IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue, 4, Feb 2019 E-ISSN: 2347-2693

Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography

S. Suvetha[1*], B. Vinodha[2]

[1,2]M.Sc Computer Science, Idhaya College for Women, Kumbakonam, Tamilnadu, India

Corresponding Author: suvetha13@gmail.com

Available online at: www.ijcseonline.org

***Abstract*—**This paper proposes a lossless, a reversible, and a combined data hiding schemes for ciphertext images encrypted by public key cryptosystems with probabilistic and homomorphic properties. In the lossless scheme, the ciphertext pixels are replaced with new values to embed the additional data into several LSB-planes of ciphertext pixels by multi-layer wet paper coding. Then, the embedded data can be directly extracted from the encrypted domain, and the data embedding operation does not affect the decryption of original plaintext image. In the reversible scheme, a preprocessing is employed to shrink the image histogram before image encryption, so that the modification on encrypted images for data embedding will not cause any pixel oversaturation in plaintext domain. Although a slight distortion is introduced, the embedded data can be extracted and the original image can be recovered from the directly decrypted image. Due to the compatibility between the lossless and reversible schemes, the data embedding operations in the two manners can be simultaneously performed in an encrypted image. With the combined technique, a receiver may extract a part of embedded data before decryption, and extract another part of embedded data and recover the original plaintext image after decryption.

***Keywords*—**Reversible data hiding, Lossless data hiding, Image encryption.

I. INTRODUCTION

Encryption and data hiding are two effective means of data protection. While the encryption techniques convert plaintext content into unreadable ciphertext, the data hiding techniques embed additional data into cover media by introducing slight modifications. In some distortion-unacceptable scenarios, data hiding may be performed with a lossless or reversible manner. Although the terms "lossless" and "reversible" have a same meaning in a set of previous references, we would distinguish them in this work.

A data hiding method is lossless if the display of cover signal containing embedded data is same as that of original cover even though the cover data have been modified for data embedding. For example, in [1], the pixels with the most used color in a palette image are assigned to some unused color indices for carrying the additional data, and these indices are redirected to the most used color. This way, although the indices of these pixels are altered, the actual colors of the pixels are kept unchanged. On the other hand, we say a data hiding method is reversible if the original cover content can be perfectly recovered from the cover version containing embedded data even though a slight distortion has been introduced in data embedding procedure. A number of mechanisms, such as difference expansion [2], histogram shift [3] and lossless compression [4], have been employed to develop the reversible data hiding techniques for digital images. Recently, several good prediction approaches [5] and optimal transition probability under payload-distortion criterion [6, 7] have been introduced to improve the performance of reversible data hiding.

Combination of data hiding and encryption has been studied in recent years. In some works, data hiding and encryption are jointed with a simple manner. For example, a part of cover data is used for carrying additional data and the rest data are encrypted for privacy protection [8, 9]. Alternatively, the additional data are embedded into a data space that is invariable to encryption operations [10]. In another type of the works, data embedding is performed in encrypted domain, and an authorized receiver can recover the original plaintext cover image and extract the embedded data. This technique is termed as reversible data hiding in encrypted images (RDHEI). In some scenarios, for securely sharing secret images, a content owner may encrypt the images before transmission, and an inferior assistant or a channel administrator hopes to append some additional messages, such as the origin information, image notations or authentication data, within the encrypted images though he does not know the image content. For example, when medical images have been encrypted for protecting the

patient privacy, a database administrator may aim to embed the personal information into the corresponding encrypted images. Here, it may be hopeful that the original content can be recovered without any error after decryption and retrieve of additional message at receiver side. In [11], the original image is encrypted by an exclusive-or operation with pseudo-random bits, and then the additional data are embedded by flipping a part of least significant bits (LSB) of encrypted image. By exploiting the spatial correlation in natural images, the embedded data and the original content can be retrieved at receiver side. The performance of RDHEI can be further improved by introducing an implementation order [12] or a flipping ratio [13]. In [14], each additional bit is embedded into a block of data encrypted by the Advanced Encryption Standard (AES). When a receiver decrypts the encrypted image containing additional data, however, the quality of decrypted image is significantly degraded due to the disturbance of additional data. In [15], the data-hider compresses the LSB of encrypted image to generate a sparse space for carrying the additional data. Since only the LSB is changed in the data embedding phase, the quality of directly decrypted image is satisfactory. Reversible data hiding schemes for encrypted JPEG images is also presented [16]. In [17], a sparse data space for accommodating additional data is directly created by compress the encrypted data. If the creation of sparse data space or the compression is implemented before encryption, a better performance can be achieved [18, 19]. images with symmetric cryptosystem in the above-mentioned RDHEI methods, a RDHEI method with public key cryptosystem is proposed in [20]. Although the computational complexity is higher, the establishment of secret key through a secure channel between the sender and the receiver is needless. With the method in [20], each pixel is divided into two parts: an even integer and a bit, and the two parts are encrypted using Paillier mechanism [21], respectively. Then, the ciphertext values of the second parts of two adjacent pixels are modified to accommodate an additional bit. Due to the homomorphic property of the cryptosystem, the embedded bit can be extracted by comparing the corresponding decrypted values on receiver side. In fact, the homomorphic property may be further exploited to implement signal processing in encrypted domain [22, 23, 24]. For recovering the original plaintext image, an inverse operation to retrieve the second part of each pixel in plaintext domain is required, and then two decrypted parts of each pixel should be reorganized as a pixel.

This paper proposes a lossless, a reversible, and a combined data hiding schemes for public-key-encrypted images by exploiting the probabilistic and homomorphic properties of cryptosystems. With these schemes, the pixel division/reorganization is avoided and the encryption/decryption is performed on the cover pixels directly, so that the amount of encrypted data and the computational complexity are lowered. In the lossless scheme, due to the probabilistic property, although the data of encrypted image are modified for data embedding, a direct decryption can still result in the original plaintext image while the embedded data can be extracted in the encrypted domain. In the reversible scheme, a histogram shrink is realized before encryption so that the modification on encrypted image for data embedding does not cause any pixel oversaturation in plaintext domain. Although the data embedding on encrypted domain may result in a slight distortion in plaintext domain due to the homomorphic property, the embedded data can be extracted and the original content can be recovered from the directly decrypted image. Furthermore, the data embedding operations of the lossless and the reversible schemes can be simultaneously performed in an encrypted image. With the combined technique, a receiver may extract a part of embedded data before decryption, and extract another part of embedded data and recover the original plaintext image after decryption.

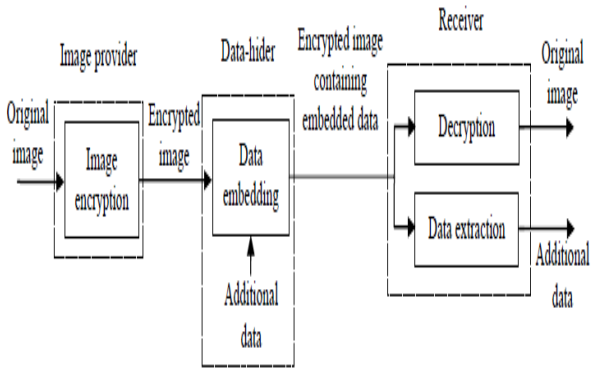

Figure 1: Sketch of lossless data hiding scheme for public-key-encrypted images

II. METHODOLOGY

The proposed scheme is made up of image encryption, data embedding and data-extraction/image-recovery phases. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Here comprehensive combination of image encryption and data hiding compatible with lossy Compression method will be used.

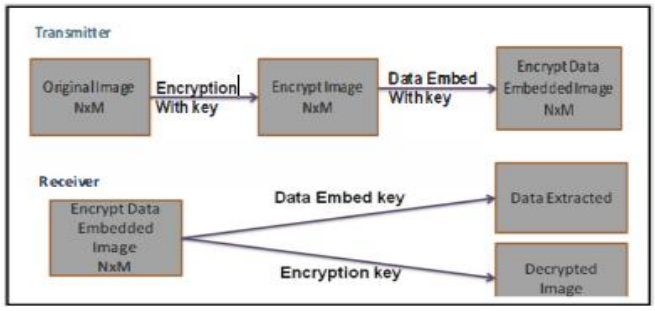

Figure 2: Block Diagram

Encryption and Decryption Algorithm
Image Decryption Algorithm
Step 1:
Find image size Colum and Row
Step 2:
Generate Key and mask
Keygen= Colum*Row*8
KeygenMask=Colum *Row*8
Step 3:
Putting value in mask
rvalue =0.30000 1;
x_N = 0;
forind = 2 : n
Encrypt Data
Embedded Image
NxM
x N = 1 - 2* rvalue * rvalue; % value generation for keymask< 0
if (x_N> 0.0)
bin_x(ind-l) = 1;
end
rvalue = x_N;
end
Step 4:
Divide by 8 the mask to same size of image
KeygenMask= KeygenMaskl8
Step 5:
Now apply bitxor operation between original image and KegenMask.

Encrypted image = bitxor(original image,KeygenMask);
Image Decryption Algorithm
Step 1:
Find Encrypted Image size Colum and Row
Step 2:
If KeyGen=Colum*Row
Further Decryption Process
Else
Decryption is not done
Step 3:
Generated KeygenMask at step 2 and 3 will be use here
Step 4:
Now apply bitxor operation between Encrypted image and KegenMask
Decrypted image = bitxor(Encrypted image,KeygenMask);

Table1: Comparison table

Image Encryption Methods	PSNR	MSE
AES Based Algorithm	30.2303	61.663
Block-Based Transformation	24.2485	244.4749
Proposed Method	**Inf**	**0**

III. EXPERIMENTAL RESULTS

Four gray images sized 512×512, Lena, Man, Plane and Crowd, shown in Figure 4, and 50 natural gray images sized 1920×2560, which contain landscape and people, were used as the original plaintext covers in the experiment. With the lossless scheme, all pixels in the cover images were firstly encrypted using Paillier cryptosystem, and then the additional data were embedded into the LSB-planes of ciphertext pixel-values using multi-layer wet paper coding as in Subsection 2.B. Table 1 lists the average value of embedding rates when *K* LSB-planes were used for carrying the additional data in the 54 encrypted images. In fact, the average embedding rate is very close to $(1-1/2K)$. On receiver side, the embedded data can be extracted from the encrypted domain. Also, the original plaintext images can be retrieved by direct decryption. In other word, when the decryption was performed on the encrypted images containing additional data, the original plaintext images were obtained.

With the reversible scheme, all pixels were encrypted after histogram shrink as in Subsection 3.A. Then, a half of ciphertext pixels were modified to carry the additional data as in Subsection 3.B, and after decryption, we implemented the data extraction and image recovery in the plaintext domain. Here, the low-density parity-check (LDPC) coding was used to expand the additional data as a bit-sequence in data embedding phase, and to retrieve the coded bit-sequence and the embedded additional data on receiver side. Although the error-correction mechanism was employed, an excessive payload may cause the failure of data extraction and image recovery. With a larger value of δ, a higher embedding capacity could be ensured, while a higher distortion would be introduced into the directly decrypted image. For instance, when using Lena as the cover and δ = 4, a total of 4.6×104 bits were embedded and the value of PSNR in directly

decrypted image was 40.3 dB. When using δ = 7, a total of 7.7×104 bits were embedded and the value of PSNR in directly decrypted image was 36.3 dB. In both of the two cases, the embedded additional data and the original plaintext image were extracted and recovered without any error. Figure 5 gives the two directly decrypted images. Figure 6 shows the rate-distortion curves generated from different cover images and various values of δ under the condition of successful data-extraction/image-recovery. The abscissa represents the pure embedding rate, and the ordinate is the PSNR value in directly decrypted image. The rate-distortion curves on four test images, Lena, Man, Plane and Crowd, are given in Figures 6, respectively. We also used 50 natural gray images sized 1920×2560 as the original plaintext covers, and calculated the average values of embedding rates and PSNR values, which are also shown as a curve marked by asterisks in the figure. Furthermore, Figure 7 compares the average rate-PSNR performance between the proposed reversible scheme with public-key cryptosystems and several previous methods with symmetric cryptosystems under a condition that the original plaintext image can be recovered without any error using the data-hiding and encryption keys. In [11] and [12], each block of encrypted image with given size is used to carry one additional bit. So, the embedding rates of the two works are fixed and low. With various parameters, we obtain the performance curves of the method in [15] and the proposed reversible scheme, which are shown in the figure. It can be seen that the proposed reversible scheme significantly outperforms the previous methods when the embedding rate is larger than 0.01 bpp.

Then, we embedded the first part of additional data into the ciphertext pixel values by the reversible embedding method, and embedded the second part of additional data into the *K* LSB-planes of the ciphertext pixel values by the lossless embedding method. When having the encrypted image containing the additional data, we firstly extracted the second part of additional data from the LSB-planes of ciphertext pixel values. After decryption, we further extracted the first part of additional data and recovered the original plaintext image in the plaintext domain. Here, the payloads of the two parts of additional data are same as the payloads of reversible and lossless schemes, respectively, and the quality of directly decrypted image is same as that of reversible scheme.

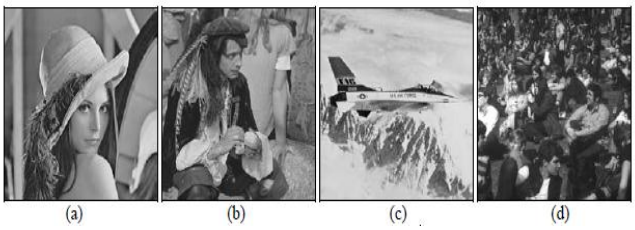

Figure 2: Cover images (a) Lena, (b) Man, (c) Plane and (d) Crowd

Table 1. Average payload of lossless scheme with respect to different *K*

K	1	2	3	4	5
Average embedding rate (bits per pixel) with Paillier cryptosystem	0.499	0.749	0.875	0.937	0.968

Figure 3: Directly decrypted Lena of reversible scheme (a) δ = 4, a total of 4.6×104 bits embedded and PSNR = 40.3 dB, (b) δ = 7, a total of 7.7×104 bits embedded and PSNR = 36.3 dB

IV. CONCLUSION

Here hiding in encrypted image is proposed, which consists of image encryption, data embedding and data extraction/image- recovery phases.In the first phase, the content owner encrypts the original uncompressed image using an encryption key then using a data hiding key to create a sparse space to accommodate the additional data. When the receiver has both of the keys, it can extract the data and recover the original content without any error. In Feature we implement data hiding and extraction algorithm and combine with our system. The new technique will solve a dilemma faced by digital image users, particularly in sensitive military, legal, and medical applications for secure message transmission.

REFERENCES

[I] X Zhang, "Separable Reversible Data Hiding in Encrypted Image", IEEE transactions on infonnation forensics and security, vol. 7, no. 2, pp. 826-832, Apr.2012.

[2] Z. Ni, Y-Q. Shi, N. Ansali, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol.' 16, no. 3 , pp. 354-362, Mar.2006.

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

[4] RiniJ ,4th Semester M.Tech ,Dept. of Computer Science and Information Systems FISAT Angamaly ,Kerala, India "Study on Separable Reversible Data Hiding in Encrypted Images" International Journal of Advancements in Research &Teclmology, Volume 2, Issue 12, December-2013 Copyright © 2013 SciResPub. IJOART

[5] VinitAghamDepaltment of Computer Engineeling R C Patel Institute of Technology, Shirpur.Dist. Dhule, Maharashtra, India.TareekPattewar Department oflnfonnation Technology R C

Patel Institute of Technology, Shirpur. Dist. Dhule, Maharashtra, India" A Novel Approach Towards Separable Reversible Data Hiding Technique" 2014 Intemational Conference on Issues and Challenges in Intelligent Computing Techniques (IClCT).

[6] Rengarajaswamy I Assistant Professor, Department of Electronics and Communication Engineeling, M.A.M School of Engineering, Trichy, Tamil Nadu "OFT Based Individual Extraction Of Steganographic Compression Oflmages", : IJRET Feb-14.

[7] VinitAghamDepaltment of Computer Engineering R C Patel Institute of Technology, Shirpur.Dist. Dhule, Maharashtra, India.TareekPattewar Department of Infonnation Technology R C Patel Institute of Technology, Shirpur. Dis!.Dhule, Maharashtra, India " A Novel Approach Towards Separable Reversible Data Hiding Technique" 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (lClCT).

[8] Ming Li, Di Xiao, ZhongxianPeng, and Hai Nan, "A modified reversible data hiding in encrypted images using random diffusion and accurate prediction," *ETRIJournal*, vol. 36, no. 2, pp. 325–328, 2014.

[9] J. Zhou, W. Sun, L. Dong, X. Liu, O. C. Au, and Y. Y. Tang, "Secure reversible image data hiding over encrypted domain via key modulation," *IEEE Transactionson Circuits and Systems for Video Technology*, vol. PP, no. 99, pp. 1–1, 2015.

[10] Xinpeng Zhang, "Separable reversible data hiding in encrypted image," *IEEE Transactions on InformationForensics and Security*, vol. 7, no. 2, pp. 826–832, 2012.

[11] Xinpeng Zhang, ZhenxingQian, GuoruiFeng, and YanliRen, "Efficient reversible data hiding in encrypted images," *Journal of Visual Communication and ImageRepresentation*, vol. 25, no. 2, pp. 322–328, 2014.

[12] ShuliZheng, Dandan Li, Donghui Hu, Dengpan Ye, Lina Wang, and Jinwei Wang, "Lossless data hiding algorithm for encrypted images with high capacity," *MultimediaTools and Applications*, pp. 1–14, 2015.

[13] Xinpeng Zhang, Chuan Qin, and Guangling Sun, "Reversible data hiding in encrypted images using pseudorandom
sequence modulation," *Digital Forensics and Watermaking*, vol. 7809, pp. 358–367, 2013.

[14] Zhaoxia Yin, Bin Luo, and Wien Hong, "Separable and error-free reversible data hiding in encrypted image with high payload," *The Scientific World Journal*, vol. 2014, pp. 8, 2014.

[15] Zhaoxia Yin, Huabin Wang, Haifeng Zhao, Bin Luo, and Xinpeng Zhang, "Complete separable reversible data hiding in encrypted image," *Cloud Computing andSecurity: First International Conference, ICCCS 2015*, pp. 101–110, 2015.

[16] Xiaotian Wu and Wei Sun, "High-capacity reversible data hiding in encrypted images by prediction error," *Signal Processing*, vol. 104, pp. 387–400, 2014.

[17] Xinpeng Zhang, Chuan Qin, and Guangling, "Reversible data hiding in encrypted images using pseudorandom
sequence modulation," *Digital Forensics and Watermaking*, vol. 7809, pp. 358–367, 2013.

[18] Chong Fu, Jun-jie Chen, HaoZou, Wei-hongMeng, Yong-feng Zhan, and Ya-wen Yu, "A chaos-based digital image encryption scheme with an improved diffusion strategy," *Optics Express*, vol. 20, no. 3, pp. 2363–2378, 2012.

[19] Zhicheng Ni, Yun-Qing Shi, N. Ansari, and Wei Su, "Reversible data hiding," *IEEE Transactions on Circuitsand Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, 2006.

[20] Y. Q. Shi, X. Li, X. Zhang, H. Wu, and Ma B., "Reversible data hiding: Advances in the past two decades," *IEEE Access*, vol. PP, no. 99, pp. 1–1, 2016, doi:10.1109/ACCESS.2016.2573308.

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

[22] K. Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE*.

[23] M. N. Islam,M. S. Alam, and M. A. Karim, _Optical security system employing quadrature multiplexing,_ Optical Engineering, vol. 47, 2008, Paper No. 048201.

[24] Z. Liu and S. Liu, _Double image encryption based on iterative fractional Fourier transform,_ Optics Communications, vol. 275, 2007, pp. 324-329.

[25] Z. H. Guan, F. Huang, and W. Guan, _Chaos-based image encryption algorithm,_ Physics Letters A, vol. 346, 2005, pp. 153-157.

[26] N. Y. Pareek, V. Patidar, and K. K. Sud, _Image encryption using chaotic logistic map,_ Image and Vision Computing, vol. 24, 2006, pp. 926-934.

