Journal of Engineering Sciences and Information Technology
Volume (6), Issue (6): 30 Sep 2022
P: 52 - 66

ISSN: 2522-3321

مجلة العلوم الهندسية وتكنولوجيا المعلومات
المجلد (6)، العدد (6): 30 سبتمبر 2022م
ص: 52 - 66

A Review of Reversible Data Hiding-Encrypted Image (RDH-EI) Methods

Dalal Naeem Hammod

College of Sciences || University of Al-Nahrain || Iraq

Abstract: In the past few years, the world had witnessed a revolution in multimedia and Information Technology (IT) development and utilization. This results from the increase of the internet-based-communications including the transfer of the digital data in text files, audio, video, and/or image formats. Which is why, multimedia and IT became one of the crucial parts of people's daily lives. There are numerous threats that target Image integrity, confidentiality, and authentication, therefore, the information security is a very important concept. The Reversible Data Hiding (RDH) is a data hiding method. RDH-Encrypted Image (RDH-EI) procedure which is working through embedding additional data to an image had emerged. Lately, the RDH-EI with the wide range is used, which is why, it has attracted the interest and focus of the employers as well as the academics. Thus, a survey that discusses previous researches will be carried out for the purpose of identifying the most significant (RDH-EI) approaches throughout the past five years. Several methods of RDH-EI with the different embedding rate, when its value is low (< 0.1 bpp), it is impossible to reconstruct the image without fault. Otherwise in the case where the embedding rate is high (>0.1 bpp), it is possible to obtain an image that is quite similar to the original image but it still needed for preprocessing step.

Keywords: Reversible Data Hiding, RDH-EI, Embedding Algorithm, Extraction Algorithm.

مراجعة طرق إخفاء البيانات العكسية في الصورة المشفرة

دلال نعيم حمود

كلية العلوم || جامعة النهرين || العراق

المستخلص: شهد العالم في السنوات الأخيرة ثورة في تطور واستخدام تكنولوجيا المعلومات والوسائط المتعددة. ويرجع ذلك إلى سبب زيادة الاتصالات المستندة إلى الإنترنت بما في ذلك نقل المعلومات الرقمية على شكل ملفات نصية، مقاطع الفيديو، التسجيلات الصوتية والصور. وهكذا، أصبحت تكنولوجيا المعلومات والوسائط المتعددة جزءًا حيويًا من حياتنا اليومية. هناك العديد من التهديدات التي تستهدف سرية، وسلامة المعلومات، ومصادقة الصور لذلك، أصبح أمن المعلومات من المواضيع المهمة جدا. وتقنية إخفاء البيانات العكسية (RDH)هي إحدى طرق إخفاء البيانات. تقنية إخفاء البيانات العكسية في صورة مشفرة (RDH-EI) والتي تعمل على إضافة بيانات إلى صورة ما. في الآونة الأخيرة، تم استخدام (RDH-EI) بشكل واسع، مما أدى إلى جذب انتباه الأكاديميين وأرباب العمل. لذلك سيتم إجراء مسح للدراسات السابقة من أجل التعرف على أهم طرق (RDH-EI) التي تم استخدامها على مدى السنوات الخمس الماضية. عدة طرق لـ RDH-EI ذات معدل التضمين مختلف، عندما يكون معدل التضمين منخفضًا (<0.1 bpp)، من المستحيل إعادة بناء الصورة بدون خطأ. بخلاف ذلك، عندما يكون معدل التضمين مرتفعًا (< 0.1 bpp)، فمن الممكن الحصول على صورة مشابهة جدًا للصورة الأصلية ولكنها لا تزال بحاجة إلى خطوة المعالجة المسبقة.

الكلمات المفتاحية: إخفاء البيانات العكسي، خوارزمية التضمين، خوارزمية الاستخراج.

1. Introduction.

Digital images security plays an important part in most the areas, in particular, in exceptionally secret regions, Here are examples of applications where the data-hiding concept has been utilized [1]:

- Image authentication
- Private communication
- Fraud detection
- Fingerprinting
- Copy control.

This Reversible Data Hiding (RDH) method has been utilized as part of several areas, for example, law, military, forensics, and medical applications [2, 3]. That requires safe transfer and retrieval processes [4-5]. Which is why, the approaches of data hiding were used for embedding the secret data (such as ownership information, serial number of the software, or authentication data) then extracts it from the marked image. However, these traditional techniques of data hiding Typically handle some distortions in the image, in spite of the fact that these distortions might a chance to be impalpable with human eyes, but, in exactly exceptional prerequisites (confidential areas) it may be wanted should recoup images without At whatever errors. Thus, RDH method has been developed **[6-7].**

RDH can be defined as a technique of embedding additional data into an image in a reversible way, assuring lossless recovery for embedded data as well as the original image. In general, 3 types of RDH technique are known: expansion-based, compression-based, and histogram modification-based **[8].**

The remainder of the present paper is organized as follows: Section (2) explains RDH structure. While, the survey of RDH has been illustrated in Section (3). Then, Section (4) includes comparative analysis and discussion. Finally, Section (5) contains the conclusion of this survey.

2. Reversible Data Hiding (RDH) Structure:

RDH can be defined as a technique of embedding additional data into an image in a reversible way, assuring lossless recovery for embedded data as well as original image. Fig 1 [9] shows basic RDH structure. The embedding represents an initial stage where a private message has been provided to the cover images in order to hide personal information. The message could act like input to embedding method. Following the recovery of image, the output will be in the covered image form [10-11]. After that, this result will be provided as input to extraction process that separates the cover from the private message. Private data and cover image have to be in the original form and thus they are referred to as the RDH. There are two phases, which are: **embedding algorithm and extracting algorithm [12-13].**

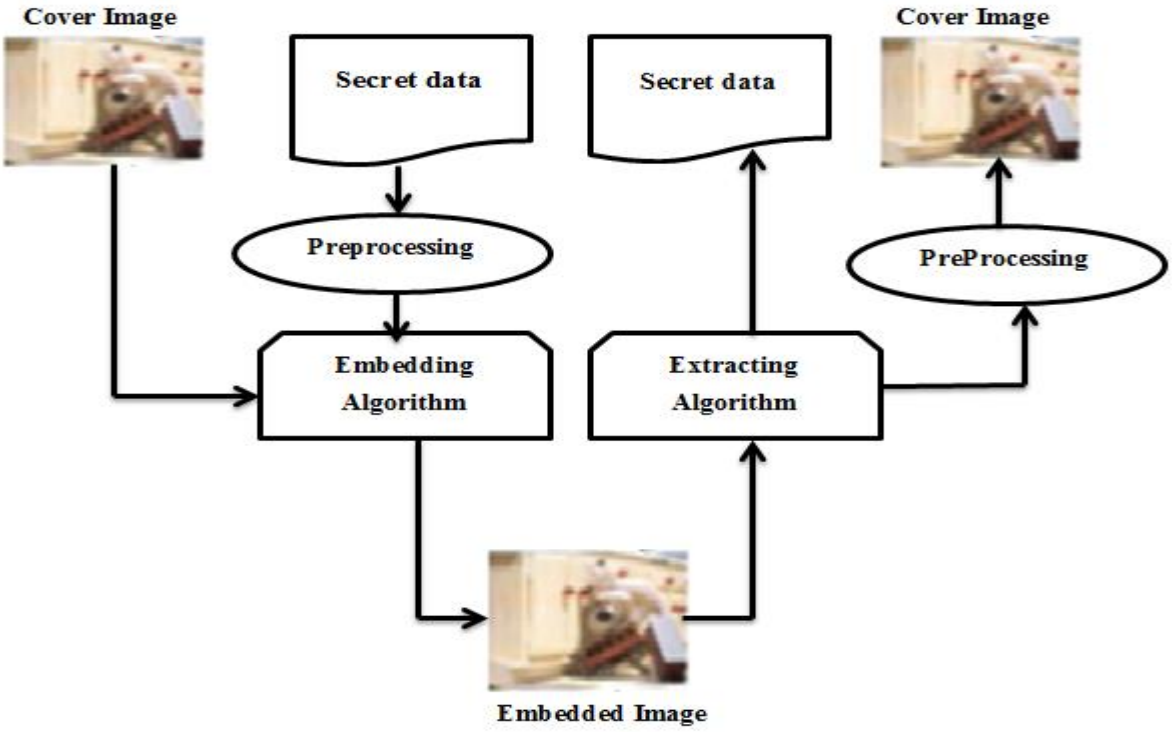

Figure (1) Basic Structure of RDH

2.1 Embedding algorithm steps [14]

Input: Secret Bits (Sb1), Bitmap Image (Bm1).

Output: Steog-image

Processes:

Step 1: compute the length of the Sb1 (secret bits) and Bm1 (bitmap Image).

Step 2: Check the hidden pixels in a Bm1. If the number of different hidden pixels is less than Sb1 (secret bits), the current bitmap is un-Embeddable Otherwise, it is Embeddable and we go to Step 3.

Step 3: If VAR of the hidden pixels is greater than or equal to the length of the Sb1 (secret bits), we go to step 4. Otherwise, no Sb1 (secret bits) will be embedded.

Step 4: The Sb1 (secret bits) is embedded into Bm1 (bitmap) then go to Step 5.

Step 5: Proceed to the next block until all blocks have been completed.

Step 6: Finally, output the steog-image

Step 7: End.

2.2 Extracting Algorithm Steps [15]

Input: steog-image, Total Length of Sb1 (TL).

Output: Secret bits (Sb1).

Processes:

Step 1: extract the bits from steg-image.

Step 2: calculated the length of the Sb1.

Step 3: If the length Sb1 < TL (Total length of Sb1) then goto step 1.

Step 4: If the length Sb1 >= TL (Total length of Sb1) then goto step 5.

Step5: show the Sb1.

Step6: End.

3. Reversible Data Hiding-Encrypted Image (RDH-EI):

RDH for the encrypted images are typically designed for applications where image owner and data-hider aren't the same person. A data-hider can't have the access to the image contents, and private message is held by the data-hider, the process of the encryption is done by sender, hiding through data-hider, and image reconstruction and/or data extractions by receiver. The available approaches of the RDH have been categorized to 2 classes, which are:

- Vacating Room After Encryption (VRAE)
- Vacating Room Before Encryption (VRBE) [16]

In VRAE method, a sender encrypts original image where a data should be embedded, whereas data is embedded by data-hider through the modification of some encrypted image bits. None-the-less, due to the fact that the original image encryption is carried out by affine transformation and pixel permutation, image histogram leakage is unavoidable under the exhaustive attacks [17]. In VRBE, original images, prior to being encrypted, are processed by owner for the creation of the vacant area for the embedding of the data, and private data are embedded by data-hider to specified positions. Separable RDH approaches have sufficient reconstruction capability and embedding rates, however, they require additional RDH process by sender prior to the encryption of the image [18]. Which means that RDH issue in the encrypted images is in fact transformed to conventional RDH in the plain-text images. Even though higher payloads could be accomplished by VRBE, it necessitates that the sender has to carry out an additional RDH before encrypting the image. If the sender does not have any idea about forthcoming data that is to be embedded by data-hider, or they do not have computational capability of conventional RDH, it appears impractical [19]. However, if a sender can reserve space to embed through the reversible hiding of the redundant bits within original plain image, all of the tasks of embedding might as well be performed on the side of the sender and after that, data-hider will become redundant [20].

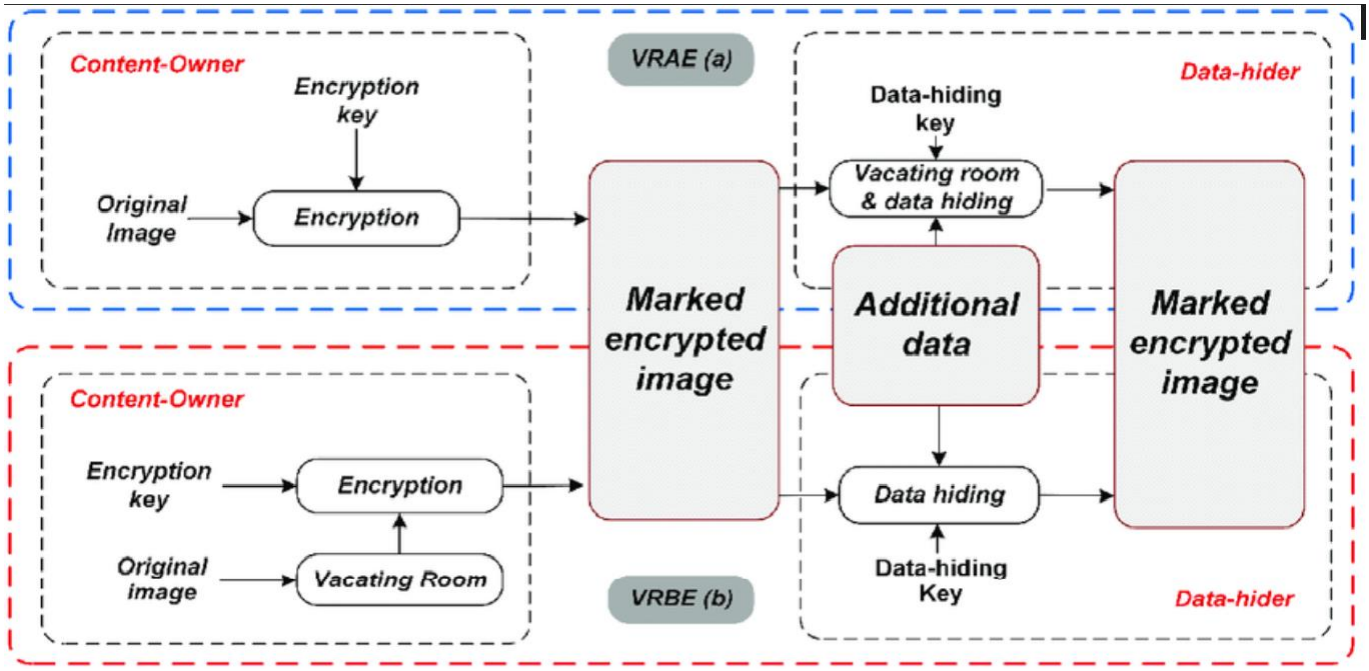

Figure (2) Two Categories of the RDH-EI

4. litruture survey.

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

Yi S., Zhou Y. (2017), have introduced binary-block embedding (BBE) approach for embedding the secret data within binary images. This approach uses an algorithm for the reversible hiding of the data within the encrypted images (BBE-RDHEI). It utilizes the BBE for embedding binary bits into the lower bit-planes of an original image within its higher bit-planes in a way that lower bit-planes may be kept so as to hide secret message within following processes. The BBE-RDHEI utilizes bit-level scrambling operation after embedding secret data for spreading the embedded secret data to the whole marked encrypted image so that it could be capable of preventing the secret data from being lost. A mechanism of security key design has been suggested for the purpose of enhancing the BBE-RDHEI security level. BBE-RDHEI processes are entirely reversible. Secret data and original image may be separately and independently reconstructed. The experimentations and comparisons have shown that the BBE-RDHEI has embedding rate which is almost twice larger compared to conventional methods, produces high quality marked decrypted images, and is capable of withstanding differential, brute-force, data loss and noise attacks [1].

Xiao, D., et al. (2017), this work suggested a method of Separable-RDH (S-RDH) in encrypted image relying on Pixel Value Ordering (PVO). In this approach, the homomorphism encryption was utilized for the purpose of encrypting image via the owner. After that, the owner sends the encrypted image to data hider that divides encrypted image to non-overlapping blocks with volume 2 (2, then

lossless compressed (arithmetic coding) was used for reduce the length if an overflow occurs. Additionally, more data has been added in each block using PVO. Finally, if both those embedded and encrypted key that the receiver has, then can restore the original image perfectly after extract the additional data [21].

Dragoi, I. et al. (2017), developed a method of RDH encrypted image which works with two diverse ways, termed: joint and reparative approach. In two ways, encrypted firstly the Image via utilizing the algorithm of stream encryption. Then, a subgroup of pixels was chosen to implement data hiding based upon data hiding key. Utilizing neighboring pixels for particular pixels to predicate through decode steps. (Joint) first approach, if one bit (i.e.'1') of secret message is added, the least significant bits (LSBs) are flipped for chosen pixel, else, they are retained unaffected if the bit of the message is '0'. Thru the decode step, the neighbouring pixels that unmarked have been utilized to predict the number for every pixel marked, also, the number of the embedded bit. In other words, in the second approach (separative) the LSBs of chosen pixels are replaced by a single bit of the secret message. Through the step of decoding, to return an approximation of the image a median filter has been used [22].

Puteaux, P., &Puech, W. (2018), presented a method based on the Most Significant Bit (MSB) Prediction for high capacity Reversible Data Hiding (HCRDH) in Encrypted Images. The reason behind using the values of MSB rather than the values of Least Significant Bit (LSB) to insert a secret message. MSB substitution does not produce artefacts in the domain of encrypted also, the prediction of the (LSB) is difficult than the prediction of MSB. Depending on these assumptions, presented two dissimilar HCRDH approaches: corrected prediction errors (CPE) with embedded prediction errors (EPE). For two cases, all image pixels does not be properly predicted via utilizing their neighbors at first specified. In case of using CPE approach, to bypass all prediction error (PE), the image is preprocessed then encrypt, hider of data easily can substitute for every value of the MSB for image encrypted secret message. Therefore, the payload is one (bpp) and the recombined image corresponding to image that pre-processed, is quite similar to original one (PSNR > 50dB). While, in case of using EPE method, the image is encrypted with no alteration, then information of location about all pixels that can't be properly predicted is added using MSB substitution. After that, all bits could notice that can be marked in data hider and change to bits of the secret data. As a result, the payload is a little lower than one (bpp) however perfect reversibility was accomplished [23].

Ge, H., et al. (2018), in this research High-Capacity-Multi-Level (HCML) method for RDH in encryption images (EI) has been introduced. The method includes: treat the image as Level-0 (L0) and adding more bits in the first level-0 (L0). However, in all levels the same algorithm of embedding. Also, Marked Encrypted Image (MEI) has been used to insert further bits into an image and produce other MEI. When adding more bits in every level, the correlations have been decreased and the fit is minimized too much with level-i (Li), the bit number that could be hidden in Li may become lesser from location map length high-i, therefore, cannot be added more bits. In any level, it is significant to replace the order, then

encrypt the image (Excluding L0) to choose new two high peaks likelihood, while, the is roughly the same at all levels. Thus, several peaks are utilized through many levels of adding which leads to high embedding capacity. Finally, In reception side, more bits have been extracted from the marked image (MI) and reprocess result image until (L0) with hidden data can be extracted [24].

Su W., *etal.* (2019), have proposed a reversible watermarking approach that has been based upon Pixel Value Ordering (PVO) embeds the secret data through the modification of maximal and minimal values in the block of pixels. This algorithm's performance is highly dependent upon inherent correlation amongst the neighbouring pixels within a block of images. For the purpose of improving intrinsic association amongst the neighbouring pixels in a block of images, a new approach for incorporating dynamic block-partition strategy into PVO approach has been suggested in the present study. This new approach includes: initially, host image division to non-overlapping areas, based on the values of the image pixels; after that, every one of the regions is divided into various blocks, classified subsequently based on local complexity and pre-defined threshold values for the embedding; and finally, the embedding of the watermark is carried out with the use of PVO-based algorithm. In this approach, every embedded block's pixel values are located in a rather small area for the purpose of improving intrinsic correlation and thus enhancing PVO's embedding performance. Experimental results have shown that the suggested approach has a better embedding efficiency in comparison to that of conventional PVO based algorithms [25].

Qin, C., et al. (2019), suggested an approach of RDH in EIutilized redundancy transfer (RT) and Sparse Block Encoding (SBE). The method works as: the input image is split to a series of the blocks, and by using encryption key, every block bit plane is disordered and pseudo-random, to generate the encrypted image, all the blocks with pixels are scrambled. Besides, an enhanced technique for compressing the LSB planes of encrypted image by the sparse matrix encoding, and reach high data hiding has been introduced. Lastly, the Receiver can accomplish image decryption, data extraction, and image recovery in a separate manner through the secret key availability [26].

Ma, G., & Wang, J. (2019), presented a framework for RDH-EI using multi-stage Integer Wavelet Transform (IWT). The framework includes: first (encryption step), the image is encrypted via permutation cipher. Second (data hiding step), the encrypted image has been decomposed with IWTto gain coefficients of high frequency subbands then preprocessed in order to add private data. Also, a ratio correction technique has been presented in order to guarantee the validity of a framework. For achieving higher-capacity, multi-level embedding and multi-stage IWT have been implemented. Furthermore, an adaptive correction (AC) technique was utilized to improve the capacity of embedding process. Third (recover step), a receiver could properly extract embedded secret data with the use of the key of hiding. Moreover, image can be perfectly recovered using key of encryption[27].

Xiao et al. (2019), have suggested a sufficient approach for the high-dimensional RDH, pair-wise prediction-error expansion (pairwise PEE) could achieve a higher level of the efficiency in comparison to traditional PEEs. With the pairwise PEE, the relations amongst prediction-errors have been well used through the modification of generated 2-D prediction-error histogram (2D-PEH). On the other hand, its efficiency may be enhanced additionally, due to the fact that histogram modification manner (in other words, utilized modification mapping) of the pair-wise PEE is fixed and independent of the content of the image. For the purpose of better utilizing the redundancy of the image, rather than embedding the data based upon empirically designed mapping of modification, a content dependent pair-wise embedding model has been suggested in this study. According to a particular 2D-PEH division, expansion bins selection has been formulated as a problem of the determination of the optimum path, and histogram modification mapping has been determined adaptively through taking optimum expansion bins. For the purpose of reducing computational costs, a dynamic programming algorithm has been suggested for the purpose of solving the problem of optimization with low computation complexity. In addition to that, through the combination of the suggested optimum expansion path with existing 1-D adaptive embedding mechanism, the performance of the embedding may be additionally improved. The suggested approach performed well and its superiority has been verified experimentally in comparison to the pairwise PEE as well as some other state-of-art approaches. [28]

Wu et al. (2019), in the past few years, the RDH in the encrypted images was developed for the purpose of transmitting useful information, whereas original images may be recovered ideally whenever required. In this study, a new approach has been suggested for the homomorphic encrypted images so that part of hidden data may be obtained in the encrypted domain and the remaining are obtainable after the decryption of the image. In particular, a plaintext image undergoes pre-processing through the by reversible embedding of bit values of some of the pixels within the image. This pre-processed image is encrypted with the use of the Paillier crypto-system and two embedding algorithms have been carried out to encrypted image after that. In comparison to state-of-art approaches, higher capacity of embedding may be accomplished through applying the suggested approach, respectively, for the data extraction prior to and post the decryption of the image. In comparison to schemes that have similar characteristics, best performances have been accomplished with the suggested approach, concerning the quality of directly decrypted image based on rate of data hiding. [29]

Gao, H., et al. (2020), have suggested a technique of high capacity- Reversible Data Hiding (HC-RDH) in the encrypted image (EI) depending upon image encoding with permutation ordered binary (POB) (which is the system of permutation ordered binary number). In this technique, the owner of image encodes the image via JPEG-LS (lossless compression), after that encrypts via bit planes. Then, the process of data hiding is being, encrypted image is shuffled, and all of the non-encoded-encrypted pixels are switched via secret data. Finally, the result image is separated into non-overlapping (2x2) blocks. The

block's feature of three-bits was computed from the pixels in the block. In case of five-bits, secret data has been added in all pixels of the block, while, the pixels often-bits lead to transfer the data to the value of POB. In the reception side, the owner was performing re-shuffled, image decryption with extracted hidden data then recovers the image [30].

Long, M., et al. (2020), in this work, the method of separable reversible data hiding (S-RDH) to encrypt the images depending on Tromino scrambling (TS) with the adaptive Pixel Value Ordering (PVO) is presented. An image in this method is passed into three steps: Data Hider (DH), Content Owner (CO), and Receiver (R). In CO, the image is divided into blocks with three pixels after that Tromino scrambling (TS) with stream encryption is executed then kept the result in the cloud. In the DH, the service provider of the cloud (DH) implements data hiding using PVO by adding more information to the image which is encrypted. Finally, in R step, there are two schemas can be executed after receipt keys of encryption and data hiding:

First: Data Extraction, Pixel Recovery, Stream decryption and Inverse TS are performed or,

Second: Stream decryption, Inverse TS, data extraction and pixel recovery are implemented[31].

Xu W., et al. (2021), have proposed a high-capacity RDHEI compressing the prediction errors in usable blocks of the block-based images that have been encrypted. On the side of the content owner, the original image has been segmented to size blocks, and every one of those blocks is encrypted through the use of the block-based modulations. On side of the data hider, a sufficient block-based predictor has been deployed for the generation of the prediction errors. Huffman coding method has been suggested for compressing the errors of prediction in usable blocks for the purpose of embedding abundant additional data. On the side of the receiver, additional data may be obtained entirely with data hiding key and original image could be recovered losslessly with the key of image encryption. The investigational results have demonstrated that the rate of the embedding of the suggested model is considerably enhanced in comparison with those of the state-of-the art models [32].

Ryota M., *etal* (2021), have proposed a new model for the RDH in the encrypted images, where hiding capacity as well as lossless compression quality are controlled flexibly. There are two fundamental aims; one is providing highly sufficient lossless compression under required hiding capacity, whereas the second one is enabling the extraction of embedded payload from the decrypted image. The suggested approach has the ability of decrypting the marked encrypted images without the extraction of data and deriving the marked images. The original image has been split arbitrarily to two areas, two different approaches for the RDH-EI have been utilized in this paper, and every one of them has been utilized for either one of the regions. After that, one of the regions may be decrypted without the extractions of data and lossless compressed as well with the use of the image coding standards even following the processing. The other area has a considerably higher hiding rate, about 1bpp. The experimental results have shown

the suggested method's effectiveness, according to lossless compression efficiency and hiding capacity. [33]

5. COMPARATIVE ANALYSIS:

In this section, a comparison will be made between previous studies from (2017) year to (2021) year, depending on the methods of encoding, with percentage decoding embedding rate as shown in Table1.

Table (1) Comparative Analysis of RDH-EI Methods.

No	Author name and year	Proposed Methods with RDH-EI	Embedding rate	Notes
1	Yi S., Zhou Y. (2017)	It utilizes the BBE-RDHEI for embedding the binary bits into the original image's lower bit-planes into higher bit-planes such that those lower bit-planes may be reserved so as to hide secret data in following processes.	embedding rate is almost twice as that of state-of-art approaches	BBE-RDHEI generates marked decrypted images with the high quality, and it's capable of withstanding differential, brute-force, data loss and noise attacks
2	Xiao, D., et al. (2017)	S-RDH in encrypted image relying on PVO	Embedding rate reaches to 0.2018bpp.	Lena, Airplane images achieved a better embedding rate.
3	Dragoi, I. et al. (2017)	Reserving Room After Encryption and Pixel Prediction	Embedding rate < 0.1 bpp.	Smaller than 1%error rate, and its offer a proposed method.
4	Puteaux, P., &Puech, W. (2018)	MSB Prediction	The embedding rate reaches to 0.0359 bpp	Using the images of Lena, Man and Crowd, Airplane, with MSB method leads to decrease the payload to 0.0359bpp for Lena, 0.0212bpp for Man, 0.0111bpp for Airplane and 0.0145bpp for a Crowd.
5	Ge, H., et al. (2018)	Multi-Level method	It was found the perfect embedding rate reaches to 0.6714bpp, while at single level it reaches to 0.1561 bpp, and finally at the double level it reaches to 0.2723. Therefore Using multi-	When using multi-level method with images: (Airplane, Barbara, Baboon, Lena, Peppers and Boat, House, Sailboat, Splash, Stream, and Tank).

No	Author name and year	Proposed Methods with RDH-EI	Embedding rate	Notes
			level improves the embedding capacity significantly.	
6	Su *etal.* (2018)	RDH is utilizing dynamic block-partition	embedding rate has extreme limit and variations in the size of the blocks	it has high imperceptibility, robustness, and maximal capacity, but variations in PSNR performance
7	Qin, C., et al. (2019),	redundancy transfer and sparse block coding	The best embedding rate was 1.5352 bpp.	A number of tests were done with images (Airplane, Barbara, Baboon, Lena, Peppers and Boat).
8	Ma, G., & Wang, J. (2019)	multi-stage integer wavelet transform	The better capacity of data embedding rate reaches until 0.8285bpp	Via are using six images: Airplane, Barbara, Baboon, Lena, Peppers and Boat, gain better capacity of data embedding rate reach until 0.7643bpp, 0.7363bpp, 0.8285bpp, 0.8101bpp, 0.6811bpp and 0.7738bpp respectively.
9	Xiao *etal.* (2019)	adaptive RDH	The embedding rate is limited	The suggested model can use the image redundancy and signifies suitable advantages in comparison to some state-of-art studies.
10	Wu *etal.* (2019)	RDH in encrypted images	Embedding rate is average	Achieve with proper algorithm, message is embedded then extracted accurately.
11	Gao, H., et al. (2020)	image encoding and POB	The maximal embedding rate reached 3.75bpp	Obtains maximum capacity of embedding rate reaches 3.75bpp, 1.93 bpp, 3.51 bpp for Lena, Peppers and Baboon images respectively.
12	Long, M., et al. (2020)	Tromino scrambling and adaptive PVO	The better embedding rate reaches to 0.1732bpp	Achieve better capacity of embedding rate reach to 0.1732bpp, 0.0653 bpp, 0.1608bpp, 0.1423bpp, 0.1687bpp, 0.1611bpp for Lena, Baboon, Peppers, Man, Barbara, Boat images.
13	Xu W., et al. (2021)	images (RDHEI) with compresses prediction errors	The embedding rate is significantly enhanced in comparison with these state-of-art	Huffman coding approach has been proposed for the compression of the prediction errors in usable blocks for embedding abundant additional

No	Author name and year	Proposed Methods with RDH-EI	Embedding rate	Notes
			schemes.	data.
14	Ryota M., et al (2021)	Two different methods for (RDH-EI)	The other region has significantly high rate of embedding, about 1bpp.	One part may be decrypted without the extraction of the data and additionally losslessly compressed with the use of the image coding standards even after processing. Experimental results have shown the suggested approach's effectiveness concerning the efficiency of lossless compression and hiding capacity

However, from the comparison has been noticed in all presented methods it is not possible to re-construct that image without fault, with a very low embedding rate (< 0.1bpp)to reduce the introduced distortion. Thus, it is possible obtaining an image that is very similar to original image during the retrieval process, but by embedding rate (>0.1 bpp) as shown in Table (2). Also, it has been observed when using the technique of BBE-RHEI with embedding rate (> 0.1bpp), the image is retrieved in a perfect manner and this leads to giving a robust to the application which is using RDHEI techniques, but the pre-processing step is still needed. Figure 3 illustrated the best method is number 11 that gives the best embedding rate reaches to 3.75 bpp.

Table (2) Effectiveness the Embedding Rate on the Retrieve Image.

No	Embedding Rate	Retrieve Image
1	Very low (<0.1)	reduce the introduced distortion.
2	High (>0.1)	very similar to the original image

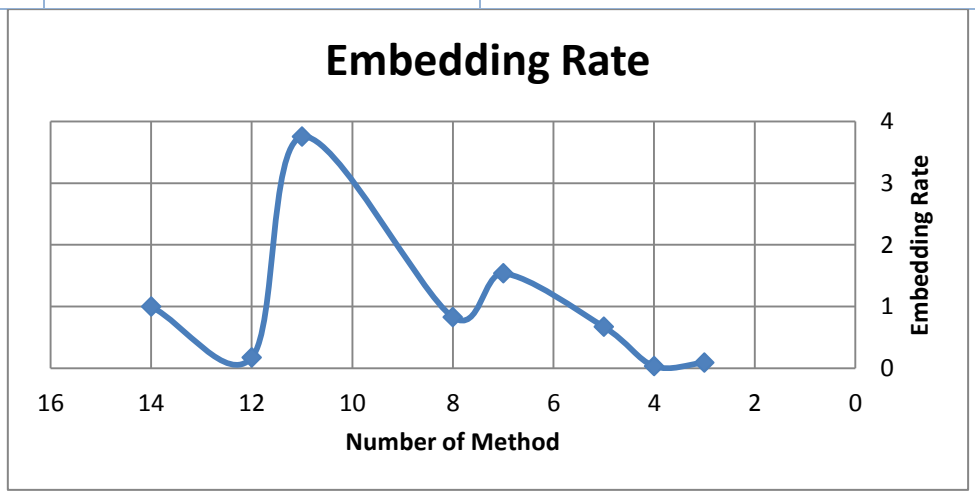

Figure (3) Embedding Rate for Many Proposed Methods

6- CONCLUSIONS.

In this paper, a literature review of RDH-EI methods over five years (2017-2021) has been presented for two purposes: to show how can maintain confidentiality, integrity and authentication of images, in addition to the ideal reconstruct it from the receiver side. Several methods of RDH-EI with different embedding rate data have been utilized to achieve the two purposes above, and it is concluded the following:

First: when the rate of embedding is low (< 0.1bpp), it is impossible to reconstruct the image without fault.

Second: it is possible obtaining an image that is very similar to original image when embedding rate (> 0.1bpp).

Third: if: an image is retrieved in a perfect manner, but still needed to the pre-processing step when the embedding rate (> 0.1bpp).

Also, the technique of BBE-RHEI with embedding rate (> 0.1bpp), the image is retrieved in a perfect manner but the pre-processing step is still needed. The best method is number 11 that gives the best embedding rate reaches to 3.75bpp. In future we can be suggested a new faster hiding method that combining the compressed sensing image steganography (CSIS) scheme with sparse block coding of encrypted image for achieving best embedding rate and requires less amount of time for data extraction & image recovery.

REFERENCES.

1. Zhang, X. (2012), “Separable reversible data hiding in encrypted image”, IEEE Transactions on Information Forensics and Security, 7 (2), 826–832.
2. Zhong, H., & Chen, X. (2020), “A separable reversible data hiding scheme in encrypted image for two cloud servers”, In Int. J. Embedded Systems (Vol. 12, Issue 1).
3. Ma B., Shi Y.Q. (2016), "A reversible data hiding scheme based on code division multiplexing", IEEE Trans. Inf. Forensics Secur., 11, (9), pp. 1914– 1927
4. Yi, S., & Zhou, Y. (2017), “Binary-block embedding for reversible data hiding in encrypted images”, Signal Processing, 133, P.P. 40–51.
5. Ma, X., Pan, Z., Hu, S., & Wang, L. (2015), “ High-fidelity reversible data hiding scheme based on multi-predictor sorting and selecting mechanism”, Journal of Visual Communication and Image Representation, 28, 71–82.
6. Li, X., Zhang, W., Gui, X., & Yang, B. (2015), “Efficient Reversible Data Hiding Based on Multiple Histograms Modification”, IEEE Transactions on Information Forensics and Security, 10 (9), 2016–2027.

7. Ong, S., Wong, K., & Tanaka, K. (2015), "Scrambling-embedding for JPEG compressed image", Signal Processing, 109, 38–53.
8. Zhang, X., Long, J., Wang, Z., & Cheng, H. (2016), "Lossless and Reversible Data Hiding in Encrypted Images with Public-Key Cryptography", IEEE Transactions on Circuits and Systems for Video Technology, 26 (9), 1622–1631.
9. Mobasseri B.G., Berger R.J., Marcinak M.P. et al. (2010), 'Data embedding in JPEG bit stream by code mapping', IEEE Trans. Image Process., 19, (4), pp. 958– 966
10. Kim S., Lussi R., Qu X. et al. (2015), " Automatic contrast enhancement using reversible data hiding'. Proc. IEEE Int. Workshop on Information Forensics and Security, Xiamen, China, pp. 1– 5
11. Cancellaro M., Battisti F., Carli M. et al. (2011), 'A commutative digital image watermarking and encryption method in the tree structured Haar transform domain', Signal Process., Image Commun., 26, (1), pp. 1– 12
12. Qin C., Zhang X. (2015), 'Effective reversible data hiding in encrypted image with privacy protection for image content', J. Vis. Commun. Image Represent., pp. 154– 164
13. Zheng S., Li D., Hu D. et al. (2016), 'Lossless data hiding algorithm for encrypted images with high capacity', Multimedia Tools Appl., pp. 13765– 13778
14. W. Bender, D. Gruhl, and N. Morimoto. (1996), "Techniques for data hiding, "IBM Syst. J., vol. 35, nos. 3-4, pp. 313-336.
15. F. Petitcolas, R. Anderson, and M. Kuhn. (1999), "Information hiding—A survey, "Proc. IEEE, vol. 87, pp. 1062-1078.
16. Ma K., Zhang W., et al. (2013) "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption, " IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, 553-562.
17. Hong W., Chen T., and Wu H., (2012) "An improved reversible data hiding in encrypted images using side match, " IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202.
18. Qian Z., Han X. and Zhang X., (2013) "Separable Reversible Data hiding in Encrypted Images by n-nary Histogram Modification, " 3rd International Conference on Multimedia Technology (ICMT 2013), pp. 869-876, Guangzhou, China.
19. Zhang X., (2011) "Reversible data hiding in encrypted images, " IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258.
20. Zhang, K. Ma and N. Yu, (2014) "Reversibility improved data hiding in encrypted images" Signal Processing, vol. 94, pp. 118–127.
21. Xiao W. D., Xiang, Y., Zheng, H., & Wang, Y. (2017), "Separable reversible data hiding in encrypted image based on pixel value ordering and additive homomorphism", Journal of Visual Communication and Image Representation, PP. 1–10.

22. Dragoi, I. Henri-George C., and Dinu C. (2017), "Improved reversible data hiding in encrypted images based on reserving room after encryption and pixel prediction. ", IEEE European Signal Processing Conference (EUSIPCO), pp. 2186-2190.
23. Puteaux, P., &Puech, W. (2018), "An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images", IEEE Transactions on Information Forensics and Security, 13 (7), 1670–1681.
24. Ge, H., Chen, Y., Qian, Z., & Wang, J. (2018), "A High Capacity Multi-Level Approach for Reversible Data Hiding in Encrypted Images", IEEE Transactions on Circuits and Systems for Video Technology.
25. Su W., Wang X., Li F. et al. (2019) 'Reversible data hiding using the dynamic block-partition strategy and pixel-value-ordering', Multimedia Tools Appl., 78, (7), pp. 7927– 7945
26. Qin, C., Qian, X., Hong, W., & Zhang, X. (2019), " An efficient coding scheme for reversible data hiding in encrypted image with redundancy transfer", Information Sciences, 487, 176–192.
27. Ma, G., & Wang, J. (2019), "Efficient reversible data hiding in encrypted images based on multi-stage integer wavelet transform", Signal Processing: Image Communication, 75, 55–63.
28. Xiao M., Li X., Wang Y. et al. (2019), 'Reversible data hiding based on pairwise embedding and optimal expansion path', Signal Process., 158, pp. 210– 218
29. Wu H.T., Cheung Y.M., Yang Z. et al. (2019), 'A high-capacity reversible data hiding method for homomorphic encrypted images', J. Vis. Commun. Image Represent., 62, pp. 87– 96
30. Gao, H., Gao, T., You, Z., & Cheng, R. (2020), "High capacity reversible data hiding in encrypted image based on image encoding and POB", Journal of the Franklin Institute, 357 (13), 9107–9126.
31. Long, M., Zhao, Y., Zhang, X., & Peng, F. (2020), "A separable reversible data hiding scheme for encrypted images based on Tromino scrambling and adaptive pixel value ordering", Signal Processing, 176.
32. Xu W., Li-Yao L., Ching-Chun C., and Chih-Cheng C. (2021), "High-Capacity Reversible Data Hiding in Encrypted Images Based on Prediction Error Compression and Block Selection', Hindawi Security and Communication Networks, 9606116, pp. 6-12.
33. Ryota M., Shoko I., and Hitoshi K. (2021), ' A Reversible Data Hiding Method in Encrypted Images for Controlling Trade-Off between Hiding Capacity and Compression Efficiency', Journal of Imaging, PP. 1-13