International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.2, Issue.4, July-Aug. 2012 pp-1951-1954 ISSN: 2249-6645

Symmetric Key Cryptography on Images in AES Algorithm and Hiding Data Losslessly

T. Arumuga Maria Devi[1], Sabitha.S[2]
Assistant Professor, Dept. of CITE M.Tech Student, Dept. of CITE
Centre for Information Technology and Engineering,
Manonmaniam Sundaranar University, Tirunelveli

Abstract: *Reversible (lossless) data embedding (hiding) has drawn lots of interest recently. Being reversible, the original cover content can be completely restored. This paper proposes a novel reversible data hiding scheme with a lower computational complexity and can be used in applications where both the image and the hidden information is highly confidential. It consists of three phases –AES image encryption, data embedding and data extraction/image-recovery phases. Here, the encrypted image is made highly secured by using an AES (Advanced Encryption standard) stream cipher. Although a data-hider does not know the original image content, he can embed additional data into the encrypted image using the data hiding key. A receiver may firstly decrypt the encrypted image using the encryption key. This decrypted image is similar to the original image. With the data-hiding key, the embedded data can be correctly extracted while the original image can be perfectly recovered.*

Index Terms: *AES encryption – Data Embedding – Image Recovery.*

I. INTRODUCTION

Data hiding is a technique that is used to hide information in digital media such as images, audio, video etc. The information that is hidden depends upon the purpose of application. Owing to data hiding, some distortion may occur in the original cover medium and cannot be inverted back to the original medium. Such a data hiding is called lossy data hiding. But in applications such as medical image system, law enforcement, remote sensing, military imaging etc it is desired to recover the original image content with greater accuracy for legal considerations. The data hiding scheme that satisfies this requirement is called reversible or lossless data hiding. Reversible data hiding was first proposed for authentication and its important feature is reversibility. It hides the secret data in the digital image in such a way that only the authorized person could decode the secret information and restore the original image. Several data hiding methods have been proposed. The performance of a reversible data embedding algorithm is measured by its payload capacity, complexity, visual quality and security. Earlier methods have lower embedding capacity and poor image quality. As the embedding capacity and image quality improved, this method became a covert communication channel. Not only should the data hiding algorithm be given importance. The image on which the data is hidden should also be highly secured.

In this paper, both the cover image and the secret data are given equal importance. The visual quality after encryption as well as the PSNR is also improved. It consists of three phases – AES image encryption, data embedding and data extraction/image-recovery phases. In the first phase, the data of original image are entirely encrypted by an AES (Advanced Encryption standard) stream cipher. The data encryption standard (DES) is weak due to smaller key size, 56 bit. Whereas AES can use three different key sizes: 128, 192 and 256 bits. In the second phase, although a data-hider does not know the original image content, he can embed additional data into the encrypted image by modifying a part of encrypted data using the data hiding key. In the third phase, a receiver may firstly decrypt the encrypted image containing the embedded data using the encryption key. This decrypted image is similar to the original image. With the data-hiding key, the embedded data can be correctly extracted while the original image can be perfectly recovered.

II. EXISTING METHODS

In Difference Expansion method [1], the differences between two adjacent neighboring pixels are doubled to generate a new least significant bit where the new data is hidden providing large information package. In Generalized DE based method [2], Tian's pixel-pair difference expansion was extended using difference expansion of vectors. In Generalized LSB method [3], the cover image undergoes lossless compression to create a space where the new data is added. Thus the PSNR is reduced. In Histogram shift mechanism [4], the pixel values at the zero and the peak points of the histogram are modified to add the new data. In wavelet technique and sorting [5], Kamstra *et al.* improved the location map by sorting possible expandable locations. In integer-to-integer wavelet transform method [6], LSB substitution and bit shifting was done to add new data to the wavelet coefficients obtained from integer-to-integer wavelet transform. In [7], Wang *et al.* uses 2-D vector maps in the cover image. In [8], Thodi *et al.* made better use of redundancy of neighbouring pixels by using payload independent overflow location map. But the compressibility is undesirable in some image types. In [9], Hu *et al.* solved the problem in [8] by constructing an efficient payload dependent overflow location map which has good compressibility. In [10], Hong et al. proposes the method of orthogonal projection and modifies the prediction error values to add the secret data. In [11], the data is hidden by modifying a part of the encrypted image. But the encrypted image is not highly secured and also the PSNR value is low.

III. PROPOSED SCHEME

Figure 1 shows the block diagram of the proposed scheme. There are three phases – AES image encryption, data embedding and data extraction / image-recovery phases.

AES Image Encryption

The original image is in uncompressed format. Firstly, if the image is a colour image, then encrypt each red, green and blue channels otherwise convert it into a gray scale image with each pixel value ranging in between [0-255] represented by 8 bits and then encrypt the image. The pixel bits are represented as $b_{i,j,0}$, $b_{i,j,1}$, ...$b_{i,j,7}$.

AES is a substitution-permutation network, which is a series of mathematical operations that uses substitutions and permutations such that each output bit depends upon every input bit. The AES algorithm consists of a set of processing steps repeated for a number of iterations called rounds. The number of rounds depends upon the key size. Each round is a cipher with four operations except the last round which is having only three operations. First, AddRoundKey step is performed where the incoming data and the key are added together. Then it performs the round operation. Figure 2 shows the operations in each round [12].

SubByte: each byte of the block is replaced by its substitute in the substitution box(S-box).

ShiftRow: bytes in last three rows are cyclically shifted left over different number of offsets.

MixColumn: Each column is multiplied with a known matrix. Multiplying by 1 means leaving unchanged, by 2 means shifting byte to the left and by 3 means shifting to the left and then performing XOR with the initial unshifted value.

AddRoundKey: XOR with the actual data and the subkey. In final round there is no MixColumn step. These steps are done for 10 rounds. Thus it becomes difficult for the attacker to obtain any information about the original content from the encrypted image.

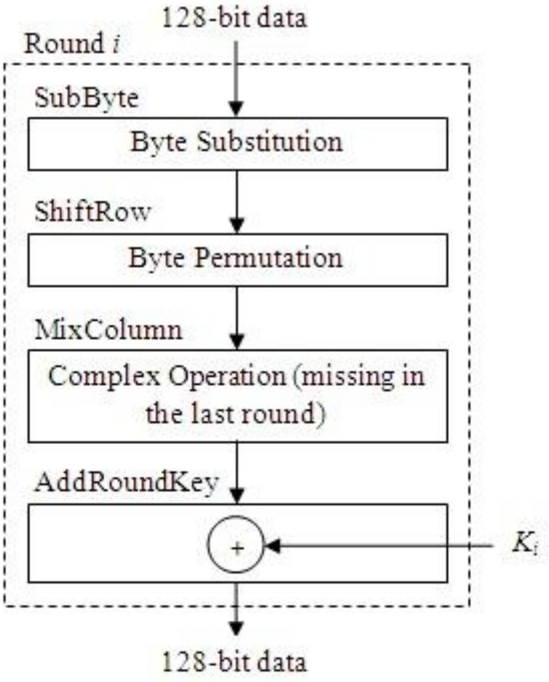


Figure 2. AES Encryption

Data Embedding

In this phase, even though a data hider doesn’t know the original content of the image he can embed the secret data into the encrypted image by modifying a small part of the encrypted image.

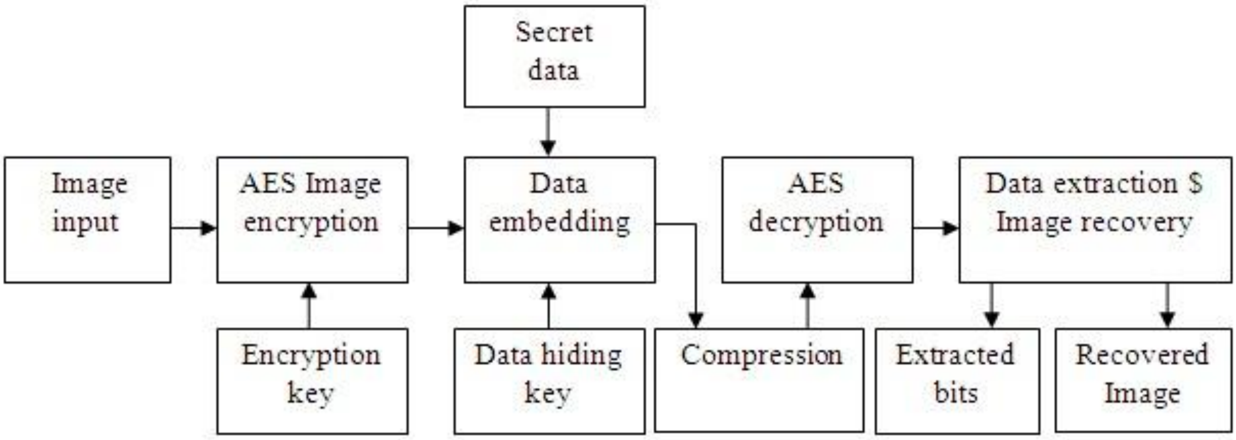


Figure 1. Block Diagram

Firstly, the encrypted image is divided into several segments of block size s x s. Each block is then used to carry one bit. The sum total of the pixel values of each block is calculated. It is then compared with a threshold value which is set manually such as to obtain greater PSNR value. The data is then added to the block whose sum of the pixel value is greater than the threshold value by xor-ing the original pixel bits with the secret data.

In order to receive the image properly at the receiver, the image is compressed using wavelet transform which is a lossless compression method.

Data Extraction and Image Recovery

In this phase, the image is decrypted using AES decryption. The steps are AddRoundkey, inverse subbyte using inverse S-box, inverse shiftrow where the bits are cyclically shifted towards right, inverse mixcolumn step using inverse P-box, and AddRoundkey.

The average energy of error between the original and decrypted pixel value is,

$$E_A = {}^{1}/_{8} \sum_{u=0}^{7}[u-(7-u)]^2 \qquad [1]$$

u is the no. of bits.

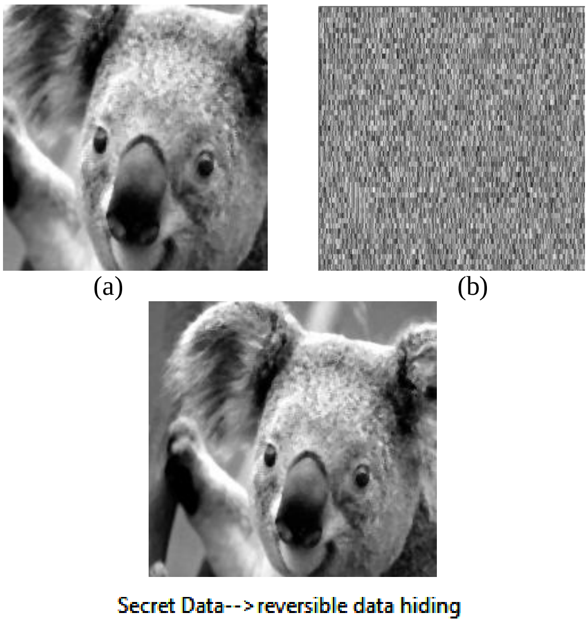
PSNR of the decrypted image,

$$PSNR = 10\log_{10}\frac{255^2}{E_A/2} = 55.11dB \qquad [2]$$

The decrypted image is segmented into blocks. The sum total of pixel values of each block is found then. For each block, if this value is greater than the threshold value then the data is hidden in that block and is extracted by xor-ing the original bits with the decrypted bits. Finally combine the extracted bits to obtain the secret data and collect the recovered blocks to form the original image.

IV. EXPERIMENTAL SETUP

Figure 3(a) shows the original cover media used. 3(b) shows the encrypted image. 3(c) shows the decrypted image carrying the secret data and the value of PSNR caused by data embedding is 55.11dB. At last, the embedded data was successfully extracted and the cover image was recovered. Figure 4 shows the PSNR with respect to the data set values.



(a) (b)

(c)

Figure 3. (a) Original image, (b) Encrypted image, (c) Decrypted image with the secret data

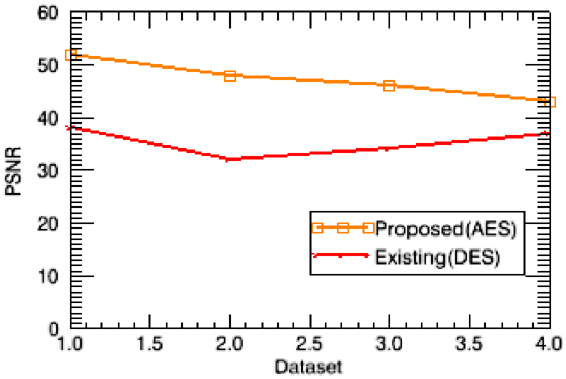


Figure 4. PSNR Vs Data set

V. CONCLUSION

In this work, the cover medium is highly secured for reversible data hiding with lower computational complexity. The data of the original image is completely encrypted by AES stream cipher which overcomes the disadvantages of DES stream cipher. Even though the data hider doesn't know the original content, he can hide the data by modifying a part of the encrypted image. The receiver decrypts the image using AES decryption. The PSNR value of the decrypted image is high. The hidden data is then extracted with the data hiding key and the original image is recovered. This work may be applicable where both the hidden data and the cover media are highly confidential.

VI. ACKNOWLEDGMENT

The authors would like to thank the members of the Dept. of CITE, M S University, Tirunelveli for various algorithms used in this research, and all the people who helped in preparing and carrying out the experiments and data collection.

REFERENCES

[1] Jun Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits System and Video Technology*, vol. 13, no. 8, pp. 890-896, Aug. 2003.

[2] A.M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," *IEEE Trans. Image Process.*, vol. 13, no. 8, pp. 1147-1156, Aug. 2004.

[3]. M.U.Celik, G.Sharma, A.M Tekalp, and E. Saber, "Loseless Generalized-LSB data embedding," *IEEE Trans. Image Process.*, vol. 14, no. 2, pp. 253-266, Feb. 2005.

[4]. Z. Ni, Y.Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits System and Video Technology*, vol. 16, no.3, pp. 354-362, Aug. 2006.

[5]. L. Kamstra and H. J. A. M. Heijmans, "Reversible data embedding into images using wavelet

techniques and sorting," *IEEE Trans. Image Process.*, vol. 14, no.12, pp. 2082-2090, Dec. 2005.

[6]. S. Lee, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," *IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 321-330, Sep. 2007.*

[7]. X. T. Wang, C. Y. Shao, X. G. Xu and X. M. Niu "Reversible data hiding scheme for 2-D vector maps based on difference expansion," *IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 311-320, Sep. 2007.*

[8]. 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.

[9]. Y. Hu, H.K. Lee, and J. Li, "DE based Reversible data hiding with improved overflow location map," *IEEE Transactions on Circuits System and Video Technology*, vol. 19, no.3, pp. 250-260, Feb. 2009.

[10]. W. Hong, T. S. Chen, Y. P Chang, C. W. Shiu, "A high capacity reversible data hiding scheme using orthogonal projection and prediction error modification," *Signal Processing.*, vol. 90, no.12, pp. 2911-2922, May. 2010

[11]. Xinpeng Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Processing.*, vol. 18, no.4, pp. 255-258, April. 2011

BOOKS

[12]. Data Communications and Networking, Behrouz A. Forouzan, fourth edition.

AUTHORS

S. Sabitha received B.Tech. Degree in Electronics and Communication Engineering from Mount Zion College of Engg., Mahatma Gandhi University, Kerala in 2010. Currently, she is doing M.Tech in Computer and Information Technology in Manonmaniam Sundaranar University, Tirunelveli. Her research interests include Signal and Image Processing and Software Engineering.

T. Arumuga Maria Devi received B.E. Degree in Electronics and Communication Engineering from Manonmaniam Sundaranar University, Tirunelveli, India in 2003, M.Tech degree in Computer and Information Technology from Manonmaniam Sundaranar University, Tirunelveli, India in 2005 and worked as Lecturer in the Department of Electronics and Communication in Sardar Raja College of Engineering. Currently, she has submitted thesis for Ph.D in Information Technology-Computer Science Engineering and also is the Assistant Professor of Centre for Information Technology and Engineering of Manonmaniam Sundaranar University. Her research interests include Signal and Image Processing, Multimedia and Remote Communication.