Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 9, Issue. 3, March 2020, pg.236 – 243

Separable Reversible Data Hiding in Encrypted Image Using Dual Data Embedding with Histogram Shifting

Anusha S
Dept. of Computer Science and Engg.
Rajalakshmi Engineering College, Chennai
anusha.s.2016.cse@rajalakshmi.edu.in

Arul Mozhi P
Dept. of Computer Science and Engg.
Rajalakshmi Engineering College, Chennai
arulmozhipanchatsaram@gmail.com

Elakkiya N
Dept. of Computer Science and Engg.
Rajalakshmi Engineering College, Chennai
elakkiyanarayanan55@gmail.com

Vijayakumar R
Assistant Professor
Dept. of Computer Science and Engg.
Rajalakshmi Engineering College, Chennai
vijayakumar.r@rajalakshmi.edu.in

Abstract — In Digital Communication, the information being transferred from the sender to receiver is not secure. Intruders attempt to steal data at any moment. Maintaining security and confidentiality is much important. For protecting privacy and security from unauthorized users, masking the data in the network is essential. Data hiding in image is mainly used to cover the privacy. It uses some manipulation methods to hide secret data. Histogram Shifting enhances the data hiding capacity. Image scanned pixel by pixel in order to embed data. Most reversible data hiding methods not involve the sender for data embedding. In this paper, secure separable reversible data hiding is used along with dual data embedding i.e. embedding data before and after encryption. Separable reversible data hiding technology in encrypted image (SRDH-EI) also has been developed extensively because of its better practicability. The experimental results showed that our proposed scheme achieved better hiding capacity than the other schemes.

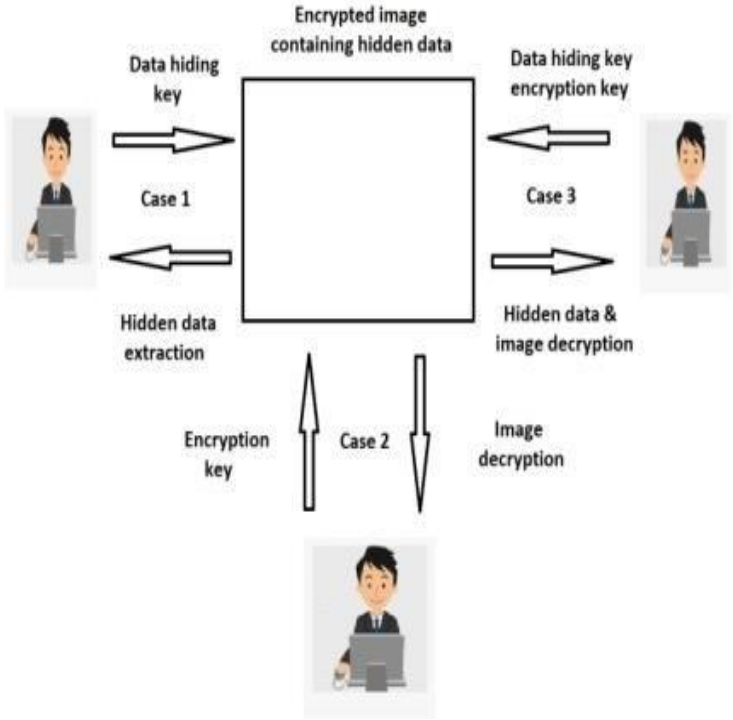
Keywords — Separable reversible data hiding, dual data embedding

I. Introduction

In advent of technology, more and more digital images are shared, stored and processed in the cloud. However, these images can be subject to various risks in the process of transmission over the network, such as stealing, tampering and copying. Thus, the issue of protecting the privacy of images and data in the cloud platform network has been of significant concerned to researchers [1][8]. In many cases, it is necessary to encrypt the image first to protect its privacy and then hide the important data in the encrypted image. This approach has led to a new research direction of data hiding, i.e. separable reversible data hiding technology in encrypted images. Since SRDH- EI provides an important combination of encryption and data hiding, it makes private data doubly secure in the process of data processing. With the increased use of cloud services, SRDH-EI has become one of the researches focuses for protecting the privacy of data in the cloud environment.

First, the original image was encrypted by using Advanced Encryption Standard (AES) and then encrypted image was divided into several blocks, and one bit of secret data was embedded in each block. Subsequently, the data extraction and restoration of the image were achieved by analyzing the local standard deviation during decryption of the image. To encrypt the original image using exclusive-or (XOR) operation and it embedded one bit of secret data by flipping the three least significant bits (LSBs) of the half pixels in each block of the encrypted image. [2] Random diffusion, accurate prediction strategy is applied to efficiently use the correlation of pixels in order to obtain higher hiding capacity in encrypted images. It extended the smoothness function in Zhang's scheme by considering the pixels in the borders of a block, and experiments have shown that this reduced the average extracted-bit error rate when the block size was appropriate. A new framework the encrypted image can be obtained by block permutation and the pixel bit-level XOR operation, and then the secret data can be embedded into the encrypted image by using the RDH methods that have been proposed previously

In order to improve the practicality of the scheme, researchers designed separable RDH-EI (SRDH-EI) schemes the three different separation cases for the receiver. When the receiver obtains the stego-images, he or she can extract secret bits or recover images according to the different needs that exist and the keys they have. [3] In 2012, Zhang proposed on SRDH-EI scheme based on LSB compression. Subsequently, inspired by the distributed source coding, [4] Qian and Zhang proposed a novel scheme of SRDH-EI. First, the original image is encrypted by using a stream cipher, and a series of selected bits taken from the encrypted image were compressed by using low-density parity-check codes to make room for the secret data. The receiver can extract the secret data or decrypt the protected original image according to the key he or she permits. [5] First, the non- overlapping blocks of the original image were encrypted by using an analogous stream-cipher and block permutation; second, encrypted image blocks were divided into two sets that corresponded to the smooth and complex regions in the original image; and third, the LSBs of the blocks corresponding to the smooth regions were compressed to create embedding room. [6] SRDH-EI using parametric binary tree labelling. A small number of pixels were used as reference values to calculate the prediction error of most pixels, and a parametric binary tree labelling method was proposed to distinguish all prediction errors. The data-hider can embed the secret data according to different prediction errors in the encrypted image with the tag value. [7] High capacity SRDH-EI scheme was proposed.



In this paper, we propose a separable reversible data hiding scheme in encrypted image based on dual data embedding along with histogram shifting. SRDH-EI methods can be classified into two classes: vacating room after encryption (VRAE) and vacating room before encryption (VRBE). In VRAE methods, the remote server generates embedding room by modified some pixel values of the encrypted image directly. VRAE methods can be further grouped into three categories, i.e., data extraction in plaintext domain, data extraction in the cipher domain, and data extraction in both domains. These VRAE methods achieve decent performances of RDH in encrypted image. But since the entropy of the encrypted image is usually maximized because of encryption, the net payloads are relatively low. In contrast, VRBE methods can achieve higher payloads by utilizing the spatial correlation of the original image to vacate embedding room before image encryption. Embedding room vacates before image encryption by embedding data into the estimated error of pixels. Though promising in embedding performance, SRDH-EI methods usually ignore the requirements of reversible data embedding for the image owner. A new RDH-EI method to allow dual data embedding, which includes data embedding for the image owner. However, the vacated room for data embedding in encrypted image is relatively small and fixed, and the technique of generalized reversible contrast mapping introduces more distortion when vacating room for encrypted image and embedding data for image owner. The embedded data by the image owner and the remote server can be exactly extracted and the original image can be perfectly recovered after image decryption.

A. IMAGE ENCRYPTION

The original image is encrypted by using symmetric key cryptographic algorithm such as AES algorithm. Each block in the image is first encrypted by using the encryption key Ke which is of 128 bit size. The data is then divided into four basic blocks. These blocks operates on array of bytes and these are then organized as 4*4 matrix which is known as state. Encryption takes place after passing the data into several rounds. During the cipher creation, input array is copied into state array a,

$$s[r,c] = in[r+4c] for\ 0 \le r < 4\ and\ 0 \le c < N_b$$

At the end of cipher creation the state is copied ino output as:

$$out[r+4c] = s[r,c] for\ 0 \le r < 4\ and\ 0 \le c < N_b$$

The remainder of this paper is organized as follows. The generalized integer transformation algorithm for SRDH is described in Section II. The details of the proposed RDH-EI method are proposed in Section III. Experimental results and analyses are provided in Section IV. Finally, this paper is concluded in Section V.

II. PROPOSED SYSTEM

Each round of the AES algorithm consists of several transformations. The transformations are:

1)SubByte transformation: It is a nonlinear byte transformation technique. This technique is performed on each byte of the state using a substitution box called (S-Box). The S-box is invertible and can be constructed transformations. Take the multiplicative inverse in the finite field GF(2^8)

2)Shiftrows transformation: In shiftrow transformation operations are performed on each row. Each row is cyclically shifted to left except the first row. Elements in the second rows is shifted to one position left. Each element in the third row is shifted to two positions left and every element in the fourth and final row is shifted to three positions left. The shift row transformation is done as: following affine transformation

3)Mixcolumns transformation: In this technique operations are performed on each columns. In this transformation each columns are considered as polynomials instead of numbers over GF(28) with a fixed polynomial a(x).

4)Add Round Key transformation: in add roundkey transformation the subkeys are combined with each state. Sub keys are derived from the main key and it has the same size as the state. The sub keys are then XOR ed with each state.

After performing each transformation, we finally obtain an encrypted image which can be decrypted using only the shared symmetric key.

B. DATA HIDING

The data hider obtains the encrypted image in which additional secret data is to be embedded. At first, the histogram of the encrypted image is generated. Histogram is a graphical representation which shows the intensity distribution of the image. For embedding additional data into the encrypted image the histogram of the image should be expanded to make space. The actual pixel value of the image ranges from [0-255] and after histogram expansion it becomes [0-511]. The maximum and minimum frequency values of each histogram are considered

and are stored in a separate array. For ever row and column the values of histogram are shifted to one position to the right. It is to these position additional bits are embedded.

C. DUAL DATA EMBEDDING

The proposed method allows the server's secret data to be further embedded into the encrypted marked image, even if the remote server is not able to access the original image. The embedding process starts with locating the encrypted version of part A, denoted by AE.

Since AE has been rearranged to the front of Image, the remote server has direct access to read the 32-bits information in LSBs of the first
32 encrypted pixels to obtain the number of blocks to be embedded and the allowed eemembedding capacity. After that, the remote server just adopts LSB replacement to substitute the LSB-planes in AE with his additional data, which are encrypted by Key 2. This way, the marked encrypted marked image is generated. Without the data hiding Key 2, no one could extract the additional data the remote server embeds.

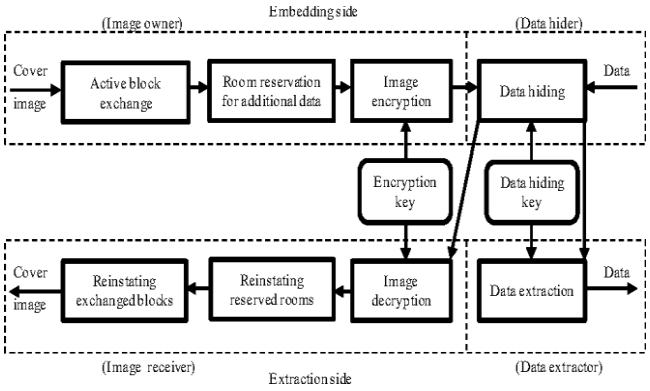
D. DATA EXTRACTION

On the recipient side, receivers may have different authorizations. Only with Key 2, the receiver can obtain the hidden server's data; with Encryption key and Key1, the receiver can get the hidden owner's data; if with Encryption key, the original image can be recovered perfectly. In general, with all the three keys, the two parts of additional data can be respectively extracted from Image and the original image can be recovered lossless.

E. IMAGE DECRYPTION

After getting the encrypted image containing embedded data the receiver can extract the image and recover the original data. Decryption of image can be performed using AES decryption algorithm. The steps in AES decryption algorithm are: 1)Inverse shift row transformation: In this transformation the row are shifted cyclically to the right. 2)Inverse subbyte transformation: It is the reverse of sub byte transformation 3)Inverse mixcolumn : Inverse of mixcolumn operation is performed. 4)Add round key After combining the output we finally obtain a decrypted image. The secret data which was hidden can also be extracted at the same time.

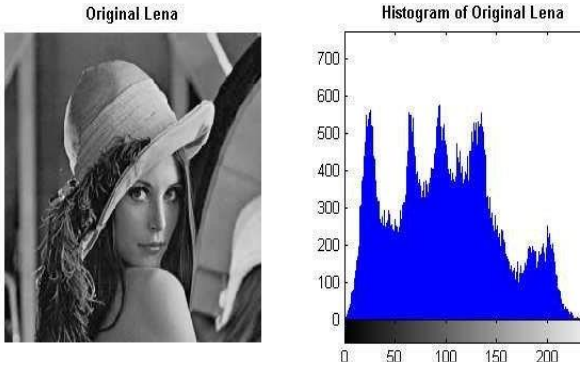
III. ARCHITECTURE



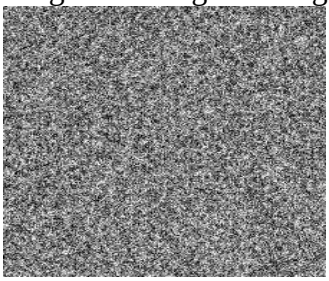
IV. EXPERIMENTAL RESULTS

The experiments have been carried out in standard gray scale images. The data which is to be hidden inside the image is a binary sequence which is generated using a pseudo random number generator.

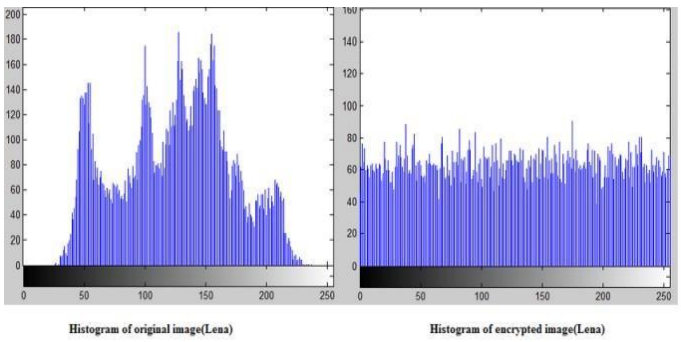
Original image



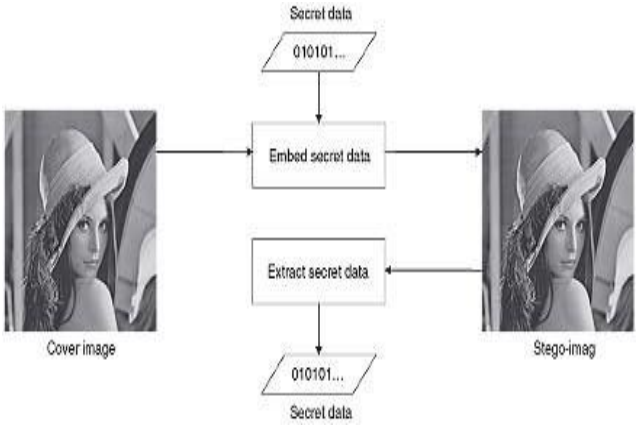
Histogram of original image



Encrypted image



Histogram of Encrypted image



Date embedding

Decrypted image

V. CONCLUSION

In this paper, we propose the content owner encrypts the image by using AES algorithm. The data embedding process is done on the encrypted domain. The image is embedded after shifting the values of the image histogram. Image histogram gives the pixel value distribution of the image. A new VRBE-based RDH-EI method which not only enables the remote server to embed data in image encrypted domain, but also allows the image owner to embed data before image encryption. Using the technique, the image owner embeds some additional data and vacates room for data embedding for encrypted domain before image encryption. After image encryption and uploading, it is easy for the remote server to embed data into the encrypted image by LSB replacement. On the recipient side, the embedded data by the image owner and the remote server can be extracted exactly, and the original image be recovered free of error after image decryption. Experimental results show that the proposed method is efficient in data embedding and effective in data security. When the receiver has the stego-images, the embedded secret data can be extracted completely or the original protected image can be recovered completely according to the key they possessed of. The reconstruction of the image and the extraction of the data are separate processes. The comparison of experimental results provided by the various approaches showed that our proposed scheme indeed achieved better hiding capacity than the other schemes. As a future expansion improvements can be made on the speed of the AES algorithm since it takes too much time for encryption and decryption.

REFERENCES

[1] L. Liu, L. Wang, Y. –Q. Shi, and C.-C.Chang, "Separable data-hiding scheme for encrypted image to protect privacy of user in cloud," *Symmetry*, vol. 11, no. 1, p. 82, Jan 2019.

[2] M. Li, D. Xiao, Z. Peng, and H. Nan, "A modified reversible data hiding in encrypted images using random diffusion and accurate prediction," *ETRI J.*, Vol. 36, no. 4, pp. 255-258, Apr. 2011.

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

[4] Z. Qian and X. Zhang, "Reversible data hiding in encrypted images with distributed source encoding," *IEEE Trans. Circuits Syst.Video Technol.*, vol. 26, no. 4, pp. 636–646, Apr. 2016.

[5] C. Qin, W. Zhang, F. Cao, X. Zhang, and C.-C. Chang, "Separable reversible data hiding in encrypted images via adaptive embedding strategy with block selection," *Signal Process.*, vol. 153, pp. 109–122, Dec. 2018.

[6] S. Yi and Y. Zhou, "Separable and reversible data hiding in encrypted images using parametric binary tree labeling," *IEEE Trans. Multimedia*, vol. 21, no. 1, pp. 51–64, Jan. 2019.

[7] D. Xu, K. Chen, R. Wang, and S. Su, "Separable reversible data hiding in encrypted images based on two-dimensional histogram modification,"" *Secur. Commun. Netw.*, vol. 2018, Feb. 2018, Art. no. 1734961.

[8] R. Vijayakumar, K. Selvakumar, K. Kulothungan, A. Kannan, "Prevention of Multiple Spoofing attacks with Dynamic MAC Address Allocation for Wireless Networks," 2014 International Conference on Communication and Signal Processing, Melmaruvathur, 2014, pp.1635-1639.

