Research and Analysis of Different RDH algorithms on Digital Images

Devee Darshani, Dr. Isha Batra*, Dr. Arun Malik

Abstract

Information Security has been one among the largest challenges during this digital era. Images are assisting disproportionately in electronic communication during this digital aeon. Somebody transmits private images over a flabby communication network at times, absolute security is an accost argument to maintain image privacy. Encryption is one of the methods for gripping image reticence. Image encryption adds to the charter security of a preeminent bite for safe transmission of view over the net. For example, medical images, forensic images, military images etc. are such sensitive images where a minimum distortion can lead to the incorrect diagnosis. Thus, these type of images needs security, a proper authentication process, data hiding mechanism for hiding sensitive data, and overall maximum reversibility of the cover image.

In digital image systems reversible data hiding has its own importance. Numerous techniques of data hiding are used for digital image hiding, among which RDH is best fit technique for lossless recovery privacy protection. In various image domains such as, compressed and uncompressed, most RDH techniques are proposed. RDH is more significant in terms of its efficiency and applicability for natural uncompressed image domain. The present RDH algorithms on digital image are outlined in this paper.

Keywords: Encryption; Embedding Capacity; Natural images; RDH

1. Introduction

Data security is basically to protect the data from unauthorized users and attackers. In the current age of multimedia and internet, large volumes of images are being transferred. A person transmits both private and essential images over a public communication network during times. Image immerses the vast snippet of data communication and, plays a significant role for example; military, medical services and diplomatic concerns. Encryption is the way protection is assured.

Encryption is the conversion of plain text message into cipher, while decryption is the otherway around to turn cipher text into plain text.Image encryption is a technique which provides security to the image by converting original image to coded image which is not easier to detect. No one can know the content of the image without a key for decryption.In the field of recent digital image applications Reversible data hiding is an important means for guaranteeing security and privacy.

This is a method of secret communication where a piece of data or secret message is hidden in such a way that the very presence of the key information remains obscured without raising any doubt in the viewers' minds and thus preventing its detection. This is often done by embedding a chunk of data into another piece of innocent looking information, and may be a spatial or time-consuming or transforming domain method of these methods hides information in various media varieties such as text, picture, audio, video, etc. Digital images are more widely used in the implementation of knowledge hiding strategies due to their scale and popularity among these kinds of mediaavailable.

2. Reversible Data Hiding

Reversible Data Hiding intends to extract the original and lossless state of the image at the receiver end from the cover image. This method is used not just for hiding data but also for the whole recovery from the encrypted image of the original image. This technique is most desirable in those applications where degraded restoration is not allowed, like, medical images, forensic images, military maps, etc. Although a lot of data hiding techniques are there but only RDH holds the top priority when there is a demand for lossless retaining.

RDH can recover the initial image with none distortion from the marked or embedded image.It is a way that the marked media can be returned to the first coverage after the secret information has been removed. It requires reversible or lossless capability.A special reversible data hiding algorithm, which can retrieve the original image without distortio n from the marked image after removing the hidden images.

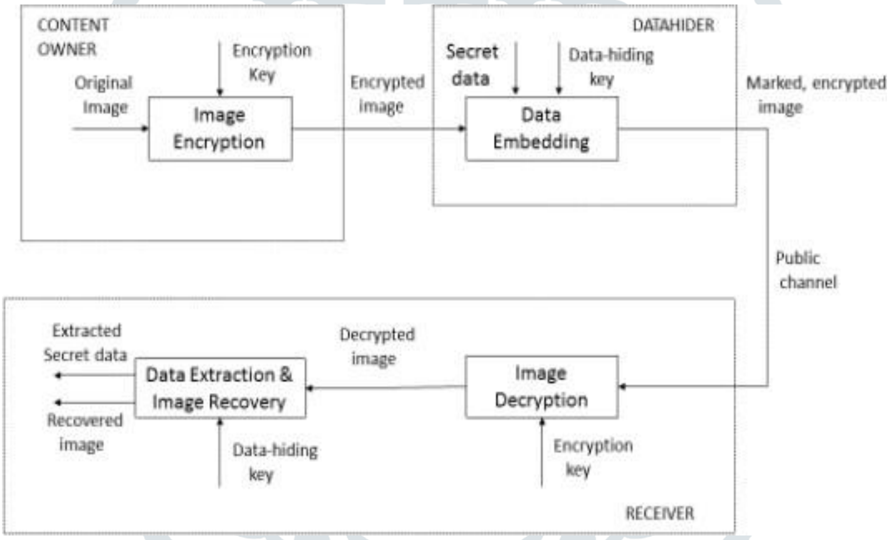

Figure 1: Framework of Reversible Data Hiding

As shown in figure, to get the encrypted image, the content owner encrypts the original image using a key known as encryption key. The data hider then conceals the secret data with a key known as data hiding the information to produce marked encrypted image. This process is known as process of data embedding. The encrypted image marked is sent via a public channel to the recipient. The marked encrypted image is first decrypted at the receiver end, using the encryption key. So it generates a decrypted image. And then the secret data is retrieved and image recovered from the image that is decrypted by using key based on data hiding.

3. Data Hiding Schemes in Digital Images

a. Reversible Data Hiding in Encrypted Image [1]

In 2011 Xinpeng Zhang initially proposed an RDH technique for images that are encrypted. The uncompressed taken image is first encrypted totally using a stream cipher by the content owner.Itisassumedthatthepixelvaluerangeofthegrey-scaleoriginalimagefallsinto0to

255. Encrypted image is constructed by an XOR operation with the encryption key which is calculated by a standard stream cipher. The data hider cannot see the original image content but he can modify the encrypted image for marking the image for authentication or embed additional data for privacy preservation. The data hider divides the encrypted image intosame size non-overlapping blocks. Then one additional bit is being embedded into each S x S sized, The S^2 pixels comprising a block is segmented in two groups S_0 and S_1. The pixels are pseudo-randomly divided thus probability of a pixel belonging to groups S_0 or S_1is1/2. If secret bit that is hided is 0 then 3 LSBs of all encrypted pixels in s_0 are flipped. Likewise, 3 LSBs are flipped in groups S_1 when 1 is the additional bit. The remaining part of the encrypted image is left unchanged. The recipient by using encryption keys generates bits that are pseudo-random in data extraction and image recovery processes and computes the XOR of the information received to decrypt the image. The five MSB bits remain identical to the original MSB bits and recovered properly during decryption. The last three least significant bits needed to be recovered properly. Each and every pixel is checked for data extraction. If, the bit to be extracted is one and it resides in the S_0 portion of the pixel, and the bit to be extracted is zero and it resides in the S_1 portion of the pixel, then, there is no alteration done through the embedding process.

It suggests that the decrypted pixel is recovered totally. However, in the alternative situation, if the bit to be extracted is zero and it resides in the S_0 portion of the pixel, and the bit to be extracted is one and it resides in the S_1 portion of the pixel, then, then the extra bits are extracted through the reverse process of data embedding using the data hidingkey.

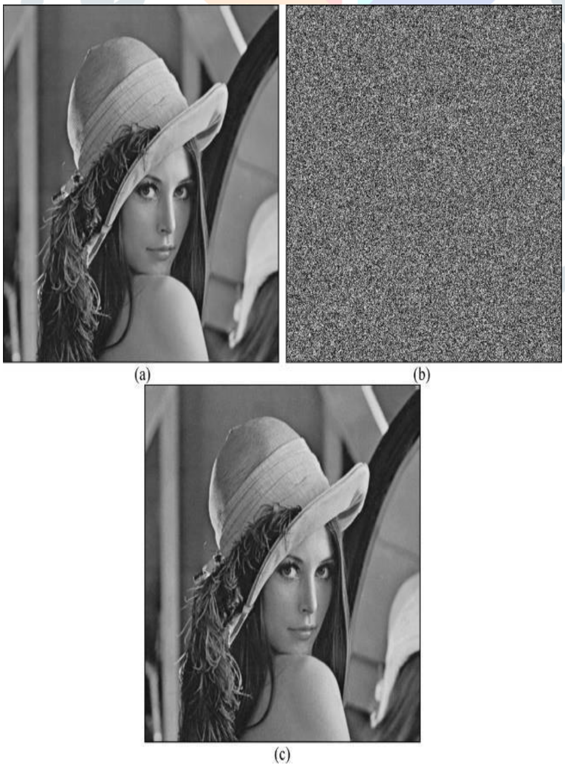

Figure 2: (a) Original Lena image, (b) encrypted image, and (c) decryptedimage.

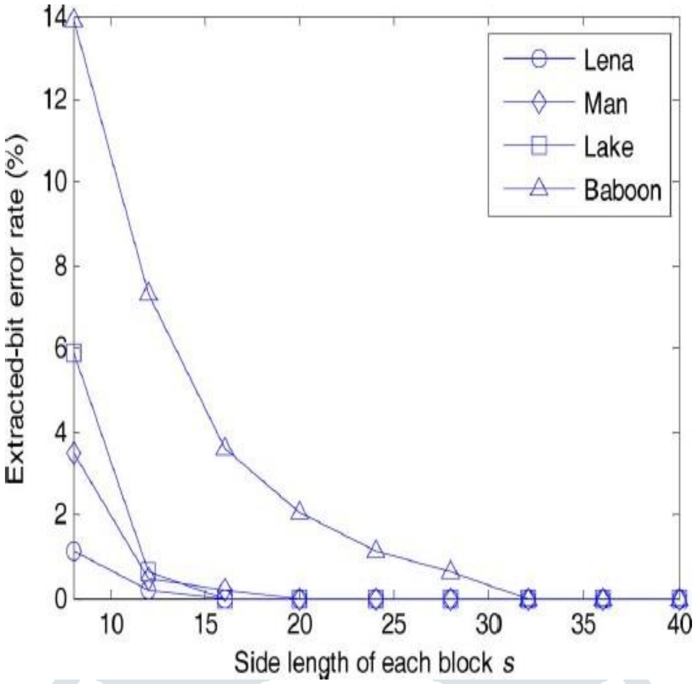

Figure 3: Extracted-bit error rate with respect to block sizes.

b. An Improved Reversible Data Hiding in Encrypted Images using Side Match [2]

In 2012, Wien Hong, et. al enhanced Zhang's method by reducingthe extracted bits error rate. In order to measure smoothness and side-matching, two metrics are used for this function. The pixel is used for smoothness assessment for each block and is used for side matching adjacent blocks, and the recovered and unrecovered blocks have a border pixel correlation.With small block size it helps to decrease the error rate of the extracted image. The fundamental embedding and encryption process is identical to the improvement in this work includes only image recovery phase with an improved version of better block smoothness estimation and recovery using side match. The neighboring pixels are left out in. The absolute differences can be utilized for accurate evaluation of smoothness of any given pixel block. The usual data extraction and recovery are done exactly as the previous method. After that, the smoothness function is applied to all the neighboring pixels. All the blocks arerecovered.

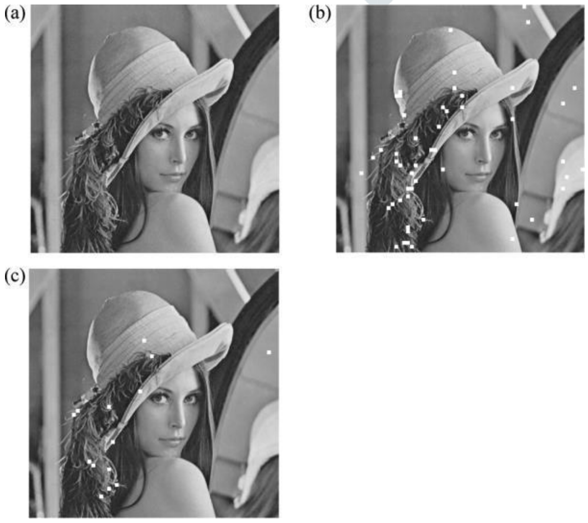

Figure 4: (a) Decrypted image using content owner’s key. (b) Blocks of incorrect recovery of Zhang’s method. (c) Blocks of incorrect recovery of the proposed method.

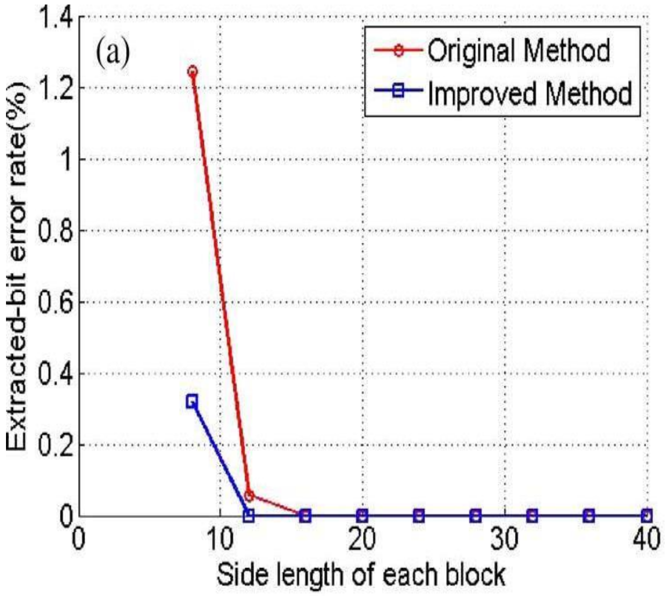

Figure 5: The error rate comparison.

c. Separable Reversible Data Hiding in Encrypted Images[3]

New separable RDH model for the encrypted image was proposed by XinpengZhang in 2012. It is still based on the same architecture as the previous model of Zhang[1]. It gives the recipient's three different options. If the recipient has the key to decrypt, the original image can be recovered, and if the recipient has the data embedding key, the additional bits can be retrieved and the key is used to encode data, the original image and the hidden bits can also be recuperated. The encryption is carried by the same method of creating the encrypted image previously used.In the embedding phase, the LSBs are compressed to create space for additional data hiding. The data hider randomly selects a small integer (N_p) which will contain the data hiding constraints. The remaining (N-N_p) pixels are distributed into groups having the same number of pixels. The LSBs are selected from each group and N_p numbers of LSB are chosen among them for additional data embedding.

During embedding, no MSB is altered and the receiver can recover the picture but not the built-in bits if it has the encryption key. The extra bits can be extracted with the data hiding key; however, the encrypted image cannot be decrypted without the encryption key.

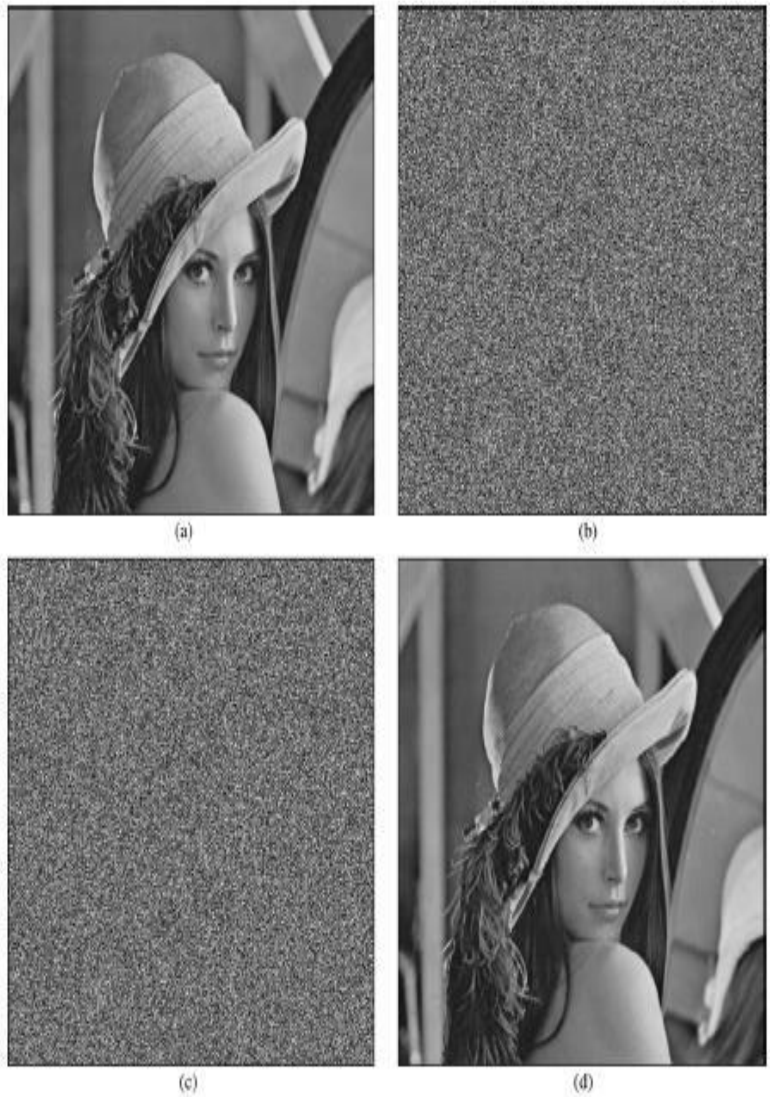

Figure 6 (a) Original Image (b) Encrypted Image (c) Encrypted image containingembedded data with embedding rate with 0.017 bpp (d) directly decrypted version with PSNR 39.0 dB

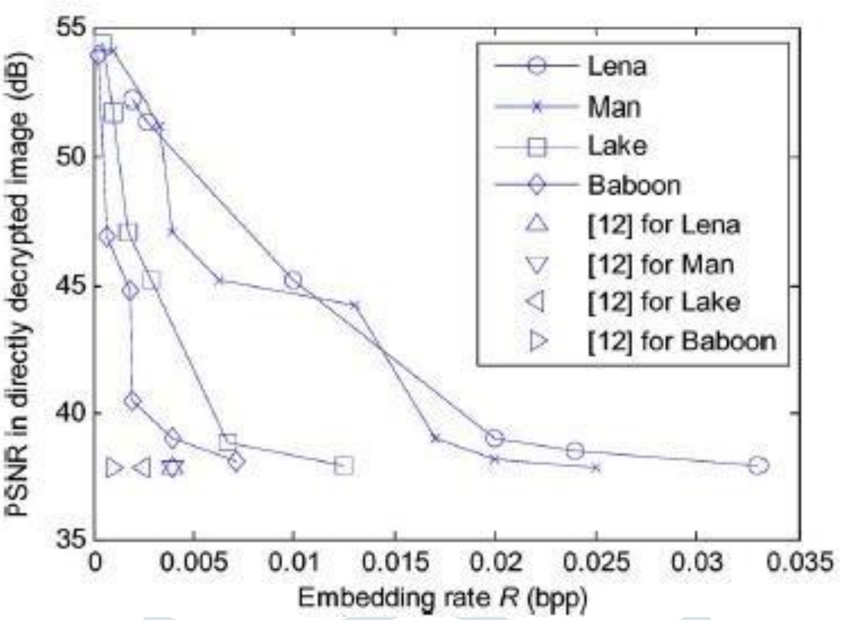

Figure 7: Comparison of Embedding Rate and PSNR

d. High-capacity Reversible Data Hiding in Encrypted Images by Prediction Error [4]

Xiaotian Wu and Wei Sun proposed in 2014 a new RDH method with the help of prediction errors for encrypted images. In this proposed scheme the implementation of a prediction error is provided with two RDH approaches. All methods are a process and a system which can be isolated. As the name implies, data recovery and image recovery is performed at once, while image recovery and data recovery are performed separately in the distinguishable method. Both technologies produce good quality of images and high capacity for embedding. The joint method consists of three phases: image encryption, hiding and collecting and reconstruction of the image.In almost the same way as previous methods, encryption and data protection are carried out. In the extraction and recovery process the difference and new features. For the actual assessment of any given pixel, an enhanced context adaptive interpolation algorithm is proposed. The pixels are grouped into eight different categories depending on their neighboring pixels to redefine the actual pixel value.

The separable method enables various mechanisms to extract data and to recover images. In the joint process, both mechanisms are strongly intertwined.If two keys are available then both the image recovery process are carried out jointly. In the separable method, one task can be performed with the concernedkey.

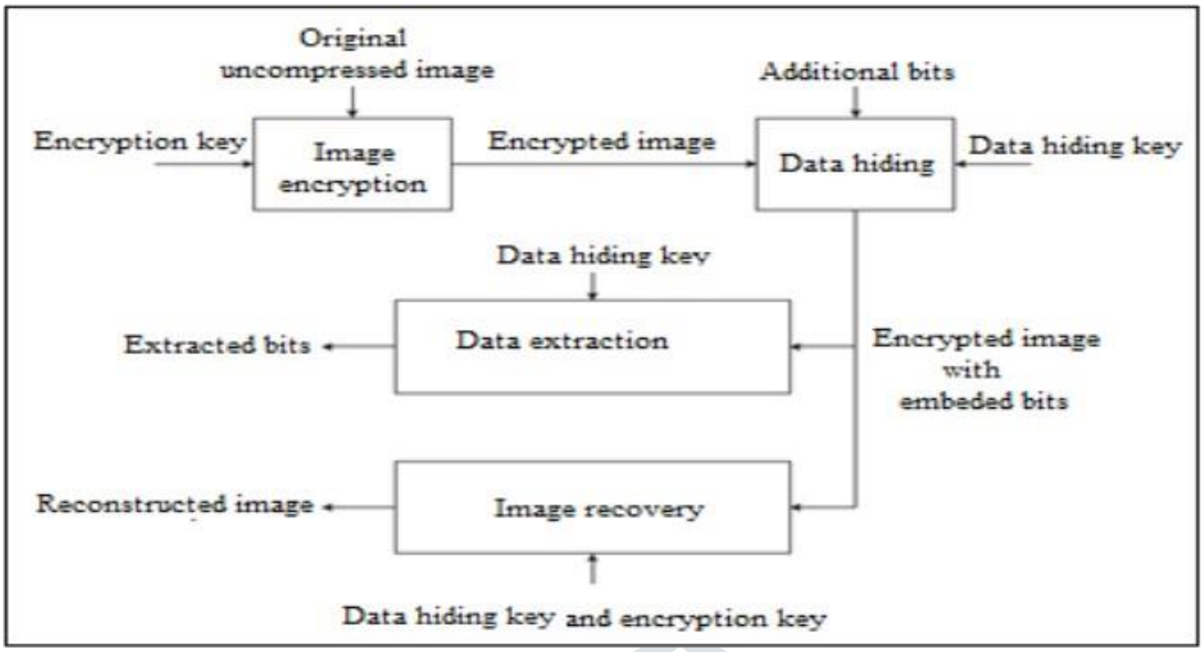

Figure 8: Architectural representation of a separable method

In the image and data recovery method of the method that is separable, two distinct cases are considered. If receiver has only one key, he can perform the task in question and almost retrieve the image lossless or extract additional bits. In case the authenticated person possesses the two necessary keys then he can perform both operations separately.

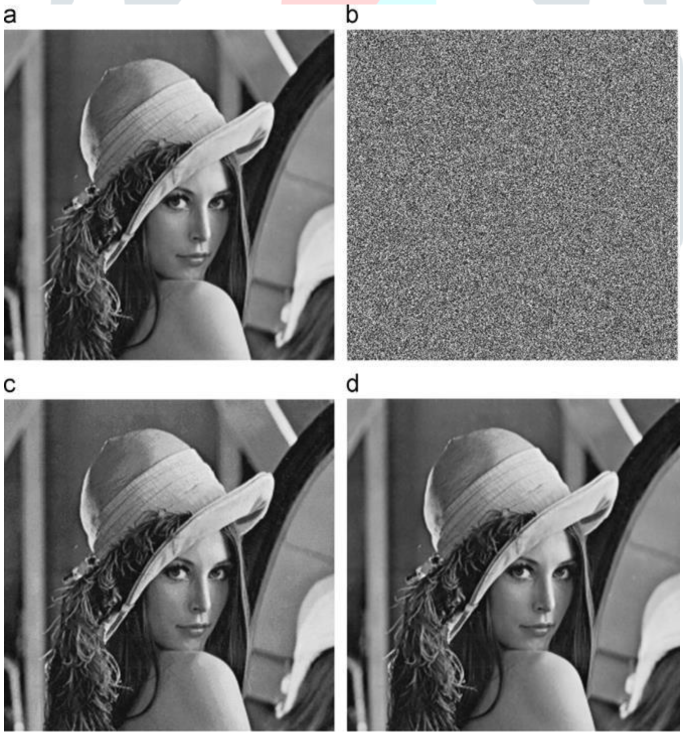

Figure 9: (a) Original image Lena, (b) encrypted image with embedded bits, (c) directly decrypted image, (d) recovered image after data extraction.

e. Improved joint reversible data hiding in encrypted images [5]

In 2016, Zhenxing Qian, Shu Dai, Fei Jiang and Xinpeng Zhang proposed a joint embedding mechanism for improved RDH methods. It follows the essential characteristics for encrypted image of conventional RDH approach. Choose an initial grayscale O image of 0 to 255 pixel size. Then, use the stream cipher to select an encryption key to produce pseudo-random bits. In order to receive encrypted image E, exclusive OR is performed between the original image and encryption key. E is divided into four sub-images E1, E2, E3 and E4 for data integration into the encrypted image.

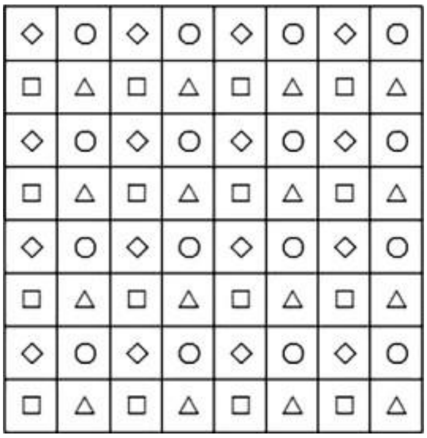

Figure 10: Image down sampling

Data hider used to embed the message on the E2, E3 and E4 for first round of embedding by removing the three LSB layers of a cyclic shifting data hiding algorithm. The hider data then replaces with updated data the original data from E2, E3 and E4 of three LSB layers. Then encrypted marked sub images are generated E2', E3' and E4'. For second round embedding the data swapping based embedding algorithm has been used for sub image E1. ExtractthreeLSB layer from E1. Then divide E1 into set of blocks of size r x r. Then block swapping of corresponding blocks has been done. Then encrypted marked image is generated E1'. After doing cyclic shifting and data swapping E1', E2', E3' and E4' are merged to construct encrypted marked image E'. For image recovery and data recovery the same process is begin repeated at the end of receiver.

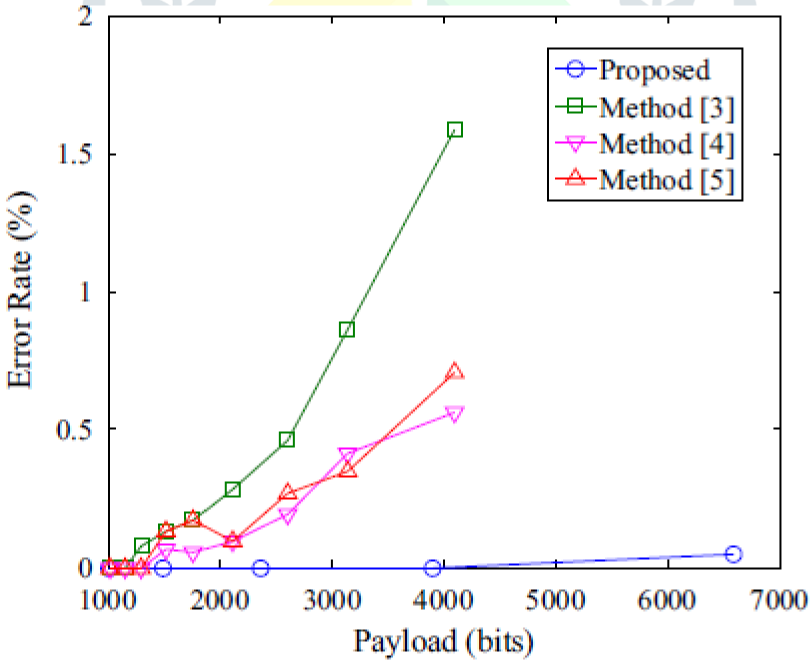

Figure 11: The relation between embedding payload and error rate

f. An improved LSB-based RDH technique with better reversibility[6]

In 2017, Mondalet. al proposed a new RDH method for LSB modification technique. The algorithm consists of four sub-processes. Each sub-process have different algorithms, like encryption, embedding, decryption, and recovery. Choose a gray image with a pixel value of 0 to 255 from original image. Then select an encryption key that generates random pseudo bits via stream cipher. In between the original image and the encryption key, exclusive OR is performed to get encrypted image E. The encrypted image is divided into blocks of the order Z x Z for the embedding of the information. The embedding of the 1st row of the pixel is also carried out in all other blocks. This then takes place between the consecutive rows, the XOR operation of three LSB. The pixel stays the same when the value is 000. The third LSB is turned to the left and the fourth LSB in the row is tilt.For decryption the XOR operation is done in between embedded image and encrypted key to generate the decrypted image. For image recovery the same process is done that is done in data embedding to get recoveredimage.

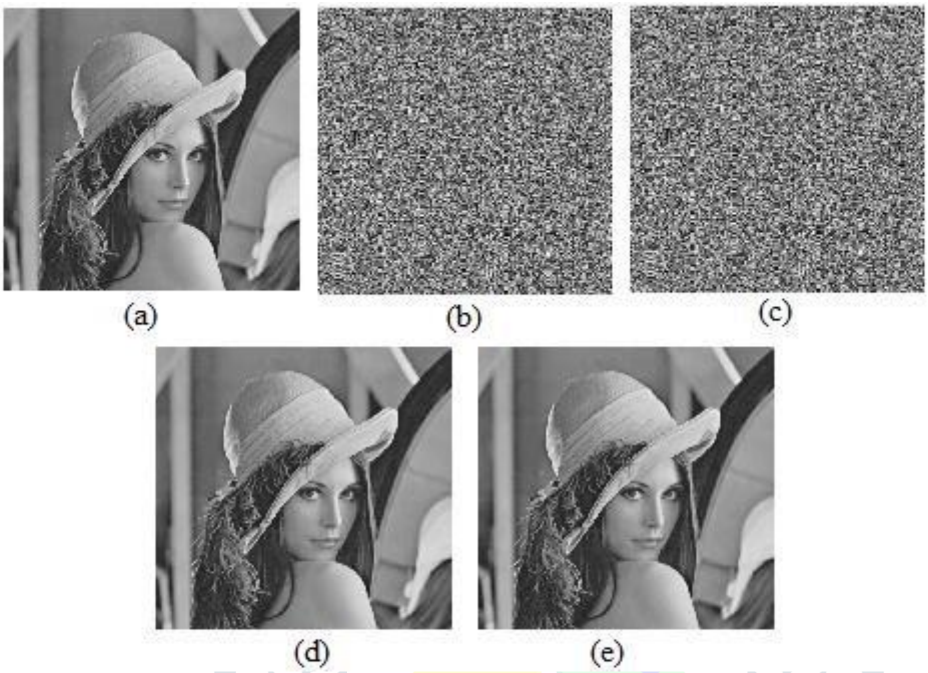

Figure 12: (a) original image (b) encrypted image (c) marked encrypted image (d) decrypted image (e) recovered image

4. Comparison of Reviewed Papers

In the previous section six recent RDH schemes aimed at digital images are reviewed. The findings of the experiment are replicated and evaluated. All approaches are pretty unique and efficient. Tables 1 and 2 show a comparison of the above-mentioned algorithms which supported their PSNR values and bits of data embedding.

Table 1: A PSNR table comparison in images directly decrypted

Papers	Baboon	Lake	Man	Lena
[1]	37.95	37.87	37.77	37.94
[2]	37.94	37.77	37.87	37.94
[3]	38.45	38.30	38.20	38.50
[4]	38.13	38.12	38.11	38.14
[5]	46.84	55.86	48.87	61.50

Table 2: Table of comparison on embedding in bits

Papers	Baboon	Lake	Man	Lena
[1]	196	1024	625	1156
[2]	225	1296	900	1296
[5]	629	2094	3630	3897

5. Conclusion

In a digitalized world, digital images need the utmost protection. With the Internet's superiority and convenience all is going online. RDH is the best method to ensure confidentiality and security of sensitive content in digital images. This article aims to explain a digital image of recent RDH ventures. All six methods that have been extensively checked during this paper are well productive in digital images for data embedding and reversibility of prime quality. The findings of the tests provide a clear picture of their success and development.

References

[1] Zhang, Xinpeng. "Reversible data hiding in encrypted image." *IEEE signal processing letters* 18.4 (2011): 255-258.

[2] Hong, Wien, Tung-Shou Chen, and Han-Yan Wu. "An improved reversible data hiding in encrypted images using side match." *IEEE Signal Processing Letters* 19.4 (2012):199-202.

[3] Zhang, Xinpeng. "Separable reversible data hiding in encrypted image." *IEEE transactions on information forensics and security* 7.2 (2011):826-832.

[4] Wu, Xiaotian, and Wei Sun. "High-capacity reversible data hiding in encrypted images by prediction error." *Signal processing* 104 (2014): 387-400.

[5] Qian, Zhenxing, et al. "Improved joint reversible data hiding in encrypted images." *Journal of Visual Communication and Image Representation* 40 (2016):732-738.

[6] Mondal, Jayanta, et al. "An improved LSB-based RDH technique with better reversibility."*InternationalJournalofElectronicSecurityandDigitalForensics*9.3(2017):254- 268.