Reversible Data Hiding In Encrypted Images

Mruga G. Patel[1], Krunal J. Panchal[2]

[1]*Research Scholar, Information & Technology Department, L.J. Institute of Engineering & Technology, Gujarat, India*
[2] *Assistant Professor, Information & Technology Department, L.J. Institute of Engineering & Technology, Gujarat, India*

ABSTRACT

There is good potential for practical applications such as encrypted image authentication, content owner identification and privacy protection, reversible data hiding in encrypted image has attracted increasing attention in recent year. Data hiding is the technique by which some data is hidden into a cover media. Data hiding can be done in audio, video, image, text, and picture. we use image for data hiding especially digital images. The data may be any text related to the image such as authentication data or author information. At the receiver side it must be able to extract the hidden data and original image. A data hiding technique satisfying this requirement is known as reversible data hiding. Reversible data hiding is a type of data hiding techniques whereby the host image can be recovered exactly. Being lossless makes this technique suitable for medical, military applications and cloud storage. Reversible data hiding in encrypted image , which can recover the original image without any distortion from the marked image after the hidden data have been extracted. Now a days reversible data hiding in encrypted images is in used due to its excellent property which is original cover can be recovered with no loss after extraction of the embedded data. Also it protect the original data. Existing reversible data hiding methods in encrypted images (RDHEI) can be divided into two categories: without or with a preprocessing before image encryption. This paper focusing on original image can be recovered from the marked image without any distortion and improve the data hiding capacity. Using adaptive Thresolding purpose of the data hiding capacity.

Keywords :- *Reversible Data Hiding, Lossless Data Hiding, Image Encryption, PSNR , Data Hiding Capacity*

---

1. 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. There are a number of schemes which performs data hiding and encryption jointly. Different methods are used to data hide. But sometimes data hiding in images causes damages to the original image and also to the embedded data during extraction. It is feasible in the applications like cloud storage and medical systems.

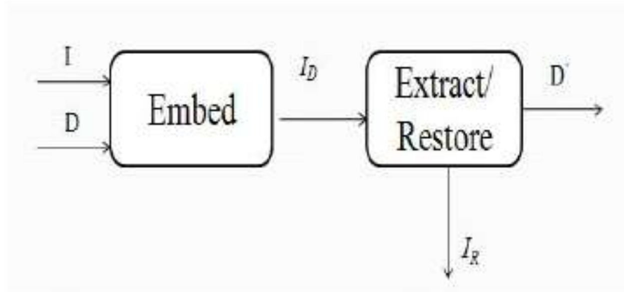


Fig-1: General Block Diagram of RDH[7]

In Fig 1, an overall view of the Reversible Data Hiding process. I represent the image and D, the data to be hidden. These two data are fed into the embed block which hides the message bits into the image. This image is represented by ID. When ID is fed into the extract/reverse block produces the original image after extracting the data. The restored image IR is same as the original image.[7]

2. LITERATURE REVIEW:

2.1 A Separable Reversible Data Hiding In Encrypted Image With Improved Performance

- In [1] Rintu Jose, Gincy Abraham paper, The owner of the image first encrypts the image by permutation, making use of an encryption key. Since permutation only shuffles the pixels, the histogram of the image remains the same. The data hider, without any knowledge about the original image content, hides data into the encrypted image by histogram modification method. Before hiding the data, the data hider permutes image using data hiding key and after data hiding he performs inverse permutation. At the receiver side, if the receiver has only data hiding key, he can extract the data, but cannot read the content of the image. If he has only encryption key, he can decrypt the image to get an image similar to the original one. If he has both keys, he may first extract the data using data hiding key and then decrypt the image using encryption key. This decrypted image is exactly same as the original image.

2.2 Reversible Data Hiding In Encrypted Images Based On Progressive Recovery

- In [2] Zhenxing Qian, Xinpeng Zhang, Guorui Feng Paper, Three parties: the content owner, the data-hider, and the recipient. The content owner encrypts the original image. The data-hider divides the encrypted image into three sets and embeds message into each set to generate a marked encrypted image. The recipient extracts message using an extraction key. Approximate image with good quality can be obtained by decryption if the receiver has decryption key. When both keys are available, the original image can be losslessly recovered by progressive recovery. this paper limits the distortion to three LSB-layers, and accordingly improves the embedding rate.

2.3 An Improved Reversible Data Hiding In Encrypted Images

- In [3] Shuang Yi, Yicong Zhou, The original work randomly selects pixels from an original image to obtain the estimation error for secret data embedding. In this work, we estimate half of the pixels in the original image to obtain the estimation error so that the maximum embedding rate can be significantly improved while keeping a high image quality of the marked decrypted image. This method is first to estimate a part of the pixels in an original image using the rest pixels and obtain the estimation errors.Then we encrypt the estimation errors and the rest pixels. The data hider then embeds the secret data into the encrypted estimation errors and scrambles the image using the sharing key. At the receiver side, the secret data and original image can be extracted and recovered separately by using different security keys.

2.4 Reversible Data Hiding In Encrypted Image Based On Block Histogram Shifting

- In [4] Zhaoxia Yin, Andrew Abel, Xinpeng Zhang, Bin Luo Proposed and evaluated a new separable RDHEI framework. Additional data can be embedded into cipher image previously encrypted using josephus traversal and a stream cipher. A Block histogram shifting (BHS) approach using self-hidden peak pixels is adopated to perform reversible data embedding. Depending on the keys held, legal receivers can extract only the embedded data with the data hiding key or they can decrypt an image very similar to the original image with the decryption key. They can extract both the embedded data and recover the original image error-free if both keys are available. The results demonstrate of that higher data embedding capacity, better decrypted-marked-image quality, error-free data extraction and accurate image reconstruction.

2.5 Lossless And Reversible Data Hiding In Encrypted Images With Public Key Cryptography

- In [5] Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng proposes a lossless, a reversible, and a combined data hiding schemes for ciphertext images encrypted. In the lossless scheme, the ciphertext pixels are replaced with new values to embed the additional data. In the reversible scheme, a preprocessing is employed to shrink the image histogram before image encryption. The data extraction procedures of the two schemes are very different. 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. So we combine 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.

2.6 Implementation of Reversible Data Hiding In Encrypted Image Using A-S Algorithm

- In [13] Aswin Achuthshankar, Aswathy Achuthshankar, Arjun K P, Sreenarayanan N M, presents a novel approach to data hiding using a symmetric stream cipher known as A-S Algorithm. In embedding data phase use histogram shift method. The A-S Algorithm is a modified version of OTP. A-S stands for “Achuth Shankar”. The algorithm produces an equally sized cipher text. OTP uses a fixed sized random key. User defined file as the KEY instead of generating the key. This user selected KEY file makes the key as a variable sized one. The user can use a text file, an image, an audio file or a video as the KEY file. The user can also use plain text as any type of file. A-S Algorithm produces a cipher text of the same size. A-S Algorithm can have a maximum possible substitution which is 256 power number of characters in the plain text.

2.7 Lossless Method For Data Hiding In Encrypted Image

- In [10] Patel Roshni, Aslam Durvesh and Patel Urvisha, This 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. When the receiver has both of the keys, it can extract the data and recover the original content without any error.

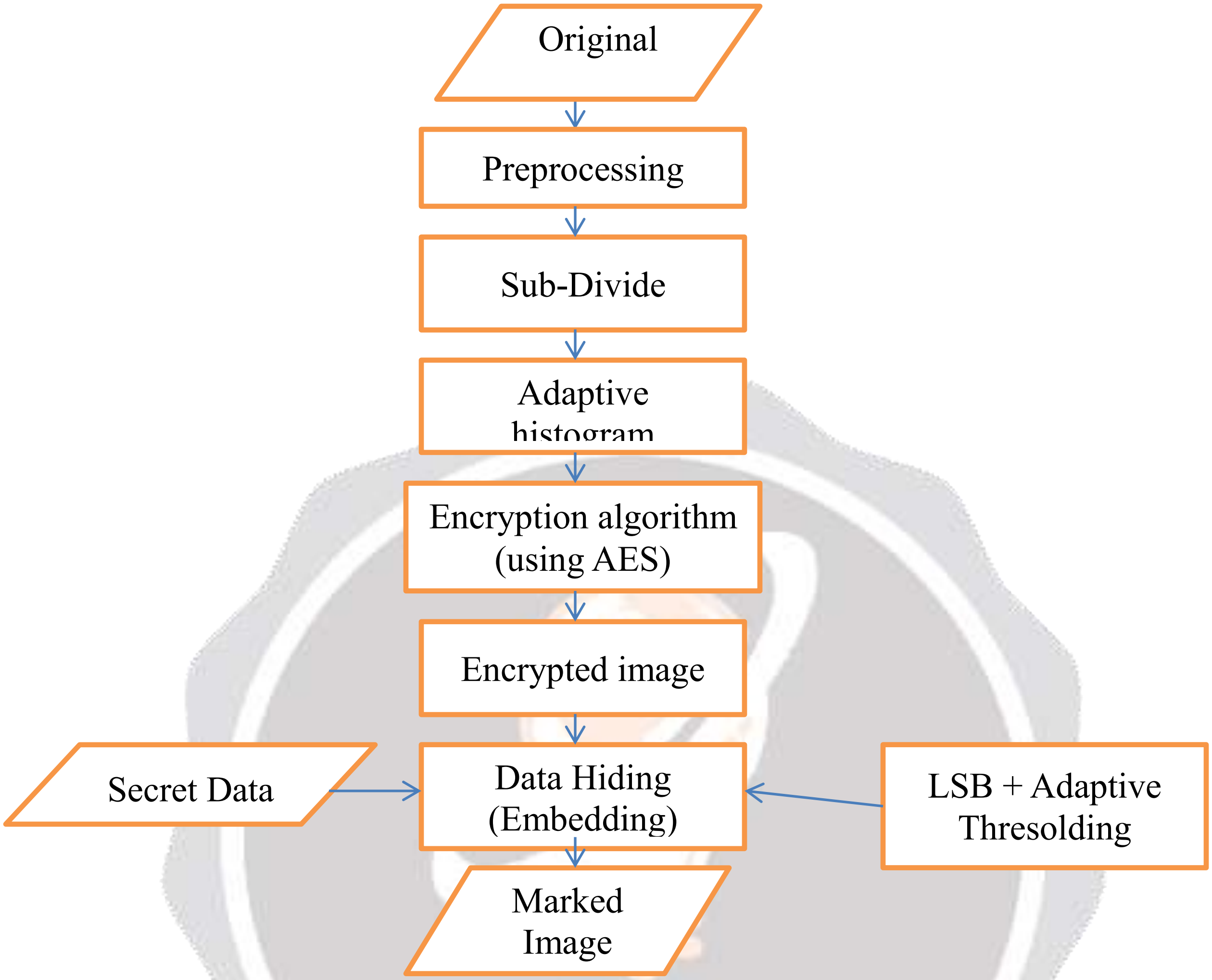
3. COMPARATIVE TABLE:

Table-1: Comparative Table

Paper Title	Methods/Techniques	Advantages	Disadvantages
A Separable Reversible Data Hiding In Encrypted Image With Improved Performance	Chaotic Based Permutation, Histogram Modification Based Method	Data Hiding Capacity Is High	PSNR Value Low
Reversible Data Hiding In Encrypted Images Based On Progressive Recovery	Stream Cipher Algorithm Used Such As Rc4, AES, LSB	Losslessly Recover Image, Good Quality	Less LSB-Layers, And Accordingly Improves The Embedding Rate
An Improved Reversible Data Hiding In Encrypted Images	Histogram Shifting Method	Embedding Rate Improved	Work On Grey Scale Images Only
Reversible Data Hiding In Encrypted Image Based On Block Histogram Shifting	Permutation Encryption Based On Josephus Traversing & Stream Cipher, Block Histogram Shifting Approach	Higher Data Embedding Capacity, Error-Free Data Extraction, Accurate Image Reconstruction	Less PSNR
Lossless And Reversible Data Hiding In Encrypted Images With Public Key Cryptography	Public Key Cryptosystems With Probabilistic And Homomophic Properties, LSB	Loss Less Encryption, High Embedded Rate, High Recovery Rate	Slight Distortion
Implementation Of Reversible Data Hiding In Encrypted Image Using A-S Algorithm	A-S Algorithm, Histogram Shift Method	Attack Free, Less Complexity, PSNR Good	Data Hiding Capacity Less
Lossless Method For Data Hiding In Encrypted Image	Bitxor Operation, LSB	Data Hiding Capacity Improve	PSNR Less

4. PROPOSED SYSTEM:

In Fig-2 and Fig-3 show the proposed work, hiding the data in encrypted image (Fig-2) and recovery process for extraction of data and recover the original image (Fig-3).


Original
Preprocessing
Sub-Divide
Adaptive histogram
Encryption algorithm (using AES)
Encrypted image
Secret Data
Data Hiding (Embedding)
LSB + Adaptive Thresolding
Marked Image

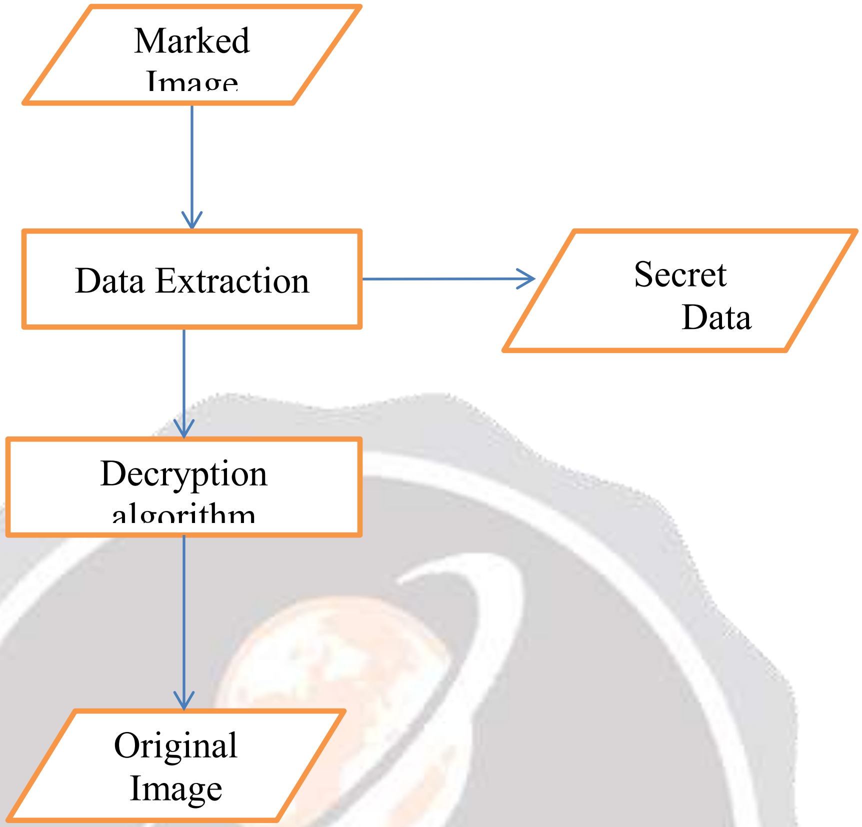


Fig-2: Proposed model for data hiding in encrypted image

Fig-3: Proposed model for reversible process for recovery

5. RESULT ANALYSIS:

We Tested the proposed method with 4 commonly used test images namely lena, Airplane, Sailboat, Baboon each of size 512x512. Table-2 show the PSNR of recovered images and embedding rate(bpp).

Table-2: Experimental results of four different images

Images	PSNR(dB)	Embedding rate(bpp)
Lena	77.7088	1.2385
Airplane	76.7575	1.7927
Sailboat	77.5228	1.2486
Baboon	77.6208	1.2923

6. CONCLUSION:

This paper mainly focuses on many related works of data hiding and comparison between them. In literature survey some methods hide large amount of data, some other embed low amount of data. In some techniques data hiding cause distortion to the original image also cause distortion to the embedded data also. The distortions in some work are relatively very low which are negligible but some distortions will very badly affect both the data and the image. Payload capacity is differ for different methods. The methods in each work have different level of applications. Each work has its own positives and negatives. Existing systems there is no provision for efficient security. Thus it is necessary to develop an efficient and effective system that provides data embedding and recovery without any distortion and provides better security. In proposed method, experimental results show four different images taken which is commonly used for the testing purpose and results show the PSNR value and embedding rate. In this method image reconstruction and embedding rate is high to compare the existing methods.

7. REFERENCES:

[1] Rintu Jose, Gincy Abraham “A Separable Reversible Data Hiding in Encrypted Image with Improved Performance” IEEE International Conference on Microelectronics, Communication and Renewable Energy (ICMiCR-2013), DOI:10.1109/AICERA-ICMiCR.2013.6576038, pp. 1-5

[2] Zhenxing Qian, Xinpeng Zhang, Guorui Feng “Reversible Data Hiding in Encrypted Images Based on Progressive Recovery” IEEE Signal Processing Letters, DOI:10.1109/LSP.2016.2585580, vol. 23, Issue: 11, Nov. 2016, pp. 1672-1676

[3] Shuang Yi, Yicong Zhou ”An Improved Reversible Data Hiding In Encrypted Images” Signal and Information Processing (ChinaSIP), 2015 IEEE China Summit and International Conference on, DOI:10.1109/ChinaSIP.2015.7230396, pp. 225-229

[4] Zhaoxia Yin, Andrew Abel, Xinpeng Zhan, Bin Luo “Reversible Data Hiding In Encrypted Image Based On Block Histogram Shifting“ Acoustics, Speech and Signal Processing (ICASSP), 2016 IEEE International Conference on, DOI: 10.1109/ICASSP.2016.7472053, pp. 2129-2133

[5] 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, DOI:10.1109/TCSVT.2015.2433194, vol. 26, Issue: 9, Sept. 2016, pp. 1622-1631

[6] Jitha Raj.T, E.T Sivadasan, “A survey paper on various reversible data hiding techniques in encrypted images” Advance Computing Conference (IACC), 2015 IEEE International, DOI:10.1109/IADCC.2015.7154881, pp. 1139-1143

[7] Rathika R, S. Kumaresan ”Survey on reversible data hiding techniques” Advanced Computing and Communication Systems (ICACCS), 2016 IEEE 3rd International Conference on, DOI:10.1109/ICACCS.2016.7586375, pp. 1-4

[8] Dr. J. Jagadeesan, Mr. Balika J. Chelliah, Nikhila Nyapathy, Neha Tiwari “Reversible Data Hiding In Encrypted Images Using AES Data Encryption Technique” International Journal of Emerging Research in Management &Technology, ISSN: 2278-9359 (vol-3, Issue-4), April 2014, pp. 28-35

[9] Parag Kadam, Mangesh Nawale, Akash Kandhare, Mukesh Patil “Separable Reversible Encrypted Data Hiding in Encrypted Image Using AES algorithm and Lossy Technique” IEEE2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME), DOI: 10.1109/ICPRIME.2013.6496492

[10]Patel Roshni, Aslam Durvesh and Patel Urvisha ”Lossless Method For Data Hiding In Encrypted Image” IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS'15, **DOI:**10.1109/ICIIECS.2015.7192907

[11]Mr. Falesh M. Shelke, Miss. Ashwini A. Dongre, Mr. Pravin D. Soni “Comparison of different techniques for Steganography in images” International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 3, Issue 2, February 2014, ISSN 2319 – 4847

[12]Priya Kumar Jambhulkar “Secure Reversible Data Hiding in Encrypted Images by Allocating Memory before Encryption via Security keys” International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 3, Issue 2, March 2014, pp. 491-497

[13]Aswin Achuthshankar, Aswathy Achuthshankar, Arjun K P, Sreenarayanan N M “Implementation of Reversible Data Hiding In Encrypted Image Using A-S Algorithm” 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), DOI: 10.1109/ICGCIoT.2015.7380662