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

Konchada Nanda Kishore[1], S. Daya Sagar Chowdary[2]
[1]*Pursuing M.Tech in Digital Electronics and Communication Systems from Thandrapaparaya Institute of Science and Technology komatipalli, bobbili, vizianagaram (dist), a.p, india*
[2]*Assistance Professor from Thandrapaparaya Institute of Science and Technology komatipalli, bobbili, vizianagaram (dist), a.p, india*

***Abstract*- The Lossless data hiding provides the embedding of data in a host image without any loss of data. This research explain a lossless data hiding and image cryptography method based on Choas Block to image encryption the lossless means if the marked image is considered reliable, the embedding distortion can be totally removed from marked image afterward the embedded data has been extract. This procedure uses features of the pixel difference to embed more data than other randomly partition using Block based Sharpness Index Filtering and refine with single level wavelet decomposition shifting technique to prevent image distortion problems. In this work also manages reversible data hiding based on chaotic technique. In which initially image histogram processes to perceive the pixels which is chosen for hiding each bit of secret data, then by the logistic chaotic map compute an order of hiding each bit stream. Performances differentiate with other exist lossless data hiding plan providing show the superiority of the research. In this proposed research PSNR is found nearly 5.5*103 and existing 4.8*103 at 100 embedding rate which enhance for our existing technique that simulated in MATLAB 2017a.**

Index Terms- chaotic S-block, reversible data hiding, Lossless data hiding, encryption, cryptography, SSI, BSSI.

1. INTRODUCTION

There are various techniques available for data protection. Out of which encryption and data hiding are two effective means of data protection. The encryption techniques convert plaintext content into unreadable cipher text. The data hiding techniques embed additional data into cover media. The data can be embedded by introducing slight modifications. Data hiding may be performed with a lossless or reversible manner. In the proposed system the terms "lossless" and "reversible" will be distinguished. In the previous references these two terms have the same meaning.

If the display of cover signals containing embedded data is same as that of original cover even though the cover data have been modified for data embedding, in this case we can say that the data hiding method is lossless. 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, in this case we can say that the data hiding scheme is reversible.

2. LITERATURE REVIEW

Author Xinpeng Zhang, in his paper" Reversible Data Hiding with Optimal Value Transfer" has tried to improve the performance of reversible data hiding. In order to achieve a good payload-distortion performance of reversible data hiding, his work first finds the optimal value transfer matrix by maximizing a target function of pure payload with an iterative procedure, and then proposes a practical reversible data hiding scheme. The differences between the original pixel-values and the corresponding values estimated from the neighbors are used to carry the payload that is made up of the actual secret data to be embedded and the auxiliary information for original content recovery [5]. Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li have developed the system by reserving room before encryption. To make the data hiding process effortless, extra space is made empty in the previous stage. .The method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. Furthermore, this novel

method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images. Reversible data hiding (RDH) in images is a technique, by which the original cover can be losslessly recovered after the embedded message is extracted [3]. Jessica Fridrich, Miroslav Goljan, Petr Lisonek, and David Soukal have shown that by using the wet paper coding, one can represent on average Nd bits by only flipping a part of dry elements where Nd is the number of dry elements. In this scenario, the data-hider may flip the dry elements by replacing [6].

3. PROPOSED WORK

3.1 Lossless Data Hiding Scheme

This scheme involves three parties:

1. An image provider.
2. A data hider.
3. A receiver.

The role of image provider is to encrypt each pixel of the original plaintext image using the public key of the receiver. The data hider is unaware with the original image. Data hider can modify the cipher text pixel values to embed some additional data into the encrypted image by multi-layer wet paper coding .There lies one condition that the decrypted values of new and original cipher-text pixel values must be same. The receiver have the encrypted image containing the additional data, a receiver knowing the data hiding key may extract the embedded data, while a receiver with the private key of the cryptosystem may perform decryption to retrieve the original plaintext image. The embedded data can be extracted in the encrypted domain, and cannot be extracted after decryption. That means the data embedding does not affect the decryption of the plaintext image [1].

3.2 Reversible Data Hiding Scheme

To shrink the image histogram some preprocessing is employed in reversible scheme. Then each pixel is encrypted with additive homomorphic cryptosystem by the image provider. When data hider has the encrypted image, he modifies the cipher text pixel values to embed a bit-sequence generated from the additional data and error-correction codes. . Due to the homomorphism property, the modification in encrypted domain will result in slight increase/decrease on plaintext pixel values. The advantage of histogram shrink before encryption is that the data embedding operation does not cause any overflow/underflow in the directly decrypted image [1].

3.3 Combined Data Hiding Scheme

In the lossless scheme and the reversible scheme, the data embedding operation is performed in the encrypted domain. The data extraction for above two schemes is very different. With the lossless scheme, data embedding does not affect the plaintext content and data extraction is also performed in encrypted domain. With the reversible scheme, there is slight distortion in directly decrypted image canused by data embedding, and data extraction and image recovery must be performed in plaintext domain. In the combined scheme, the image provider performs histogram shrink and image encryption. When having the encrypted image, the data -hider may embed the first part of additional data. On receiver side, the receiver firstly extracts the second part of additional data from the LSB-planes of encrypted domain [1].

In both of the two schemes, the data embedding operations are performed in encrypted domain. On the other hand, the data extraction procedures of the two schemes are very different. With the lossless scheme, data embedding does not affect the plaintext content and data extraction is also performed in encrypted domain. With the reversible scheme, there is slight distortion in directly decrypted image caused by data embedding, and data extraction and image recovery must be performed in plaintext domain. That implies, on receiver side, the additional data embedded by the lossless scheme cannot be extracted after decryption, while the additional data embedded by the reversible scheme cannot extracted before decryption. In this section, we combine the lossless and reversible schemes to construct a new scheme, in which data extraction in either of the two domains is feasible. That means the additional data for various purposes may be embedded into an encrypted image, and a part of the additional data can be extracted before decryption and another part can be extracted after decryption.In the combined scheme, the image provider performs histogram shrink and image encryption. When having the encrypted image, the data-hider may embed the first part of additional data using the method. Denoting the ciphertext pixel

values containing the first part of additional data as c'(i, j), the data-hider calculates where r"(i, j) are randomly selected in Z* n or 1 * s+ Z n for Paillier and Damgard-Jurik cryptosystems, respectively. Then, he may employ wet paper coding in several LSB-planes of ciphertext pixel values to embed the second part of additional data by replacing a part of c'(i, j) with c"(i, j). In other words, the method is used to embed the second part of additional data. On receiver side, the receiver firstly extracts the second part of additional data from the LSB-planes of encrypted domain. Then, after decryption with his private key, he extracts the first part of additional data and recovers the original plaintext image from the directly decrypted image. The sketch of the combined scheme is shown in Figure 1. Note that, since the reversibly embedded data should be extracted in the plaintext domain and the lossless embedding does not affect the decrypted result, the lossless embedding should implemented after the reversible embedding in the combined scheme.

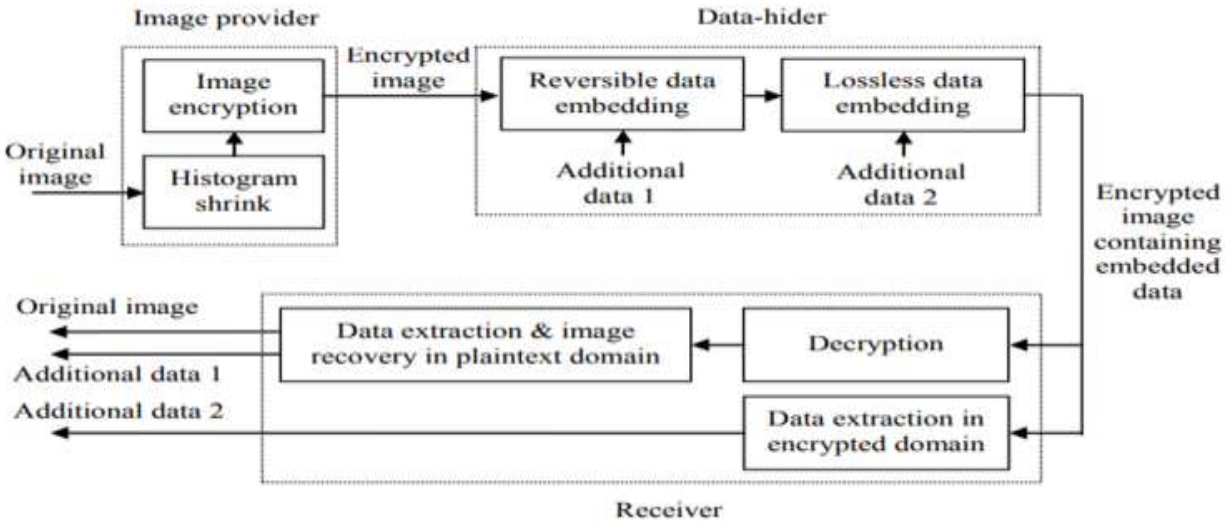

Figure 1 Sketch of combined scheme

4. SIMULATION RESULTS

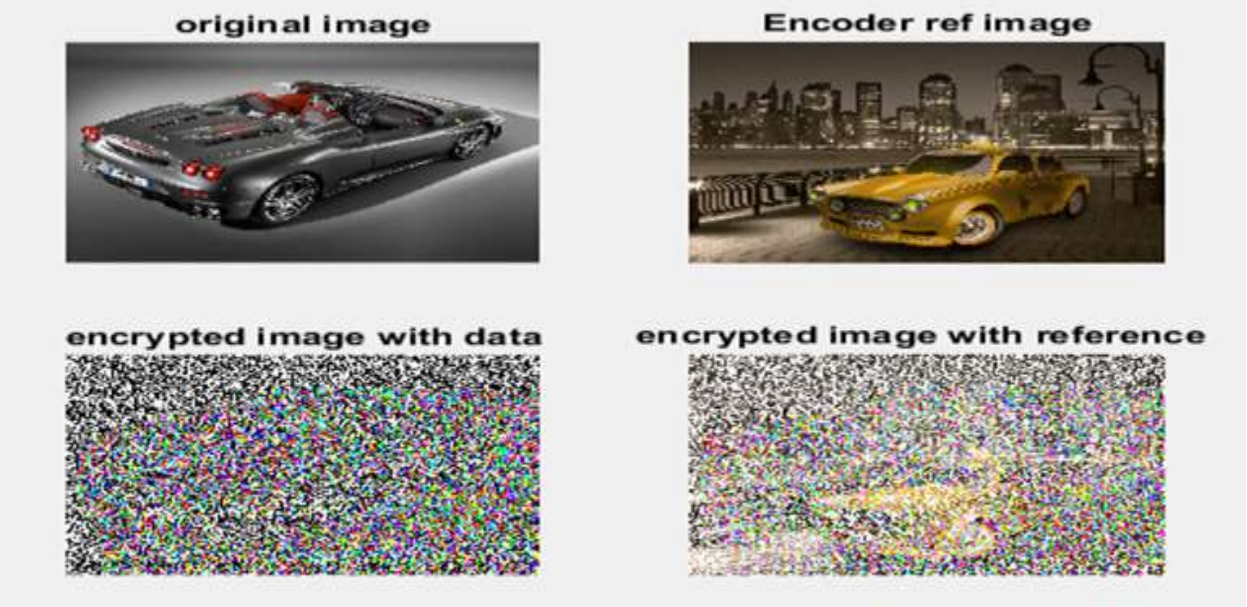

Fig 2 encryption process

Fig 3 decryption process

5. CONCLUSION

In the lossless scheme, 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, the additional data can be extracted from the plaintext domain, and, although a slight distortion is introduced in decrypted image, the original plaintext image can be recovered without any error. Due to the compatibility of the two schemes, the data embedding operations of the lossless and the reversible schemes can be simultaneously performed in an encrypted image. So, the receiver may extract a part of embedded data in the encrypted domain, and extract another part of embedded data and recover the original plaintext image in the plaintext domain.

REFERENCES

[1] Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng, " Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography" , IEEE Transactions on Circuits and Systems for Video Technology.

[2] N. A. Saleh, H. N. Boghdad, S. I. Shaheen, A. M. Darwish, " High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis," Digital Signal Processing, 20, pp. 1629−1636, 2010.

[3] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," IEEE Trans. Information Forensics & Security, 8(3), pp. 553-562, 2013.

[4] X. Zhang, "Commutative Reversible Data Hiding and Encryption," Security and Communication Networks, 6, pp. 1396−1403, 2013. Vol-2 Issue-1 2016 IJARIIE-ISSN(O)-2395-4396 1578 www.ijariie.com 351

[5] X. Zhang, "Reversible Data Hiding with Optimal Value Transfer, IEEE Trans. On Multimedia, 15(2), 316?325, 2013.

[6] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal," Writing on Wet Paper," IEEE Trans. Signal Processing, 53(10), pp. 3923-3935, 2005.

[7] W. Puech, M. Chaumont, and O. Strauss, " A Reversible Data Hiding Method for Encrypted Images," Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, Proc. SPIE, 6819, 2008.

[8] X. Zhang, " Separable Reversible Data Hiding in Encrypted Image," IEEE Trans. Information Forensics & Security, 7(2), pp. 526−532, 2012.

[9] X. Zhang, "Reversible Data Hiding with Optimal Value Transfer," IEEE Trans. on Multimedia, 15(2), 316−325, 2013

AUTHOR DETAILS

1. Konchada Nanda Kishore Pursuing M.Tech in Digital Electronics and Communication Systems Thandrapaparaya Institute of Science and Technology komatipalli, bobbili, vizianagaram (dist), a.p, india
2. s. Daya sagar chowdary Assistance Professor from Thandrapaparaya Institute of Science and Technology komatipalli, bobbili, vizianagaram (dist), a.p, india