بسمِ اللهِ الرَّحمٰنِ الرَّحِيمِ

وَلَسَوْفَ يُعْطِيكَ رَبُّكَ فَتَرْضَى۞

صَدَقَ اللَّهُ الْعَظِيْم

سورة الضحى ﴿5﴾

Survey and Comparative Analysis of RDH Methods In Encrypted Images

Supervisor: Dr. Bashar M. Nema

Submitted By

Hanan Abed Alwally & Taghreed Abdel Hameed

Outline

- Abstract
- Introduction
- Reversible Data Hiding
- RDH in EI
- Why RDH- EI used?
- Applications of RDH-EI
- Methods of RDH-EI Encoder and Decoder
- Survey of RDH Methods in EI
- Comparative analysis
- Conclusions

Abstract

In recent years, the world witnessed a revolution in the development and utilization of Information Technology (IT), and multimedia. This is due to the reason for increasing internet-based-communications include transferring digital information in text files, videos, audio, and/or images form. Thus, IT and multimedia have become a vital part of our daily life. However, there is a question that comes in our minds is this data of multimedia (especially images) secure? The answer according to the information security is no, because there are many threats targeting the confidentiality, integrity and authentication of images. To bypass this problem, Reversible Data Hiding(RDH) technique which is works via embedding extra data to an image has emerged. Recently, RDH with the encrypted images (RDH-EI) is utilized ,thus, attracting the attention of academics and employers. Therefore, the most important methods of (RDH-EI) over the last 5 years has been shown.

Introduction

The security of digital images acting a vital role in all fields, particularly, in **highly confidential areas** (i. e. the military, medical world, and law enforcement), Which are required safe transfer and retrieval processes. Therefore, data hiding techniques have been utilized to embed secret data (i.e. information of ownership, or authentication data) then extract it later from the **marked image**. However, these traditional methods of data hiding usually produce some distortions in the image, although these distortions may be invisible to human eyes, but, in some special requirements (confidential areas) it is desired to recover images without any errors. Thus, **Reversible Data Hiding** (RDH) method has been developed**.**

Fig. (1): Examples of Highly Confidential Areas.

Reversible Data Hiding

Reversible Data Hiding (RDH) is a method of embedding extra data to an image reversibly, which assurances lossless recovery for both the embedded data and the original image. Generally, there are three kinds of RDH methods:

1. **Compression based RDH:** In this approach, spatial domain compression techniques are applied on bit planes of the cover image to generate space for secret data embedding. A Generalized LSB (GLSB) embedding is one of the earliest works in compression based data hiding. According to this scheme, the cover image is quantized and then the difference between quantized pixel value and cover pixel value is calculated. Those differences are compressed using lossless compression techniques. The compression provides some empty space to store the secret data.

2. **Histogram Shifting (HS) based RDH:** The HS scheme utilizes the knowledge of cover image histogram for data embedding. A set of the Peak Points (PP) and Zero Points (ZP) are selected from the cover image histogram. Then the values between PP and ZP are shifted towards ZP by 1 position. Now, there will no longer be an empty or minimum bin in ZP position. The empty bin would appear near PP, then embeds the secret messages into the peak point.

3. **Difference Expansion (DE) based RDH:** extra space can be discovered by exploring the redundancy in the image content. Since, the secret data is embedded into LSBs of expanded differences between the adjacent pixels. A pixel pair with intensities x and y are selected from an 8 bit grayscale cover image. Then their integer average and difference are calculated. After that, the difference value is expanded via multiplying with a factor of 2 and then appended with the secret binary bit (d) into the expanded difference value. Finally, the result image is computed using the new difference value DiffE and the original integer average value.

RDH IN EI

Recently, RDH in Encrypted Images (RDH-EI) has been introduced. This combined can be utilized together in four diverse ways: **Insert-Then-Encrypt (ITE), Encrypt-Then-Insert (ETI), Insert-To-Encrypt (I2E), and Encrypt-To-Insert (E2I).** In the ITE and ETI, data hiding and encryption are executed sequentially. While, I2E objectives to severely distort the quality of the image, which is going completely against the principle of data hiding. Finally, E2I limits the tasks in the conventional perceptual encryption method, where the cipher text image is produced based on the data to be hidden. This lecture focuses on the ETI method, since, it is wide spread in combining data hiding and encryption .

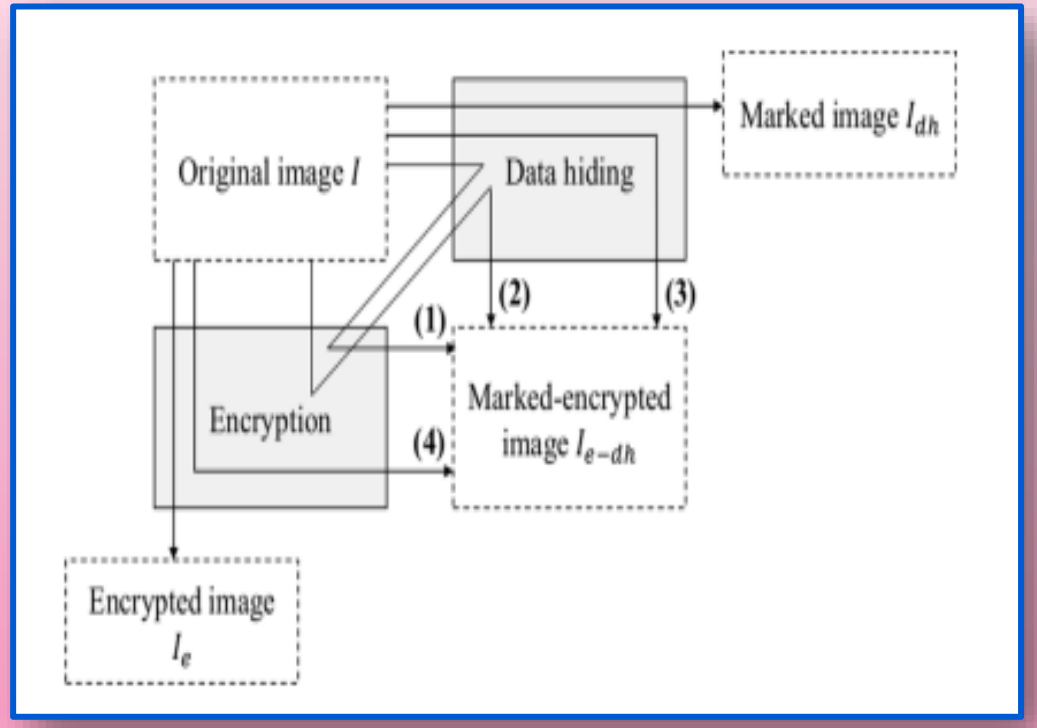


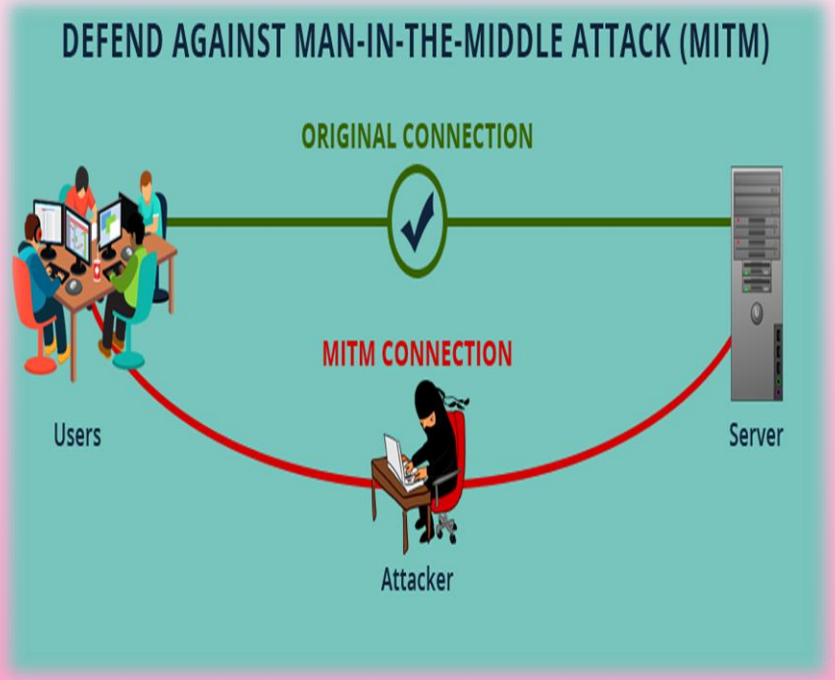
Fig. (2): Deploy RDH with Encryption Image by Four Ways: (1) ITE, (2) ETI, (3) I2E, and (4) E2I.

Why RDH with EI Used?

RDH and encryption are the two main techniques for secure communication. In process of encryption includes converts the original representation of the information, known as plain-text, into an alternative form known as cipher-text. These techniques are used together for two reasons

1- **Security:** It is the resistance of the technique to an attack even after realization of the existence of secret data.

2- **Quality:** Payload can be concealed in an image without affecting its visual quality.



Applications of RDH-EI

there are several applications for RDH-EI, some of them are:

1. **Cloud storage:** the user could encrypt the content of image for privacy purposes, before uploading it to cloud for storage. The administrator of Cloud embeds data for management purposes.

2. **Patient's privacy:** Patient images In hospitals can be encrypted for privacy insurance, and for identification purposes the information of patients is embedded in these contents. Then embedded information can be extracted via nurses or doctors by handling the contents.

3. **Reporter from the field:** Encryption of an image, audio or video by a reporter before transmitting it back to headquarters, so that, only the designated persons can have access to the content for presenting exclusive coverage of the event. Information such as the Global Positioning ,sender ID can be embedded for the field reporter to avoid content forgery for authentication purposes.

4. **Classified information:** In military situations, authorized persons can extract the embedded data from the encrypted files (i. e. image, video, audio), while other person with a higher clearance can access both embedded data and original file for management purpose.

Methods of RDH-EI Encoder

The methods of encoder can be divided into two classes: Reserving Room Before Encryption (RRBE), and Vacating Room After Encryption (VRAE)

1. In RRBE, image is pre-processed via its owner in order to release some space for the hiding purpose, then encrypted it. after that, parts of the secret message can be embedded at the specific positions as shown in the fig.(3).

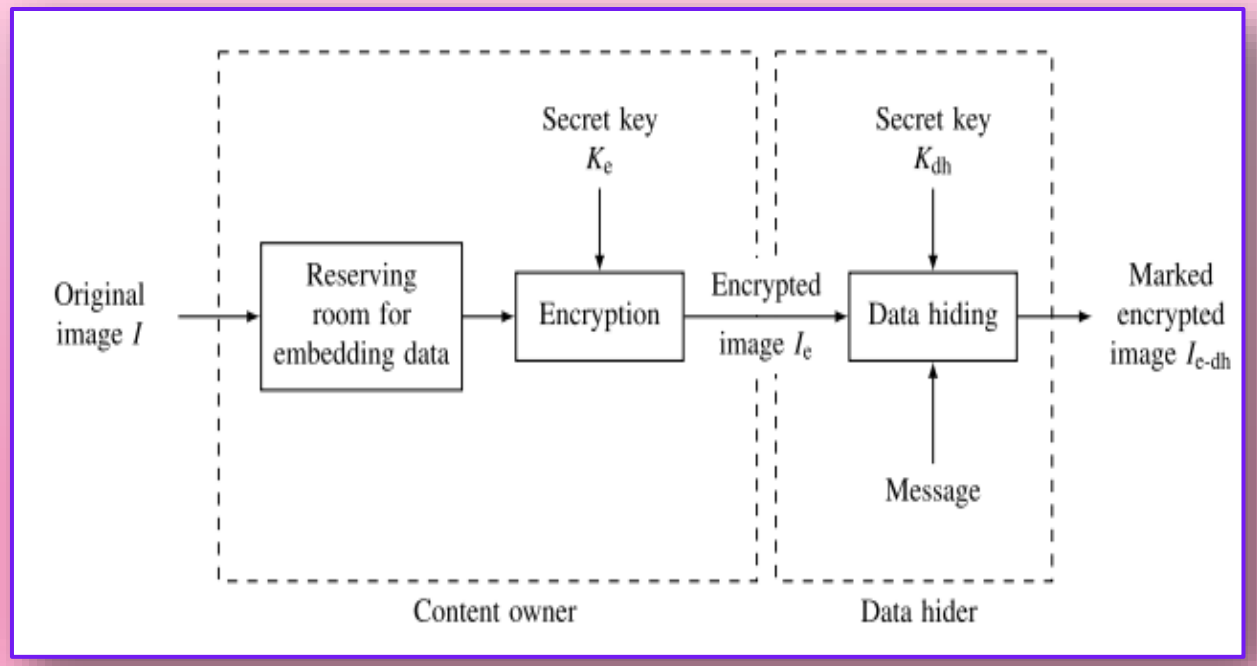


Fig. (3): RRBE Encoder Method.

Methods of RDH-EI Encoder

2 While in VRAE, encryption is done directly without any pre-processing in the content of image, then the encrypted data modifies by hide a secret messages.

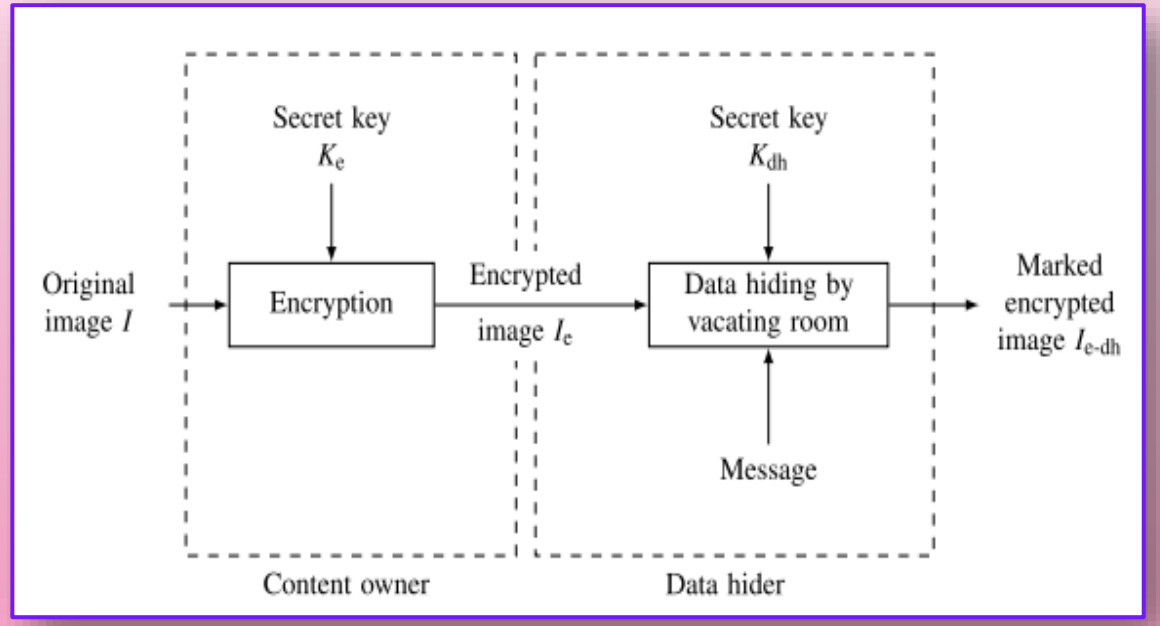


Fig. (4): VRAE Encoder Method.

Generally, in RRBE longer secret messages can embedded with pre-processing step. Instead in VRAE, the reconstructed image is usually an estimation of the original image and perfect reconstruction cannot be achieved. In addition, a large number of secret bits not be embedded in order to minimize the introduced distortion.

Methods of RDH-EI Decoder

In the decoding process, data extraction and reconstruction of an image can be executed in two ways:

1. **Jointly :**image cannot be obtained without knowing the key of data hiding. Also, using only encryption key leads to degrading the version of original image

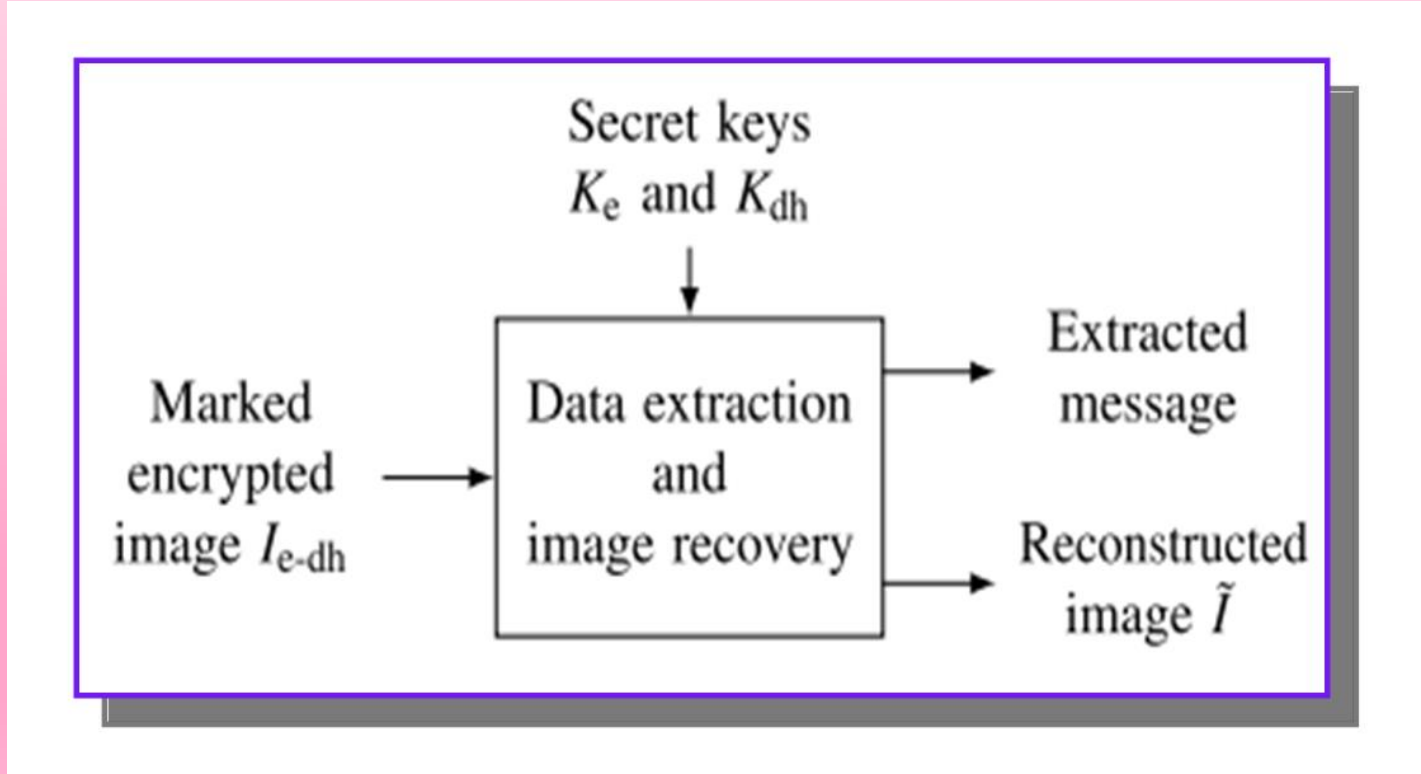


Fig. (5): joint decoder Method.

Methods of RDH-EI Decoder

2

Separable: extracting the message and reconstructing the image can be done independently. Thus, there are two scenarios **:**

1- A clear image with the embedded secret message is obtained. This image is very similar to the original image, but not identical**.**

2- The original image can be perfectly reconstructed, which does not contain the secret message

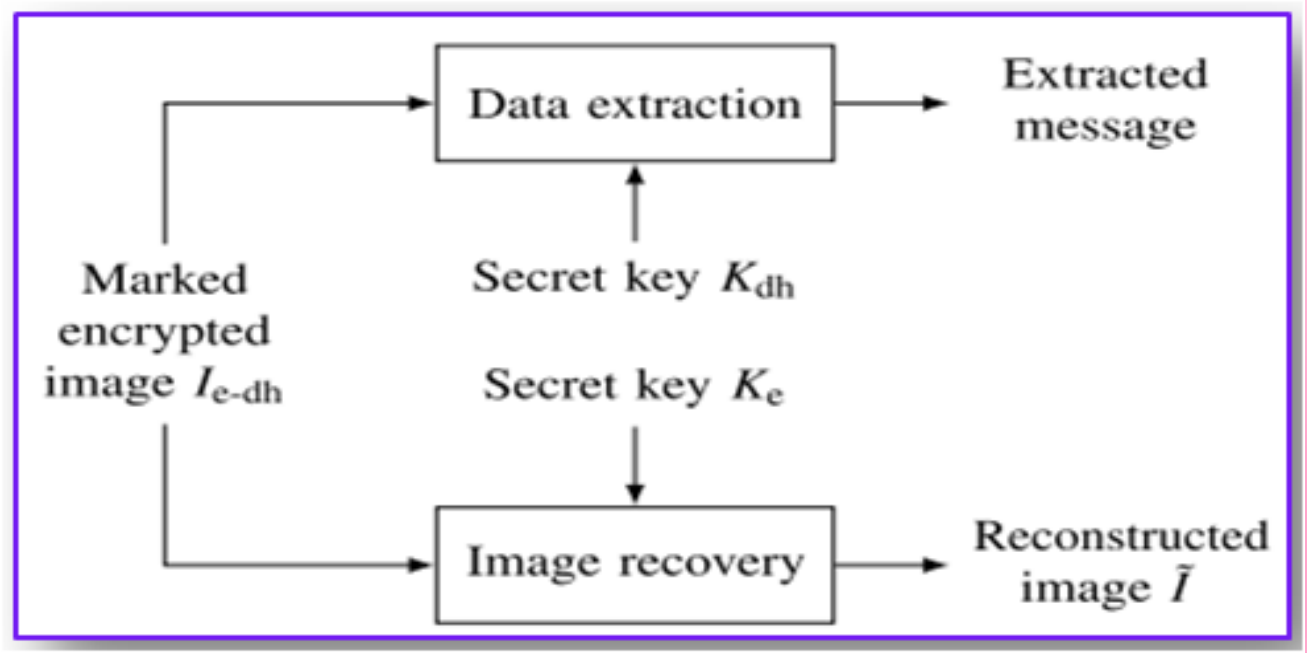


Fig. (6): separable decoder Method**.**

LITERATURE SURVEY

In the last years many contributions have been accomplished in the methods of RDH with Image encryption ; some of them are explained briefly:

Table (1): Summarize of RDH-EI Methods.

Author name and year	Methods of encoding	Methods of decoding	Proposed Methods with SDH-EI	Notes
Xiaochun Cao, Ling Du, Xingxing Wei, Dan Meng, and XiaojieGuo (2016)	RRBE	Separable	Patch-Level Sparse Representation & stream cipher	The results of tests illustration that our suggested technique reaches about 1.7 times as large payloads as the method in S-RDH.
Zhenxing Qian, and Xinpeng Zhang (2016)	VRAE	Separable	Distributed Source Encoding & stream cipher	Encrypted images enhance with embedding payload, Since Embedding Rate in Man, Lena, Baboon and Lake images was 0.2952 bpp.
Di Xiao , Yanping Xiang , Hongying Zheng , and Yong Wang (2017)	RRBE	Separable	pixel value ordering and additive homo morphism & homomorphic encryption	Lena, Airplane images achieves higher embedding rate reach to 0.1066 bpp with 0.2018bpp.
IoanCatalinDragoi, Henri-George Coanda and DinuColtuc (2017)	RRBE	Separable &Joint	Reserving Room After Encryption and Pixel Prediction & stream cipher	smaller than 1% error rate, and its offer a proposed method with capacity of payload < 0.1 bpp.

LITRUTURE SURVEY

Pauline Puteaux and and William Puech (2018)	RRBE	Separable	MSB Prediction & stream cipher	Using the images of Lena, Airplane, Man and Crowd, with MSB method lead to decrease the payload to 0.0359 bpp for Lena, 0.0111 bpp for Airplane, 0.0212 bpp for Man and 0.0145 bpp for Crowd.
Haoli Ge, Yan Chen, Zhenxing Qian, and Jianjun Wang (2018)	VRAE	Separable	Multi-Level method & stream cipher	When using multi-level method with images:(Airplane, Barbara, Baboon, Lena, Peppers and Boat, House , Sailboat , Splash , Stream , and Tank), it was found the perfect embedding rate reaches to 0.6714 bpp, while at single level it reaches to 0.1561 bpp , and finally on the double level it reaches to 0.2723. therefore Using multi-level improves the embedding capactiy significantly.
Chuan Qin, Xiaokang Qian, Wien Hong, and Xinpeng Zhang (2019)	VRAE	Separable	redundancy transfer and sparse block encoding	A number of tests were done with images (Airplane, Barbara, Baboon, Lena, Peppers and Boat) , but the best embedding rate was 1.5352 bpp.

LITRUTURE SURVEY

Guangyao Ma, and Jianjun Wang (2019)	VRAE	Joint	multi-stage integer wavelet transform & permutation cipher	Via using six images: Airplane, Barbara, Baboon, Lena, Peppers and Boat,gainbetter capacity of data embedding rate reach to 0.7643bpp, 0.7363bpp, 0.8285bpp, 0.8101bpp, 0.6811bpp and 0.7738bpp respectively.
Tiegang Gao ,Hang Gao, Renhong Cheng and Zhaoning You, (2020)	RRBE	Separable	image encoding with POB and bit planes	Obtains maximum capacity of embedding rate reach to 3.75 bpp, 1.93 bpp, 3.51 bpp for Lena, Peppers and Baboon images respectively.
Min Long , Yu Zhao , Xiang Zhang , and Fei Peng (2020)	RRBE	Separable	Tromino scrambling and adaptive pixel value ordering & stream encryption	Achieve better capacity of embedding rate reach to 0.1732 bpp, 0.0653 bpp, 0.1608 bpp, 0.1423bpp, 0.1687bpp, 0.1611bpp for Lena, Baboon, Peppers, Man, Barbara, Boat images.

COMPARATIVE ANALYSIS

In this section, a comparison will be made between previous studies from (2016) year to (2020) year depending on the methods of encoding , decoding and payload (embedding rate) as shown in Table (1). However, from the comparison has been noticed in all presented methods when utilizing for example, a VRAE through the encoding step with joint decoding, it is impossible to reconstruct the image without fault, with a very low payload (< 0.1 bpp) to reduce the introduced distortion. Thus, it is possible to obtain image that is very similar to the original image during the retrieval process ,but by utilizing VRAE with Separable and payload (>0.1 bpp). Therefore, the researchers continued to work until perfect image retrieval was achieved by using RRBE besides Separable with payload (> 0.1 bpp), and this leads to giving a robust to the application which is used RDHEI techniques, but the pre-processing step is still needed.

CONCLUSIONS

The methods of RDH with EI over five years (2016- 2020) has been presented for two purposes: to show how confidentiality, integrity and authentication of images is maintained against attacks, in addition to the ideal reconstruct of it from the receiver side. Several methods of RDH-EI encoding (RRBE, VRAE) and decoding (joint and separable) with different payload data have been utilized to achieve the two purposes above, and it is concluded the following:

First: when using VRAE and joint with a very low payload (< 0.1 bpp) in EI, the first purpose (security of I) is achieved but, in the receiver side it is impossible to reconstruct the image without fault.
Second: it is possible to obtain an image that is very similar to the original image by utilizing VRAE with Separable and payload (> 0.1 bpp).
Third: if it is utilized RRBE besides Separable with payload (> 0.1 bpp), the image is retrieved in a perfect manner but still needed to the pre-processing step.


THANKS FOR WATCHING