this image is permuted and divided into blocks and then transmitted, that can improve the level of security. In the proposed work, advanced encryption standard is used to encrypt the data to be hidden. This type of data encryption ensures security of data transmission, in applications where secure data transmission is of prime concern. AES is a block cipher intended to replace des for commercial applications. In this method room is reserved in the original image prior to data embedding. The data to be transmitted is hidden in this reserved portion of the image. For this self reversible embedding is done. Reversible data hiding algorithm is used for embedding the LSB planes of one portion of image into another part, so that the emptied portion can be utilized for data hiding. The software tool used here is MATLAB.

II. LITERATURE REVIEW

The technique of reversible data hiding received more attention over the years because of its high efficiency and simplicity. Many researchers tried to improve its performance in terms of hiding capacity and visual perceptibility. Some of the traditional reversible data hiding schemes are based on modulo-arithmetic additive and spread-spectrum techniques [1, 2]. Although some of these schemes are fast, the modulo-arithmetic based reversible data hiding algorithms have the drawback of salt and pepper artifacts.

In recent years, many reversible data hiding techniques have emerged. A rate- distortion model for RDH was established by Kalker and Willems [3], through which they proved the rate-distortion bounds of RDH for memory less covers and proposed a recursive code construction. In the work done by Zhang et al [4] ,[5] , the recursive code construction method was improved In the work done by Fridrich et al, [4] ,[6] the compressive features of original cover where first extracted and then compressing them loss Lessly so that spare space can be saved for embedding auxiliary data. Another method is based on Difference Expansion (DE) [7], where the difference of each pixel group is expanded.

The histogram shift (HS)[8],method is a promising method in which space is saved for data embedding by shifting the bins of histogram of gray values. The methods [9] – [13], combined DE or HS to residuals of the image.

The work done by A J Menezes [14], suggests a popular method for image encryption in [15] , Hwang et al proposed a reputation- based trust-management scheme enhanced with data coloring and software watermarking. To separate the data extraction from image decryption, Zhang [20] emptied out space for data embedding following the idea of compressing encrypted images [16] ,[17]. The method in [20] compressed the encrypted LSBS to vacate room for additional data by finding syndromes of a party-check matrix. In the methods proposed in [18] – [20], a content owner encrypts the original image using a standard cipher with an encryption key. After generating the encrypted image, the content owner hands over it to the data hider and the data hider can embed some auxiliary data into the encrypted image by loss lessly vacating some room according to a data hiding key.

In the work done by kede ma [21], histogram shifting method was used for data embedding. But the PSNR was quite low. Wien and Tung - Show [22] , proposed a reversible data hiding method based on image interpolation. But this method rendered low performance. Diljith [23], proposed a prediction –error expansion and histogram shifting method for reversible data hiding. Jessica [24] developed lossless watermarking techniques that preserve the file size. The major drawback was high computation time. Ching - Yu yang [25] developed a simple reversible data hiding scheme based on the integer wavelet transform.

Revised Version Manuscript Received on December 24, 2016.

Revathi Nath H A, M.Tech. Student, Department of Electronics and Communication, College of Engineering Trivandrum (Kerala) India.

Jeena R S, Assistant Professor, Department of Electronics and Communication Engineering at College of Engineering Trivandrum, (Kerala) India.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

III. PROPOSED METHOD

In this work reversible data hiding and reservation of room for data is implemented using the standard RDH algorithm such as [10], [11], and the data to be hidden is encrypted using the Advanced Encryption Standard (AES) [26].

The Framework of the entire process is shown in figure a and b.

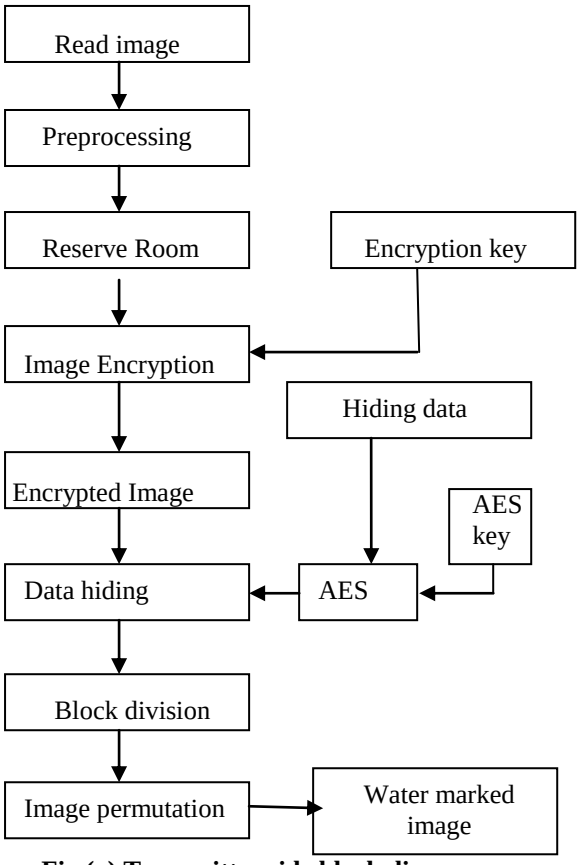


Fig.(a) Transmitter side block diagram

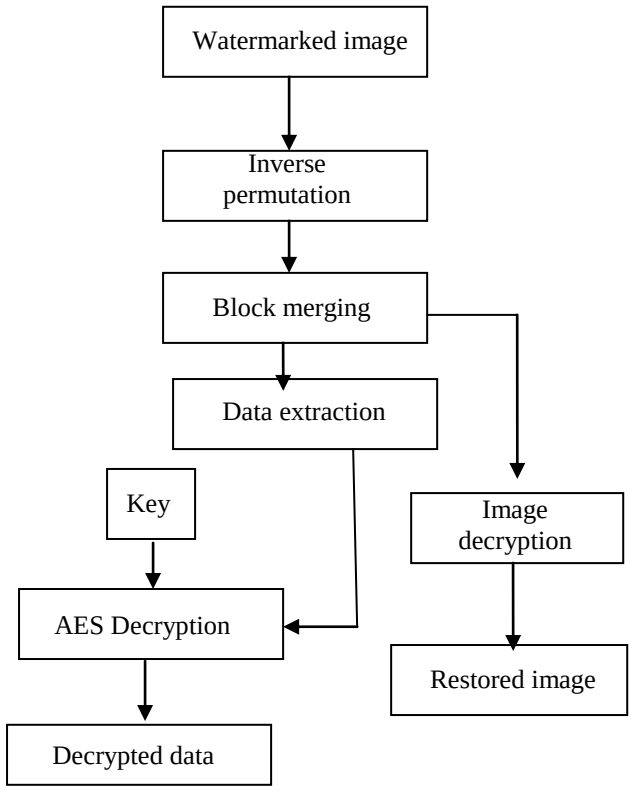


Fig.(b) Receiver side block diagram

Methodology of the proposed method is described below.

Here the original image is partitioned into two parts X and Y, then the LSBs of X are reversibly embedded into Y, so that the LSBs of X can be used for accommodating messages. The rearranged image is then encrypted. At the data hider side, the data hiding key is generated and encrypted using an advanced encryption system .once the data hider acquires the encrypted image, he can embed data into it. The image containing data is then divided into blocks and permuted. This marked image is transmitted. At the receiver side, when the database manager gets the data hiding key, data will be extracted from the encrypted image. The original image can be recovered using the encryption key.

A. Steps Involved at the Transmitter Side

1. Reserving Room

Image encryption takes place at the owner side. First the original image will be taken. The original image C is partitioned into two blocks: say X and Y. First the owner has to extract from the original image certain overlapping blocks. The no of blocks is determined by the size of the message to be embedded.

In detail, every block consists of m, rows, where $m = \lceil r/N \rceil$ and the number of blocks can be computed through for each block, a function P is defined to measure its first order smoothness.

$$P = \sum_{u=2}^{m} \sum_{v=2}^{n-1} \left| C_{u,v} - \frac{C_{u-1,v} + C_{u+1,v} + C_{u,v+1}}{4} \right|$$

The block with higher value of P is selected as X and those with lower values of P as Y.

Now the LSB planes of X are reversibly embedded into the LSB planes of Y using the following steps defined in the standard algorithm.

1) Get an original image R.
2) Find the interpolated values R^1 of the image R.
3) Find the interpolation error e by taking the difference between R and R^1
4) Obtain the portion of image say X whose LSBS are to be embedded into Y .it is the key image.
5) If the interpolation error e is odd and X is 1 then add bit 1 to e otherwise nothing has to be done.
6) If e is even and X is 0 then add bit 0 to e otherwise do nothing.
7) Repeat the steps 3-6 to get the self reversible embedded Image.

The self reversible embedded images C is then encrypted by performing modulo 256 additions with a standard stream cipher. The encrypted image can be used for hiding the message.

2. Data Encryption using AES

The data to be hidden is encrypted using the advanced encryption system.

Steps in AES encryption

1) The input to the encryption algorithm is a single 128 bit Block
2) The plain text is converted into an input state matrix
3) Enter an encryption key of 16 bytes is expanded into words.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

4) The cipher consists of 10 rounds for a 16 byte key
5) The first step in the algorithm is initial transformation in Which the input state matrix is added to round 0 key.
6) The output state matrix undergoes 4 transformations in the Next round.
7) After undergoing 10 rounds of transformations it is Possible to obtain a cipher text.

The AES encrypted data is to be hidden in that part of the image that was already reserved in the image.

3. AES structure

The cipher takes a plaintext block size of 128 bits, or 16 bytes. The key length can be 16,24,or 32 bytes(128,192,or 256 bits).the algorithm is referred to as aes-128,aes-192, or aes-256, depending on the key length.The input to the encryption and decryption algorithms is a single 128-bit block. In FIPS pub 197, this block is depicted as a square matrix of bytes. This block is copied into the state array, which is modified at each stage of encryption or decryption. After the final stage, state is copied to an output matrix. similarly; the key is depicted as a square matrix of bytes. This key is then expanded into an array of key schedule words.. Each word is four bytes, and the total key schedule is 44 words for the 128-bit key. Note that the ordering of bytes within a matrix is by column. So, for example, the first four bytes of a 128-bit plaintext input to the encryption cipher occupy the first column of the in matrix, the second four bytes occupy the second column, and so on. Similarly, the first four bytes of the expanded key, which form a word, occupy the first column of the w matrix.

The cipher consists of rounds, where the number of rounds depends on key length: 10 rounds for a 16 byte key, 12 rounds for a 24-byte key, and 14 rounds for a 32-byte key. The first rounds consist of four distinct transformation Functions: Sub Bytes, Shift Rows, Mix Columns, and Add Round Key, which are described subsequently. The final round contains only three transformations, and there is a initial single transformation (Add Round Key) before the first round,
Which can be considered round0.each transformation takes one or more matrices as input and produces a matrix as output. Also, the key expansion function generates round keys, each of which is a distinct matrix. Each round key serve as one of the inputs to the Add Round Key transformation in each round.

4. Data hiding

Each bit form the right end of the data to be embedded is concatenated with the first 6 MSB bits of each pixel of the encrypted image. The resultant value is converted in to decimal and saved as a pixel in the image. The image is then converted in to a single column matrix.

5. Image Permutation

The image after data hiding can be permuted. This is done by converting the image in to four blocks each of size 128*128 and then rearranging the position of the blocks. This technique of image permutation ensures a more secure form of data transmission.

B. Steps involved at the receiver side

At the receiver side the permuted image is rearranged to get the original encrypted image. After that image is further processed for data extraction and image recovery.

1. Data extraction

Steps involved:

1) Read each pixel value from encrypted image
2) Obtain last 2 bits of each pixel
3) Combine 2 LSB of 4 Pixel to obtain 1 byte of hidden data.
4) Repeat the steps until all hidden data bytes are extracted

2. Image decryption

A modulo 256 subtraction is performed on the encrypted image using the encryption key, there by recovering the original image.

IV. EXPERIMENTAL RESULTS

By using AES in reversible data hiding it was possible to improve the PSNR to up to 65db, whereas in all the previous methods the PSNR was nearly 40db.Also the permutation of image has led to a technique that would ensure a secure transmission.

Standard image 'Barbara' is shown in Fig (c), to demonstrate the feasibility of proposed method. Fig(d) shows the partitioned image, Fig(e) shows the self reversible embedded image, Fig(f) shows the concatenated image Fig(g) shows the encrypted image, Fig(h) shows the transmitted image after data embedding and Fig(i) shows the reconstructed image which is exactly similar to that of the original image.

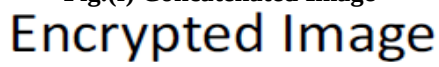
Fig. (c) Original Image

Fig.(d) Partitioned Image

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Fig. (e) Self Reversible Embedded Image

Fig.(f) Concatenated Image



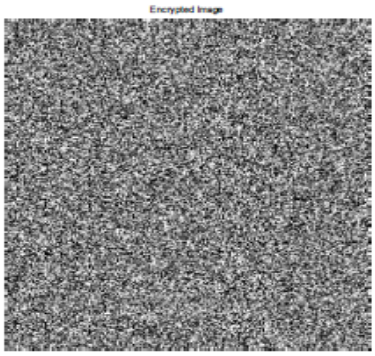


Fig.(g) Encrypted Image

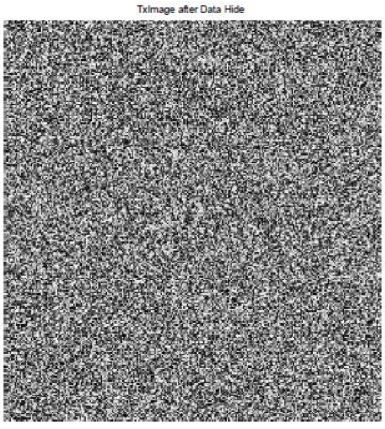


Fig.(h) Transmitted Image After Data Transfer

Fig.(i) Reconstructed image

Table (a) Shows the PSNR Comparison with the Existing Method for Various Image Samples

Title	Image	PSNR(db)	MSE
Existing method by Kede Ma[21]	Barbara	40	0.01339
Proposed method	Barbara	65	0.011
Existing method by Kede Ma[21]	Airplane	41	0.041
Proposed method	Airplane	67.059	0.01281
Existing method by Kede Ma[21]	Boat	38.07	0.0412
Proposed method	Boat	65	0.002
Existing method by Kede Ma[21]	Baboon	37.12	0.03251
Proposed method	Baboon	67.192	0.024
Existing method by Kede Ma[21	Lena	39.125	0.0341
Proposed method	Lena	66.987	0.01311

Table (a) PSNR comparison with the existing method for various image samples

V.CONCLUSION

Reversible data hiding technique has now been used widely because of the efficiency of this technique to hide data by encrypting the image on which data is embedded thereby ensuring a secure form of data transmission. In all the previous methods only the image holding data was encrypted as opposed to which I proposed in this paper by encrypting the data to be hidden. Thus it is possible for the data hider to ensure security of data transmission as the data holding encrypted image is again block divided and permuted to another form so that it becomes impossible for a fake user to detect the original image. The proposed method can be applied to all standard images and achieve excellent performance without loss of secrecy.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

REFERENCES

1. W. Bender, D.Gruhl, N.Morimoto and A.Lu., Techniques For Data Hiding, IBM Systems Journal ,Vol.35,Pp 313-336,1996
2. C.W.Honsinger, P.W.Jones, M.Rabbani and J.C.Stoffel, Lossless Recovery Of An Original Image Containing Embedded Data, U S Patent, Ed, 2001
3. T.Kalker and F.M.Willems. "Capacity bounds and code construction for reversible datahiding," in proc.14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71-76.
4. 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.
5. W. Zhang, B. Chen, and N. Yu, " Improving various reversible data hiding shemes via optimal codes for binary covers," IEEE Trans. Image Process., vol. 21, no. 6, pp. 2991-3003, Jun. 2012
6. J. Fridric h and M. Goljan, "Lossless data embedding for all image for-mats," 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. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible Waterm- arking algorithm using sorting and prediction," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989-999, Jul. 2009.
14. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC, 1996
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.
16. M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramachandran, "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, pp. 1097-1102, Apr. 2010.
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.
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. Kese Ma, Weiming Zhang, Xianfeng Zhao, "Reversible data hiding in Encrypted images by reserving room before encryption" IEEE Transactions on information forensics and security, Vol.8, No.3, March 2013
22. Wien Honga, Tung-Shou Chen, Reversible Data Embedding For High Quality Images Using Interpolation And Reference Pixel Distribution Mechanism., Elsevier Journal For Visual Image R.22(2011) 131-140.
23. Diljith.N.Thodi And Jeffrey.J.Rodriguez, Expansion Embedding Techniques For Reversible Watermarking, IEEE Transactions On Image Processing, Vol.16, No.3, March 2007
24. Jessica Fridrich, Niroslav Goljan, Lossless Data Embedding With File Size Preservation, Proc. SPIE 5306, Security, Stenography And Watermarking Of Multimedia contents Vi, 354(June22,2004)
25. Ching -Yu Chang, Chih - Hung Lin And Wu - Chih Hu, Reversible Data Hiding For High Quality Images Based On Integer Wavelet Transform, Journal Of Information Hiding And Multimedia Signal Processing Ubiquitous International, Volume 3,No.2, April 2012
26. M.Pitchchaiah, Philenon Daniel, Praveen, Implementation Of Advanced Encry- ption Standard Algorithm, International Research Volume 3,Issue 3, March -2012.
27. Miscellaneous Gray Level Images (Online) Available: http:// decsai. ugr.es/ cvg/ dbimagenes/ g512.php

AUTHORS

Revathi Nath H A is currently pursuing M.tech degree in Signal Processing with the Department of Electronics and Communication Engineering, at College of Engineering Trivandrum, Kerala. She received her B.tech degree from University of Kerala in the year 2009. She is an Assistant Professor at College of Engineering Muttathara under CAPE and is doing evening M.tech at College of Engineering Trivandrum. Her research interest includes Digital image processing and Communication Engineering.

Jeena R S is an Assistant Professor in the Department of Electronics and Communication Engineering at College of Engineering Trivandrum, Kerala. Her research areas include Digital Image Processing and Medical Imaging.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.