International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

A Novel Method for Reversible Data Hiding in Encrypted Images

Amol Baban Chavan[1], Ashis A. Zanjade[2]

[1]Department of Electronics & Telecommunication, Yadavrao Tasgaonkar Institute of Engineering & Technology Chandai, Karjat. Dist- Raigad – 410 201 (Maharashtra)

[2]Department of Electronics & Telecommunication, Yadavrao Tasgaonkar Institute of Engineering & Technology Chandai, Karjat. Dist- Raigad – 410 201 (Maharashtra)

Abstract: ***Recently, reversible data hiding (RDH) in encrypted images is the most important property that the original cover can be lossless recovered after embedded data is extracted while protecting the image content's confidentiality. Due to use of embedding data by reversibly vacating room from the encrypted images, this method may be subject to some errors on data extraction and image restoration. In this paper, we propose method by reserving room before encryption with a traditional reversible data hiding algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. This method can achieve real reversibility, data extraction and image recovery are free of any error. According to this method, it can embed more times as large payloads for the same image quality as the previous methods, such as for PSNR dB.***

Keywords: Reversible Data Hiding, Image Encryption, Novel Method of RDH, Encryption Techniques, Difference Expansion, Histogram Shift

1. Introduction

Reversible data hiding (RDH) is a technique in image processing area for encryption, by which the original cover can be losslessly recovered after the embedded message, is extracted. The RDH approach is widely used in medical science, defense field and forensic lab, where there is no degradation of the original content is allowed. Since more research RDH method in recently. In theoretical aspect rate-distortion model for RDH Kalker and Willems [2], through which they proved the rate-distortion bounds of RDH for memory less covers and proposed a recursive code construction which, however, does not approach the bound. The recursive code construction for binary covers and proved that this construction can achieve the rate-distortion bound as long as the compression algorithm reaches entropy, which establishes the equivalence between data compression and RDH for binary covers. Many RDH techniques have emerged in recent years. Fridrich et al [3] constructed a general framework for RDH for method. By first extracting compressible features of original cover and then compressing them lossless, spare space can be saved for embedding auxiliary data.

A various RDH method is more popular is based on difference expansion (DE) [4], in which the difference of each pixel group is expanded by various method or technique. Example, multiplied by 2, and thus the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages. Another reliable strategy for RDH is histogram shift (HS), in which space is saved for data embedding by shifting the bins of histogram of gray values. With respective to providing confidentiality for images, encryption is an effective and popular means as it converts the original and meaningful content to non-readable one. Although there are few RDH techniques in encrypted images have been published yet, there are some promising applications if RDH can be applied to encrypted images. Hwang et al. advocated a reputation-based trust management scheme enhanced with data coloring (a way of embedding data into covers) and software watermarking, in which data encryption and coloring offer possibilities for upholding the content owner's privacy and data integrity.[5]In our system we provide the high quality image to the users. It also provides the more security of the data. The proposed system is reduces the time as well as cost as compared to previous system.

2. Previous Methods

The methods proposed in [6]-[8] can be summarized as the framework, "vacating room after encryption (VRAE)", as illustrated in Fig. 1(a).

In this framework, a content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider (e.g., a database manager) and the data hider can embed some auxiliary data into the encrypted image by losslessly vacating some room according to a data hiding key. Then a receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key.

In all methods of [6]-[8], the encrypted 8-bit gray-scale images are generated by encrypting every bit-planes with a stream cipher. The method in [6] segments the encrypted image into a number of non-overlapping blocks sized by *a X a*; each block is used to carry one additional bit. To do this, pixels in each block are pseudo-randomly divided into two sets *S1* and *S2* according to a data hiding key. If the additional bit to be embedded is 0, flip the 3 LSBs of each encrypted pixel in *S1*, otherwise flip the 3 encrypted LSBs of pixels in *S2*. For data extraction and image recovery, the receiver flips all the three LSBs of pixels in *S1* to form a new decrypted block, and flips all the three LSBs of pixels in *S2* to form

another new block; one of them will be decrypted to the original block. Due to spatial correlation in natural images, original block is presumed to be much smoother than interfered block and embedded bit can be extracted correspondingly. However, there is a risk of defeat of bit extraction and image recovery when divided block is relatively small (e.g. a=8) or has much fine-detailed textures.

Hong *et al.* [7] reduced the error rate of Zhang's method [6] by fully exploiting the pixels in calculating the smoothness of each block and using side match. The extraction and recovery of blocks are performed according to the descending order of the absolute smoothness difference between two candidate blocks and recovered blocks can further be used to evaluate the smoothness of unrecovered blocks, which is referred to as side match.

Zhang's method in [8] pseudo-randomly permuted and divided encrypted image into a number of groups with size of L. The P LSB-planes of each group are compressed with a parity-check matrix and the vacated room is used to embed data. For instance, denote the pixels of one group by $x_1,\ldots,x_L$, and its encrypted P LSB-planes by c that consists of $\boldsymbol{P \cdot L}$ bits. The data hider generates a parity-check matrix $\boldsymbol{G}$ sized, $\boldsymbol{(P \cdot L - S) X P.L}$ and compresses $\mathbf{c}$ as its syndrome $\mathbf{s}$ such that $\mathbf{s = G \cdot c}$. Because the length of $\mathbf{s}$ is $\boldsymbol{(P \cdot L - S)}$, $\boldsymbol{S}$ bits are available for data accommodation. At the receiver side, $8 - \boldsymbol{P}$ the most significant bits (MSB) of pixels are obtained by decryption directly. The receiver then estimates x_i $(1 \le I \le L)$ by the MSBs of neighboring pixels, and gets an estimated version of $\boldsymbol{c}$ denoted by $\boldsymbol{c}'$. On the other hand, the receiver tests each vector belonging to the coset $\boldsymbol{\Omega(s)}$ of syndrome $\mathbf{s}$, where $\boldsymbol{\Omega(s) = \{u \,|G.u = s\}}$. From each vector of $\boldsymbol{\Omega(s)}$, the receiver can get a restored version of $\boldsymbol{c}$, and select the one most similar to the estimated version $\boldsymbol{c}'$ as the restored LSBs.

3. Reversible Data Hiding (RDH)

Digital steganography and watermarking are the two kinds of data hiding technology to provide hidden communication and authentication. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" [3] defining it as "covered writing". In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises, the goal of steganography is to hide a secret message inside harmless medium in such a way that it is not possible even to detect that there is a secret message. To human eyes, data usually contains known forms, like images, videos, sounds and text. Most internet data naturally includes unwarranted headers too. These are media exploited using steganograpy techniques. Images are the most powerful medium for data hiding because of the limitation of Human visual System(HVS). Basic idea of watermarking is to embed covert information into a digital signal, like digital audio, image, or video, to trace ownership or protect privacy. Data hiding can be used in a large amount of data formats in the digital world of today. The most popular data formats used are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav mainly because of their popularity on the Internet.

An information-hiding system is characterized using four different aspects: capacity, security, perceptibility and robustness [2] .

- Capacity -refers to the amount of information that can be hidden in the cover medium.
- Security- refers the inability of the hacker to extract hidden information.
- Perceptibility -means the inability to detect the hidden information.
- Robustness- is the amount of modification the stego-medium can withstand before an adversary can destroy the hidden information.

The data embedding process will usually introduce permanent loss to the cover medium. However in some applications such as medical, military, and law forensics degradation of cover is not allowed. In these cases, a special kind of data hiding method called reversible data hiding or lossless data hiding is used. Reversible Data Hiding (RDH) in digital images is a technique that embeds data in digital images by altering the pixel values for secret communication and the cover image can be recovered to its original state after the extraction of the secret data. The block diagram of RDH is shown in Fig.2. Reversible steganography or watermarking can restore the original carrier without any distortion or with ignorable distortion after the extraction of hidden data. So reversible data hiding is now getting popular. In this paper some important reversible data hiding techniques for digital images are explained and the results are analyzed.

Cryptographic key may compress the encrypted data due to the limited channel resource. Encryption is an effective means of privacy protection. To share a secret image with other person, a content owner may encrypt the image before transmission. In some cases, a channel administrator needs to add some additional message, such as the origin information, image notation or authentication data, within the encrypted image however he does not know the original image content. It may be also expected that the original content can be recovered without any error after decryption and retrieve of additional message at receiver side. That means a reversible data hiding scheme for encrypted image is desirable. Data hiding is referred to as a process to hide data (representing some information) into cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data

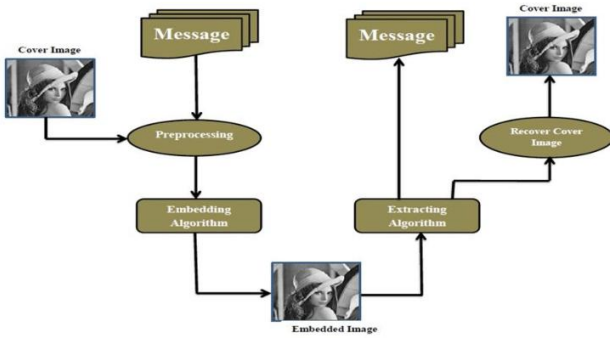

Figure 1: General Block Diagram of RDH

cryptographic key may compress the encrypted data due to the limited channel resource. Encryption is an effective means of

privacy protection. To share a secret image with other person, a content owner may encrypt the image before transmission. In some cases, a channel administrator needs to add some additional message, such as the origin information, image notation or authentication data, within the encrypted image however he does not know the original image content. It may be also expected that the original content can be recovered without any error after decryption and retrieve of additional message at receiver side. That means a reversible data hiding scheme for encrypted image is desirable. Data hiding is referred to as a process to hide data (representing some information) into cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data.

In most cases of data hiding, the cover media becomes distorted due to data hiding and cannot be inverted back to the original media. That is, cover media has permanent distortion even after the hidden data have been removed. In some applications, such as medical diagnosis and law enforcement it is desired that the original cover media can be recovered efficiently with no loss. The marking techniques satisfying this requirement are referred to as reversible, lossless, distortion-free or invertible data hiding techniques. Performance of a reversible data-

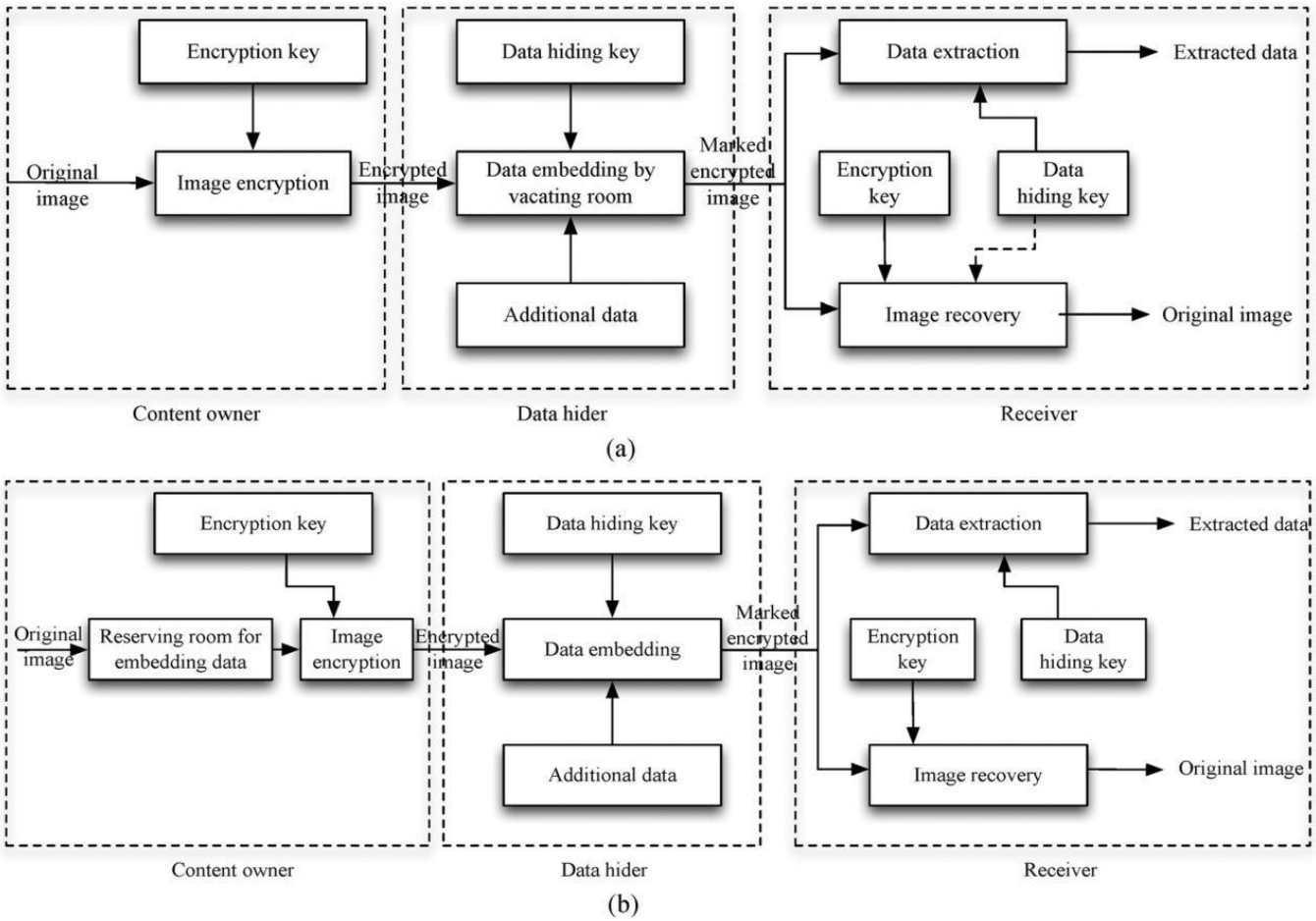

Figure 2: Framework: "vacating room after encryption (VRAE)" versus framework: "reserving room before encryption (RRBE)."

(Dashed line in (a) states that the need of data hiding key in image recovery varies in different practical methods).
(a) Framework VRAE. (b) Framework RRBE
embedding algorithm Reversible data embedding, which is also called lossless data embedding, embeds invisible data (which is called a payload) into a digital image in a reversible fashion. As a basic requirement, the quality degradation on the image after data embedding should be low. An exciting feature of reversible data embedding is the reversibility, that is, one can remove the embedded data to restore the original image. Reversible data embedding hides some information in a digital image in such a way that an authorized party could decode the hidden information and also restore the image to its original state. The performance of a reversible data-embedding algorithm can be measured by the following

- Payload capacity limit
- Visual quality
- Complexity

The distortion- free data embedding is the motivation of reversible data embedding. Data will certainly change the original content by embedding some data into it. Even a very slight change in pixel values may not be desirable, especially in sensitive imagery, such as military data and medical data. In such a scenario, every bit of information is important. From the application point of view, since the difference between the embedded image and original image is almost unnoticeable from human eyes, reversible data embedding could be thought as a secret communication channel since reversible data embedding can be used as an information carrier.

4. Proposed Method

In proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. If we reverse the order of encryption and vacating room, i.e., reserving room prior to image encryption at content owner side, the RDH tasks in encrypted images would be more natural and much easier which leads us to the novel framework, "reserving room before encryption (RRBE)".

As shown in Fig. 2(b), the content owner first reserve enough space on original image and then converts the image into its encrypted version with the encryption key. Now, the data embedding process in encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space previous emptied out. The data extraction and image recovery are identical to that of Framework VRAE. Obviously, standard RDH algorithms are the ideal operator for reserving room before encryption and can be easily applied to Framework RRBE to achieve better performance compared with techniques from Framework VRAE. This is because in this new framework, we follow the customary idea that first losslessly compresses the redundant image content (e.g., using excellent RDH techniques) and then encrypts it with respect to protecting privacy.

Next, we elaborate a practical method based on the Framework "RRBE", which primarily consists of four stages: generation of encrypted image, data hiding in encrypted image, data extraction and image recovery. Note that the reserving operation we adopt in the proposed method is a traditional RDH approach.

4.1 Encrypted Image Generation

In this module, to construct the encrypted image, the first stage can be divided into three steps:

- Image Partition
- Self Reversible Embedding followed by image encryption. At the beginning, image partition step divides original image into two parts and then, the LSBs of are reversibly embedded into with a standard RDH algorithm so that LSBs of can be used for accommodating messages; at last, encrypt the rearranged image to generate its final version .
- Image Parition: The operator here for reserving room before encryption is a standard RDH technique, so the goal of image partition.
- Self Reversible Embedding: The goal of self-reversible embedding is to embed the LSB-planes of into by employing traditional RDH algorithms.

4.2 Data Hiding In Encrypted Image

In this module, a content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider (e.g., a database manager) and the data hider can embed some auxiliary data into the encrypted image by lossless vacating some room according to a data hiding key. Then a receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key.

4.3 Data Extraction and Image Recovery

In this module, the data extraction is completely not dependent on image decryption, hence this order implies two different ways of practical applications such as

1) Extracting Data from Encrypted Images

To manage and update personal information of images which are encrypted for protecting clients' privacy, an inferior database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. When the database manager gets the data hiding key, he can decrypt and extract the additional data by directly reading the decrypted version. When requesting for updating information of encrypted images, the database manager, then, updates information through LSB replacement and encrypts up dated information according to the data hiding key all over again. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.

2) Extracting Data From Decrypted Images

In this case, the user wants to decrypt the image first and extracts the data from the decrypted image when it is needed. The following example is an application for such scenario. Assume Alice outsourced her images to a cloud server, and the images are encrypted to protect their contents. Into the encrypted images, the cloud server marks the images by embedding some notation, including the identity of the images' owner, the identity of the cloud server and time stamps, to manage the encrypted images. Note that the cloud server has no right to do any permanent damage to the images. Now an authorized user, Bob who has been shared the encryption key and the data hiding key, downloaded and decrypted the images. Bob hoped to get marked decrypted images, i.e., decrypted images still including the notation, which can be used to trace the source and history of the data. The order of image decryption before/without data extraction is perfectly suitable for this case.

More specifically, the distortion is introduced via two separate ways: the embedding process by modifying the LSB-planes of and self-reversible embedding process by embedding LSB planes of into . The first part distortion is well controlled via exploiting the LSB-planes of only and the second part can benefit from excellent performance of current RDH techniques.

4.4 Data Extraction and Image Restoration

In this module, after generating the marked decrypted image, the content owner can further extract the data and recover original image. Reversible hiding allows extraction of the original host signal and also the embedded message. There are two important requirements for reversible data hiding techniques: the embedding capacity should be large; and distortion should be low. These two requirements conflict with each other. In general, a higher embedding capacity results in a higher degree of distortion. An improved technique embeds the same capacity with lower distortion or vice versa.

The result for PSNR with different plane as follow

Table 1: PSNR Comparison for different LSB planes

		PSNR results (dB)							
embedding rate (bpp)		0.005	0.01	0.05	0.1	0.2	0.3	0.4	0.5
Lena	peak points	67.16	63.44	55.46	52.33	49.07	45.00	40.65	35.84
	proper points	64.53	62.05	55.90	51.64	48.99	44.83	40.54	36.08
Airplane	peak points	65.94	63.18	57.02	54.20	50.98	48.26	44.67	40.78
	proper points	63.89	62.74	57.46	53.98	51.09	48.48	44.91	40.52
Barbara	peak points	65.39	62.56	55.56	51.46	47.68	43.56	39.24	34.80
	proper points	59.62	58.08	53.63	51.04	47.10	43.02	39.24	34.88
Baboon	peak points	57.493	55.71	50.19	46.17	40.68	35.87	31.16	25.92
	proper points	59.61	56.80	50.49	46.26	40.51	35.91	31.07	25.94
Peppers	peak points	63.77	61.30	54.17	51.02	46.00	42.08	36.91	——
	proper points	64.71	62.31	51.20	51.23	46.11	42.20	37.10	——
Boat	peak points	67.22	64.13	56.75	52.62	49.10	45.21	41.24	35.99
	proper points	63.28	60.73	55.53	51.62	49.03	45.29	41.36	35.99

5. Conclusions

RDH for encrypted images is the new topic which is important to pay attention because of demand of privacy preventing from cloud management. Existing system can't unable to do this. The proposed method can achieve excellent property that the data extraction and image recovery are free of any error and take benefits of all traditional RDH techniques.

References

[1] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4,pp. 1097–1102, Apr. 2010. Wagh Mahesh J, Manish Koul, Murtadak Sona U, Shinde Kavita S, Prof. Bhandare M.G, "RDH (Reversible Data Hiding) in Encrypted Images by Reserving Room Before Encryption", Volume 4, Issue 4, April 2014.

[2] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in *Proc. SPIE Proc.* Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–58

[3] Kede Ma, Weiming Zhang, Xianfeng Zhao,"Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL:8 NO:3 YEAR March 2013 .

[4] T. Kalker and F.M.Willems, "Capacity bounds and code constructions for reversible data-hiding," in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71–76.

[5] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896,Aug. 2003.

[6] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.

[7] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats,"in Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.

[8] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Comput., vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.

[9] Miscelaneous Gray Level Images [Online]. Available:http://decsai.ugr.es/cvg/dbimagenes/g512.php