IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

Encrypting Image by Lossless and Reversible Data Hiding using Cryptography

Bhavanjali Pathare[1], Vaishnavi Bidwe[2], Neeraj Yadav[3], Vishal Thorat[4], Ms. S. H. Lokhande[5], Dr. G. S. Navale[6]
Student, Department of Computer Engineering[1,2,3,4]
Head of Department, Department of Computer Engineering[5]
Sinhgad Institute of Technology and Science, Pune, Maharashtra, India
Savitribai Pune University of Pune, Pune, Maharashtra, India

Abstract: *This paper proposes a lossless and reversible data hiding scheme for images by using chaotic system with the help of public key cryptography. In this system original grey scale image will be encrypted using shuffling and scrambling using double encryption via chaotic system. And encryption will not affect original grayscale image. With the help of this 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: Encryption, Decryption, Chaotic System, Shuffling, Scrambling, etc.

I. INTRODUCTION

Now a days, in world doing communication with people is getting complicated using social media due to security threats. Due to this security threats some Government Institutes, Military Communication, Confidential Medical Information, etc. going through data breaches. It may leads security threats for that organizations.

The solution for this problems is to we can communicate through encrypted messages. So we are designed system which is capable of sending confidential messages in the form of Image and it will be retrieved at user end with original image using Chaotic System and Encryption.

In [1] proposed a system that perform the Reversible Data hiding by using ***the histogram shift*** operation for RDH. In this system used the spare space for embedding the data by shifting the bins of gray scale values. This paper proposes an analysis of the local standard deviation of the marked encrypted images in order to decryption step. Which is going to help for making things clear. Also, this paper has focuses on the time compression to increase the security. At the receiver end after the decryption of the image, the digital signature can be used to verify the authenticity of the image and therefore the key to encrypt and decrypt the data should be secret. It is simple and has constant PSNR ratio, capacity is high and distortion is very low. Main disadvantage is, more time consuming while searching the image number of times. in [2] In this paper they uses difference expansion method. They have proposed a Encryption and data hiding algorithm. The apparent disadvantage of those techniques is increasing the payload and the complexity is necessary. Advantages are It is possible to embed data in encrypted images and then decrypt the image and to rebuilt the original image by removing the hidden data. in [3] used Reversible data hiding (RDH) image technique. Some of the advantages are Able to protect the security of confidential data. And some of the disadvantages are It can be more accurate and can achieve real reversibility separate data encryption and greatly improvement on the quality of marked decrypted images.in [4] They uses prediction error expansion method which divides the pixels of image in 2 sets i.e. cross set & dot set. In this paper a novel optimized histograms modification scheme is presented to approximate the optimal embedding performance on the generated Prediction error sequence. In these method all probabilities are considered and adaptive prediction based on block classification. It causes error because it is based on prediction technique. in [5] HE used data expansion, location map, reversible data embedding, reversible integer transformation methods for design this method. He used difference expansion method for embedding data in reversible manner for digital images. In this method there is data loss for audio and video is minimized. It achieving error because of division by 2 and due to bit replacement visual quality degrade. in [6] He had used prediction based model for data embedding data images in this model using conditional entropy coding, context modelling, arithmetic coding, LSB

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

modification, watermark, data embedding and data hiding. The main disadvantages is that model uses prediction based conditional entropy which causes some error. in [7] Reversible image watermarking restores the original image without any distortion after performing the extraction of hidden data. In this model we can embed large amount of covert data for imperceptible modification. But, main disadvantage of this system is that it is time consuming.in [8] they used compression & decompression algorithm for embedding the data. This system checks the equivalency between data compression and RDH for binary bounds. It reduces the distortion, improve the RDH schemes for spatial. Main drawback is that it not consider grey scale for designing recursive codes. In [9] They have used a hybrid algorithm. It is basically uses three algorithms adaptive embedding, Predictive –Error Expansion (PEE) and Pixel selection. Predictive Error expansion is important for embedding the data and used for reversible watermarking. It provides authentication and integrity to the user. It also improves the payload with low distortion. Disadvantage of this model is, it is based on prediction technique which causes error. in [10] they proposed the methodology based on Partial encryption algorithm and Watermarking. Partial encryption is the encryption method that encrypts only parts of the original data while leaving the other parts unchanged. Watermarking is a technique with similarities to steganography. It has been around for centuries and is commonly used in money and stamps to assist in identifying counterfeiting. The idea behind watermarking is to create a translucent image on the paper to provide authenticity. Advantages of this paper are Media data are first watermarked, and then encrypted. However, in this case, the encrypted media data should be decrypted before the watermark can be extracted or another watermark can be embedded. Its Limitation is no practical solution but also time consuming. in [11] they paper proposed the methodology based on Image encryption, Data modification, Data integration, and Data extraction. The owner encrypts the cover image using an encryption key. The data owner uses the encrypted image to insert information in the form of text or image. Then the key is securely obtained by the recipient by the exchange protocol algorithm. Virtual embedding of information extracts pixel indices corresponding to the bits of data and is performed by the data manager and generates a data extraction key. This extraction key is encrypted using the public key generated, and sent to the recipient. If the recipient has data extraction key then original data can be retrieved. If the recipient has encryption key then original image can be retrieved. If he has both the keys then both, image and data can be retrieved. Advantages are Encrypted binary images can be compressed without loss by detecting the low density parity check code syndrome. And Limitation is Data loss. in [12] they proposed the methodology based on improved algorithm, Signal processing in Encrypted domain (SPED). Signal processing in Encrypted domain (SPED) can be applied in following, some important digital signals need to be sent by their owners to other parties for processing, but the other parties may be not trustworthy, so the signals should be encrypted before they are sent out. In this case, the signals to be processed by other parties are in cypher text format. Its Advantages are the improved algorithm was proposed mainly to reduce such mistakes in data extraction. The error rate is significantly decreased and the visual quality of the decrypted marked image is enhanced as well and Its Limitation is Error in data extraction. in [13] the methodology is based on JPEG encryption and decryption, Data hiding in JPEG Bit stream, Iterative recovery of original image. JPEG encryption algorithm, which enciphers an image to a smaller size and keeps the format compliant to JPEG decoder. After the sender uploads the encrypted JPEG bit stream to a remote server, a data hider embeds an additional message into the encrypted copy without changing the bit stream size. On the recipient side, the original bit stream can be reconstructed lossless using an iterative recovery algorithm based on the blocking artifact. Since message extraction and image recovery are separable, anyone who has the embedding key can extract the message from the marked encrypted copy. Advantages are High Security for encrypted data and good quality image will be obtained without decryption and Limitations are it is Time consuming.

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 Double encryption, 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

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

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.

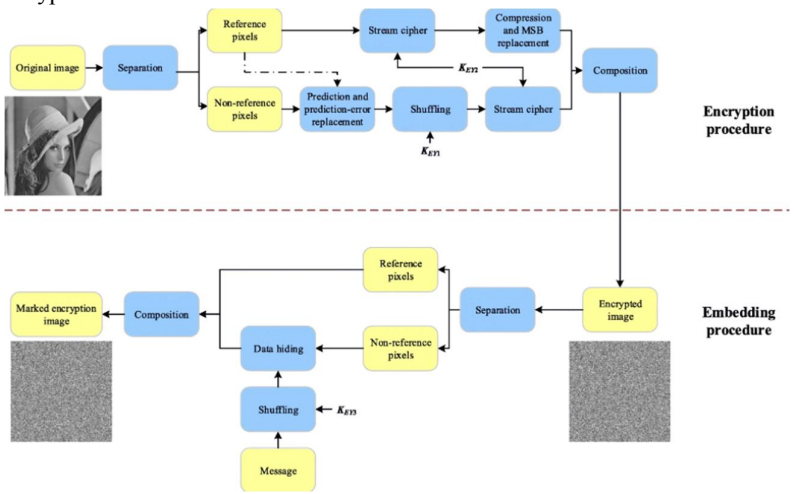


Figure 2: System Architecture

II. Proposed System

Proposed System of Encrypting Image by Lossless and Reversible Data Hiding using Cryptography Consist of following tasks:

1. Input
2. First Encryption
3. Second Encryption
4. First Decryption
5. Second Decryption
6. Output

III. Result and Discussion

Greyscale images sized 512×512, persons, animals, fruits, etc. shown in Figure, were used as the original plaintext covers in the experiment. With the lossless scheme, all pixels in the cover images were firstly encrypted using chaotic cryptosystem, and then the additional data were embedded into the LSB-planes of cipher text pixel-values using multi-layer wet paper coding. 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 greyscale images were obtained.

After decryption, we further extracted the first part of additional data and recovered the original plaintext image in the six plaintext domain filters. 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.

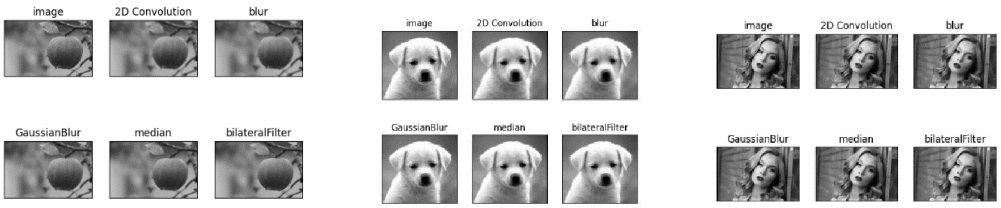
(a) (b) (c)

Figure 2: Cover images (a) Fruits, (b) Animal, (c) Person

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

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

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



Figures 3: Directly decrypted grayscale images of reversible scheme

IV. CONCLUSION

This work proposes a lossless, a reversible, and a combined data hiding schemes for cipher-text images encrypted by public key cryptography with double encryption and Decryption. In the lossless scheme, the ciphertext pixel values are replaced with new values for embedding the additional data into the LSB-planes of ciphertext pixels. This way, 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 of histogram shrink is made before encryption, and a half of ciphertext pixel values are modified for data embedding. On receiver side, 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

ACKNOWLEDGMENT

We would prefer to give thanks the researchers likewise publishers for creating their resources available. We are conjointly grateful to guide, reviewer for their valuable suggestions and also thank the college authorities for providing the required infrastructure and support.

REFERENCES

[1]. 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.

[2]. 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.

[3]. W. Zhang, K. Ma, and N. Yu, "Reversibility Improved Data Hiding in Encrypted Images," Signal Processing, 94, pp. 118-127, 2014.Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding," IEEE Trans. on Circuits and Systems for Video Technology, 16(3), pp. 354−362, 2006.

[4]. Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding," IEEE Trans. on Circuits and Systems for Video Technology, 16(3), pp. 354−362, 2006.

[5]. W. Hong, T.-S. Chen, and H.-Y. Wu, "An Improved Reversible Data Hiding in Encrypted Images Using Side Match," IEEE Signal Processing Letters, 19(4), pp. 199−202, 2012.

[6]. X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding," IEEE Trans. on Information Forensics and Security, 10(3), pp. 653-664, 2015.T. Bianchi, A. Piva, and M. Barni, "On the Implementation of the Discrete Fourier Transform in the Encrypted Domain," IEEE Trans. Information Forensics and Security, 4(1), pp. 86–97, 2009.

[7]. T. Bianchi, A. Piva, and M. Barni, "Composite Signal Representation for Fast and Storage-Efficient Processing of Encrypted Signals," IEEE Trans. Information Forensics and Security, 5(1), pp. 180–187, 2010.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

[8]. Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding," IEEE Trans. on Circuits and Systems for Video Technology, 16(3), pp. 354−362, 2006.

[9]. J. Tian, "Reversible Data Embedding Using a Difference Expansion," IEEE Trans. on Circuits and Systems for Video Technology, 13(8), pp. 890−896, 2003.

[10]. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless Generalized-LSB Data Embedding," IEEE Trans. on Image Processing, 14(2), pp. 253–266, 2005.

[11]. L Luo, Z Chen, M Chen, X Zeng, Z Xiong, "Reversible image watermarking using interpolation technique,", IEEE Transactions on information forensics and security 5 (1), 187-193

[12]. M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, "A Commutative Digital Image Watermarking and Encryption Method in the Tree Structured Haar Transform Domain," Signal Processing: Image Communication, 26(1), pp. 1−12, 2011.

[13]. S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative Encryption and Watermarking in Video Compression," IEEE Trans. on Circuits and Systems for Video Technology, 17(6), pp. 774−778, 2007.

[14]. X. Zhang, "Reversible Data Hiding in Encrypted Image," IEEE Signal Processing Letters, 18(4), pp. 255−258, 2011.

[15]. J. Yu, G. Zhu, X. Li, and J. Yang, "An Improved Algorithm for Reversible Data Hiding in Encrypted Image," Proceeding of the 11th International Workshop on Digital-Forensics Watermark (IWDW 2012), Shanghai, China, Oct. 31-Nov. 02, 2012, Lecture Notes in Computer Science, 7809, pp. 358-367, 2013.

[16]. Z. Qian, X. Zhang, and S. Wang, "Reversible Data Hiding in Encrypted JPEG Bitstream," IEEE Trans. on Multimedia, 16(5), pp. 1486−1491, 2014.