VOL. 13, NO. 3, FEBRUARY 2018 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

A REVIEW OF REVERSIBLE DATA HIDING TECHNIQUE BASED ON STEGANOGRAPHY

K. Upendra Raju and N. Amutha Prabha
School of Electronics Engineering, VIT University, Vellore, India
E-Mail: kupendraraju@gmail.com

ABSTRACT

This paper describes the concept of Reversible Data Hiding (RDH) method is based on steganography. Recently more attention is paid to RDH in encrypted image. Generally when a secured /confidential data is transmitted over an insecure channel, loss in data occurs. To secure the data, encrypt the wrap data and embed is secret data into cover media. Since RDH manages the outstanding secured property, the original picture can be recovered without any loss. In this survey paper, different RDH methods are analyzed. All the existing methods in RDH have some limitations. In Vacating Room after Encryption method, during data extraction or image restoration, some errors occurs and in vacating Room previous to Encryption is easy for the data hider to reversibly embed the data in the encrypted image but highly complex in retrieval of the image. Cryptography is also used to maintain the security. Many researchers find difficulty in attaining the cover image and therefore different methods implemented for this is elaborated in the survey based on the field of steganography, Reversible Data Hiding.

Keywords: cryptography, water marking, steganography, reversible data hiding, reversible data hiding, encrypted domain.

1. INTRODUCTION

With the rise of internet, communication through media has become more and more popular. These days people shifting to digital world, where digital media is the major source of communication. When secret data of persons, organizations and corporate are communicated through network in every moment, which entails a risk of copy or corruption when data is received. In the computer world, it is very important to keep secret information, private information and protect the copyrights of data. Hence there is a need to provide security for safe transmission of data on the chosen communication channel [1].

Data security methods are classified into three major categories. These are cryptography, watermarking and steganography. In cryptography the data is encrypted into unreadable form. So, that it becomes scrambled [3] - [5]. Since cipher text has meaningless form and thus easily stimulates the curiosity of cruel attackers who are willing to recover or destroy data. But it does not encourage the existence of the message [2].

A copyright is protected through watermarking which is defined as a process of inserting information an image [6], [7]. A watermark is hidden data embedded into the original image. The watermark must be imperceptible. The watermarking has to done by creating invulnerability against various types of attacks. Attacks are carried out through both intentional and unintentional processing performed on the image in order to delete the watermark or prevent the identification of it.

Image steganography is the art and science of invisible communication. The word steganography is derived from the Greek word *Steganos*, which is used to covered or hide a secret and a *graphy* means for writing or drawing. Therefore, steganography is, literally, covered writing. The principal aim steganography is to cover the information and used it for secure communication in a completely undetectable manner. Also the process prevents generating suspicion to the transmission of a hidden data [8] - [11]. This transmission process enables change in the structure by eluding identification of human eye. Cover or carriers is used to hide the secret information that is available in the form of Digital images, audio and video files, and other files of computer. Stego image is obtained by embedding a message into cover image.

The secret message is embedded into the cover medium, a convenient algorithm is used by the sender and the same algorithm is used by the receiver to take out the message from the cover. “stego” is a result of embedding the secret in the cover image. The stego file is transmitted to the communication channel as shown in Figure-1. The branch of study dealing with the secret message can be extract from the cover medium is termed as ‘steganalysis’. In steganography cover image is original image in image processing, and the message embedded to the image is called a *stego image* [9].

Three significant aspects viz. Security, Capacity and Robustness are affecting steganography and its utility. Inability of eavesdroppers to discover hidden information is security. Quantum of information that can be hidden in the cover medium is defined as capacity. Robustness is the ability of stego medium to survive an attack by adversary and preventing the hidden information from being destroyed.

For past two decades data hiding has emerged as interesting area of research [12]-[14]. In this method, secret data can be encoded into a cover medium, and subsequently facilitates the user to take out the embedded data from the stego medium for various applications. In many data hiding methods, the data is distorted during the operation and prevent the receiver from retrieving original form of data. In crucial areas of medical diagnosis and law enforcement, it is vital to reverse the marked media back to the original cover media after retrieving the hidden data. In some other areas like remote sensing and experimenting

high-energy particle it is quite essential to recover the original cover media for many scientific researchers. In view of the above difficulties, Reversible Data Hiding (RDH) also called Lossless or Invertible data hiding is proposed to avert continuous distortion and exact recovery of original cover medium [15]-[17].

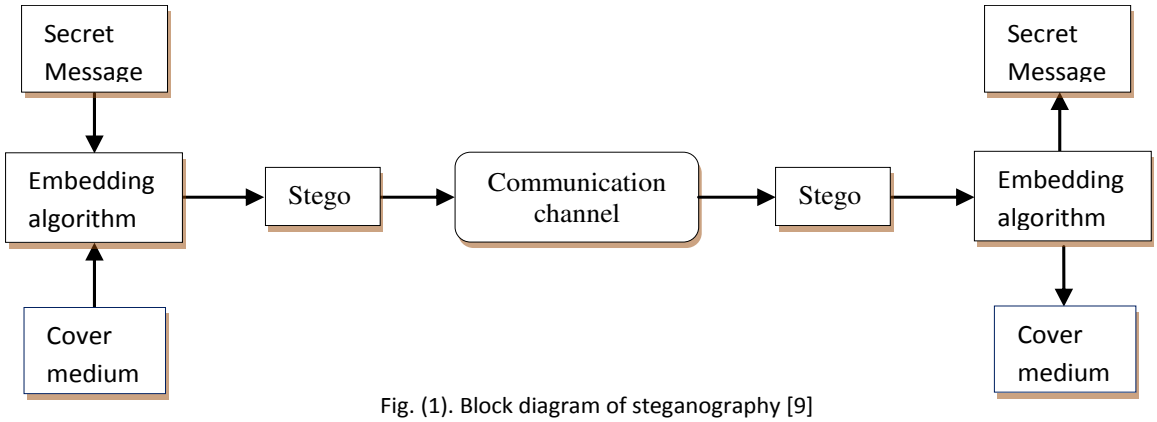

Fig. (1). Block diagram of steganography [9]

This paper is discussed with previous works on RDH in images are surveyed in section - II. In section - III presents different types of RDH methods in images and RDH in Encryption domain. In section – IV concludes the paper.

2. REVERSIBLE DATA HIDING

While filing for the patent from US in 1997 [18], Barton proposed RDH algorithm in embedding authentication information into digital medium and let the authorized user to recover the embedded information. Literature review pronounces the need for growing application of RDH in image authentication processing [18], [19], medical image processing [20], [21]. RDH technique is used to recover embedded message from the original cover without loss [22]. The extensive use of this method is more visible in the areas of medical images, military images and a law forensic, where distortion free of the original cover is allowed.

RDH scheme in the beginning days was majorly developed for the purpose of fragile authentication. RDH method received more attention in their studies entitled Lossless recovery of an original image containing embedded data by Honsinger, *et al.'s* [19]. Honsinger, *et al.'s* method is used to add the secret data with original image to get marked image and then take resulting value modulo 256. The formula for embedding the data is $J = (I + M)$ *mod* 256, where I is the cover image, M is the payload derived from the hash function and J is the marked image. In the receiver side, first reconstruct the payload M from the marked image and then subtract the payload from the marked image to recover the original image without any loss. In data embedding modulo-256 operation prevents the overflow and underflow problem, i.e., a pixel value crossing the upper and lower boundaries and paving the reversibility of data hiding. However, a major disadvantage with this method is that the image is blurred image due to effect of salt-and-pepper noise when the cover image boundary pixel ranges between 255 or 0. The capacity is this method is restricted as fragile authentication does not need much data to be embedded into a cover medium.

Fragile authentication or high capacity RDH schemes were initially based on lossless compression [23] - [31]. RHD schemes are meant to embed data in the saved space after creating some space by lossless compression of a subset S of the cover image. Message and compressed form S_C are placed in place of S for implementing the embedded process. So, the size S - S_C gives the maximum embedding capacity. In [23], space was created for compressing a bit plane of cover image by Fridrich *et al*. A hash value of 128 bit was embedded after determining bit plane at lower level providing enough space for hash value. Goljan *et al*. proposed R-S scheme [24]. The authors divided the cover image into three blocks namely Regular, Singular and Unusable and a discrimination function indicating the smoothness of the blocks is mainly used for the classification of the blocks. RS vector is formed with R block representing 1, S block is by 0 and ignoring U block. After classifying the R and S block according to embedded bit, it is changed or unchanged according to specification of R and S using a flipping function. Overhead information i.e compressed RS-vector and pure payload are included in the actual embedded data.

Integer Wavelet Transform (IWT) formed the basis for high capacity RDH proposed by Xuan *et al* [26]. In IWT method, the main idea is to embed the data into IWT coefficients of high frequency sub bands. Xuan *et al* were very particular about lossless compression of middle bit planes of IWT coefficients with space for data embedding. Study by Xuan *et al* could realize higher capacity in comparison with Goljan *et al* [24]. Generalized Least Significant Bit (G-LSB) compression method aims to advance compression efficiency with the help of unchanged portions of cover data as side information, observed Celik *et al* [30] in their study. Payload bits are improvised after fixing low level raw pixel values through quantization. Research work done by Celik *et al* [30] is proved to be better than previous lossless compression studies [23] and [25] because of precise scalability along

the capacity distortion curve. Rajini *et al* [32] proposed a new technique on image steganography based on Fractional Random Wavelet Transform (FrRnWT) embodies the features of wavelets transform with randomness and fractional order.

Tian [33] and [34] in his empirical study stated that a high capacity RDH method can be developed based on Difference Expansion (DE). In DE method application of Integer Haar Wavelet Transform (IHWT) to the cover image for deriving the difference values is preceded by expansion of values derived to create the reversible data embedding. DE method betters studies [25] and [28] in terms of performance related to lossless compression. It also enhances the Embedded Capacity (EC) by minimizing the distortion. DE can be considered as the first Integer Transformation (IT) based RDH. After wards Alattar [35] came up with an idea of generalizing DE from the stand point of Integer Transform (IT). Alattar had brought out generalizing DE from pixel pair to pixel block of arbitrary size by simplifying Tian's method.

Reversible contrast mapping which is an IT of integer pair has been applied by Coltuc and Chassery [36] in their study. This method is unique from DE in that it does not need additional loss less compression. The issue of computational complexity is also addressed in more effective manner. Weng *et al* [37] have improved DE by deploying two different ITs of pixel pair by considering the magnitude of difference value. The major premise of their study is invariability of the sum of pixel pairs and pair wise difference adjustment. In another study by Weng *et al* [38] embedding rule of DE was reformulated as transformation of integer pair by using a new IT. In the process the researchers [38] also invented new algorithms by extending the transformation.

Histogram Shifting (HS) is identified to be the important approach for RDH as this method generates histogram and change the histogram through reversible data embedding. Ni *et al.* in [39] and [40] were incidentally the first to underline the need for HS-based RDH. In this method the PSNR of stego image and the original attained image is at least 48.13dB. In their study Fallahpour and Sedaaghi [41] decided to apply HS for image blocks in place of the whole image. In this method histogram is created for each divided block after segmenting cover image into blocks. Application of Ni et al's HS method is followed for data embedding. Embedding Capacity can be augmented with decreased distortion in the block based HS [42].

Lee *et al.* [42] were successful in devising a new method by using the histogram of difference image. Difference histogram is much better than ordinary image pixel intensity histogram as it is a Laplacian-like distribution with higher peak point. This method exploited spatial correlation of natural images for improved performance. Xuan *et al.* [43], modified histogram prepared from high-frequency IWT coefficients and developed a novel HS based technique which is better performing than HS [40]. Li *et al* [44] formulated a general construction for designing HS-based RDH with due priority for many previous methods. General framework covers the division of image into non overlapping blocks, with each block consisting of n-pixels. Further n-dimensional histogram is constructed from the frequency of each divided block. At the end, data embedding is completed by altering the resulting n-dimensional histogram.

3. REVERSIBLE DATA HIDING INTO JPEG IMAGES

A Joint Photographic Experts Group (JPEG) offers a good compression rate and the visual quality of compressed image. A digital camera and other photography devices are used in image formats. The JPEG images are cover images for RDH. But RDH can't receive the compressed images. It receives only un-compressed images. RDH technique provides the opportunity to retain the quality of original images where as JPEG compression diminishes the image size and eliminate the high frequency components.

The first type of RDH in JPEG images is based on changes effected in the quantized DCT coefficients. In [45] Fridrich *et al.* developed an idea to compress the LSB plane of the preferred DCT coefficients in a JPEG image in a lossless way for RDH space. In another research model developed by Xuan *et al.* [46] histogram pairs were used in a lossless data hiding scheme for JPEG images. For this purpose histogram of quantized DCT coefficients were segmented into three types. (i) the part convenient for embedding the data; (ii) the unchanged part in which absolute value of coefficients is lesser than the predetermined threshold (T) (iii) the displaced absolute value of coefficients is greater than the threshold. Further improvements were carried out by Sakai *et al* [47] in the form of avoiding data into blocks existing in the noisy parts of the image. This new method can estimate where block size of 8×8 DCT coefficients is placed in smooth part of image by observing the fluctuation of the DC coefficients happening in adjoining blocks. Hence the smooth parts of a JPEG image selected for data embedding. Li *et al.* [48] presented a method for embedding a message bits into the quantized DCT coefficients to specific frequencies so that minimum changes are made in the original JPEG images. In [49], Efimushkina *et al.* adopted embedding messages to some specific coefficients with less magnitude to prevent distortion in the host JPEG images. There has been substantial increase of 44% in average payload compared in this method compared with less average payload at the same image distortion due to un-optimized counterpart.

The RDH scheme is used in the case of un-compressed image. The important criterion for marked JPEG file to evaluate the performance of RDH is the storage size of JPEG file. Modified quantized DCT coefficients in RDH can improve the embedding capacity and visual quality while preserving the storage size of the marked JPEG image. RDH method is more famous due to balanced embedding capacity, image fidelity and storage size of the marked JPEG file.

Quantization tables were changed to lossless embeds one bit DCT coefficients by Fridrich *et al.* [50].

When the quantization factor is even, it is divided by two and the corresponding coefficients are multiplied by two without affecting the visual quality of the image. But this method has two drawbacks. One is the quantization table used to hide the data in the JPEG image is not of standard form. Major disadvantage is the changed quantization coefficients with decrease compressibility in the presence of Huffman coding. As the embedding capacity is limited despite offering fidelity and storage size, this method can only utilized for image authentication where low payload is likely.

4. ROBUST REVERSIBLE DATA HIDING

Processing is taken up to hide the data in an image in several applications. Original image cannot be recovered fully if the processing is not reversible. RDH need the essential property of Robustness to recover the hidden data completely from the processed image.

In [51], [52], Vleeschouwer *et al.* proposed reduction of overflow and under flow problems by using modulo-256 scheme with the help of additions and subtractions based on correlation among surrounding pixels. Modulo-256 addition helps in changing the white pixels into black ones and black ones into white ones leading to the creation of salt-and-pepper noise and also diminishing the image visual quality. Ni *et al.* [53], [54] presented a Robust Reversible Data Hiding (RRDH) scheme to avoid the salt-and-pepper noise. The host image is initially categorized into blocks of size 8×8 by using the Error Correction Coding (ECC) and permutation methods. In order to realize reversibility of the image and robustness if the image is subjected to JPEG compression, the proposed method is quite effective

RDH is widely used in medical and military images. The original image is fully recovered and the hidden data can appropriately extracted provided image and hidden data are not changed. If image and hidden data are subjected to some processing or incidental changes like JPEG compression, the hidden data is recovered correctly even though the original image may be recovered partly. Hence RRDH is useful in reality.

5. REVERSIBLE DATA HIDING WITH CONTRAST ENHANCEMENT

RDH which has developed on original basis for authenticity purpose in the distortion sensitive applications like medicine, satellite and military. An important task of the quality of the host image should be preserved as far as possible regarding the visual quality. The visual quality is measured by MSE and PSNR. The PSNR is the difference between the original image and stego image. The prime intention is when embedding the data operations by image content, the PSNR value diminishes when more distortions are introduced. Generally, A transaction lies between the PSNR and Embedding Capacity (EC), In the process of data hiding can be improved the visual quality with more or less distortions. Improving visual quality along with protecting image quality by avoiding poor illumination is significant. For example, for better visual inspection of medical and satellite images are often desired through contrast enhancement**.** In some cases where PSNR is unsuitable for quality assessment of image. Improved version of RDH is much desirable for improving the host image quality.

Pixel values of histogram are modified by H.T.Hu *et al.* [55]. To obtain the gray-level image, image histogram is calculated with the help of pixel value ranging from 0 to 255 in the host image. f_L and f_R, which denote the non-empty bins in the histogram are selected. Then two bin with highest values in the modified histogram are selected from among updated values enlarged f_L and f_R, Host image is reprocessed to prevent overflow and underflow which commonly occur due to expansion of histogram bins. Wu,*et al* [55] concluded that artificial distortions have to be introduced to the images with strong background. Wu'*et al* [56] in their analysis submitted a new RDH method for medical images. Otsu's method [57] is employed to conduct background segmentation and separate the image into background the Region of Interest (ROI). After this pixel values segregated background more than a pre defined percentage, are located as the major ones. The contrast of ROI can be specifically increased by not considering the histogram bins. Structural SIMilarity (SSIM) was calculated for the quality of the image between the images in the research paper developed by Wang *et al.*[58]. SSIM index is developed for the quality assessment by degrading structural information and take into cognizance the error difference between distorted reference images two images. The established range of SSIM index is 0 to 1, and is assumes a maximum value of 1 if the two images are similar. This index is used ascertain image quality and also PSNR.

6. REVERSIBLE DATA HIDING IN ENCRYPTED DOMAIN

One of the major forms of privacy protection is encryption. Signal processing over encrypted domain is currently witnessing wide spread research activity. Previously both data hiding and encryption got desired attention. Currently existing combination of data hiding and encryption schemes cover only a part of data encrypted and remaining part is made to bear additional research. This was stated by Lian *et al*, Cancellaro *et al* and Schmitz *et al* respectively in their research papers. Lian *et al* [59] used intra-prediction mode to encrypt motion vector difference and signs of DCT coefficients. In the process watermark is embedded into the amplitudes of DCT coefficients. Cancellaro *et al* [60] could successfully encrypt and water marked the higher and lower bit planes of cover data in transform domain. As only partial encryption is involved both the schemes resulting leakage of partial information. In addition to this the water marked version is not considered for the partitioning original cover. Embedded data is irreversible.

RDH methods studied in the above mentioned works are conducive for plaintext domain, where the extra bits are embedded into the original un encrypted multimedia data with more focus on signal processing over encrypted domain. This creates scope for

investigation of embedded additional data in the encrypted domain in a reversible manner. Content owner can encrypted the media data before transmission for securing storing and sharing multimedia file with the receiver. In various applications, a low grade assistant or a channel administrator can add extra message like original information, image rotation or authentication data within the encrypted media though a grade channel assistant or channel administrator do not know the original content. In the administration of medical images when they are to be encrypted for protecting patient privacy, administrator can embed the personal information into corresponding encrypted images. By doing so original content can be recovered accurately after decryption at the receiving. The above process is enabled with the help RDH in Encrypted Domain (RDH-ED). The principal aim of RDH-ED technique is to embed additional information into cipher data without disclosing the plain text content. This is also helpful to the receiver in terms of recovering the plain text without errors.

Reversible Data Hiding in Encryption Domain as in Figure-2 has three blocks in the RDH-ED Content owner, Data-hider, and Receiver. Encryption of original media to the principle content can be done by the content owner with processing and without processing after selecting the encryption key. Data hider takes the help of data hiding key

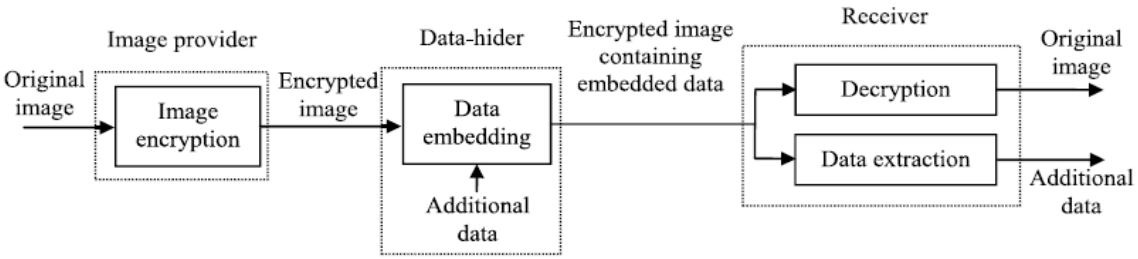

Figure-2. Reversible data hiding in encryption domain [69].

for embedding additional bits into encrypted media for security purpose. Receiver has three options: first option is used to decrypt the marked encrypted media to obtain appropriate media. Second option deals with extracting the additional embedded bits. Then lies the third option generating recovered media with similar identity of the original message.

The RDH-ED technique can be divided into two types:

a) Vacating Room After Encryption (VRAE)
b) Vacating Room Before Encryption (VRBE).

7. VACATING ROOM AFTER ENCRYPTION (VRAE)

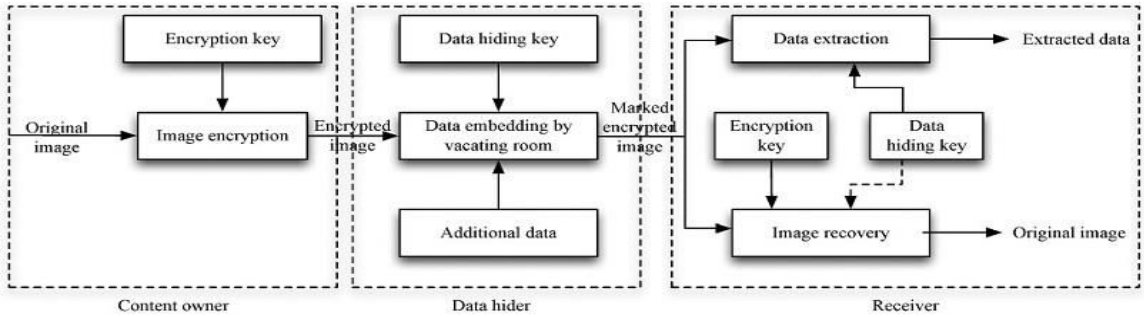

Figure-3. Vacating room after encryption [61].

In V R A E method, original image content is encrypted using a standard cipher with an encryption key. Then encrypted image is submitted to the data hider (Data Base Manager) by the content owner to enable the data base manager embed additional bits of data into the encrypted image by losslessly vacating room in accordance with data hiding key. From the receiver point of view, authorized third party or content owner can retrieved the embedded data and recover original image from encrypted image with the help of data hiding and encryption keys as shown in Figure-3.

In [62] Zhang proposed an innovative method to embed the encrypted image into blocks by changing three LSB bits of the pixels in the blocks and dividing the encrypted images into blocks. From the receiver side the marked encrypted image is decrypted to an approximate image. Image texture of every block is arrived at by the receiver after changing the three LSBs of pixels to form a new block. Original block is supposed to be much smoother than the interfered block due to spatial correlation in natural images. Extraction of embedding bits and original image are simultaneously retrieved. Block size influences the embedding. Minimizing errors during data extraction and image recovery is very much possible by selecting an appropriate block size.

Hong *et al* [63] is in interesting study utilized a side match algorithm for higher embedded pay load in the recovery of the image by creating spatial correlation among the adjacent blocks. The major advantage of this method is reducing error rates. The performance is improved by developing spatial correlation between neighbouring blocks and using a side-match algorithm to accomplish higher embedding payload with lower error rates in the recovery of image. Authors Yu et al [64] and Hong *et al* [65] played a key role in enhancing the performance by improvising flipping ratio and unbalanced bit flipping. Liao *et al* [66], improved precision of data extraction of image recovery is realized by establishing a particular function to estimate image texture of each block. Qin *et al* [67] experimented by flipping only few pixels of LSBs in place of changing LSBs of half pixels in the encrypted image and succeeded in visual quality improvement of the approximate image. A new adaptive judging function which relies on the distribution characteristic of image local contents is used to calculate approximately the image-texture of each block in the process of data extraction and image recovery. By way of this errors in extracted bits are eliminated and image is recovered to larger extent.

Chen *et al* [68] observed that RDH scheme for an encrypted signal is developed by taking digital image as an illustration for description. While encryption the image, each pixel value was divided into two parts. Those two parts are Most Significant Bits (MSBs) numbering seven and one LSB and these parts are encrypted. Based on the principles of homomorphism modification was effected to two encrypted LSBs of each encrypted pixel pair in order to reversibly embed one secret bit. This enables the receiver to retrieve the embedded bits easily and recover the original image which is possible by ascertaining the relationship between two decrypted LSBs in each pixel pair. But, the intrinsic overflow could not be averted. Qian *et al* [69] used LDPC codes into syndrome bits not only to make room to include additional bits but also encode the selected bits drawn from stream - cipher image in VRAE method.

8. VACATING ROOM BEFORE ENCRYPTION (VRBE)

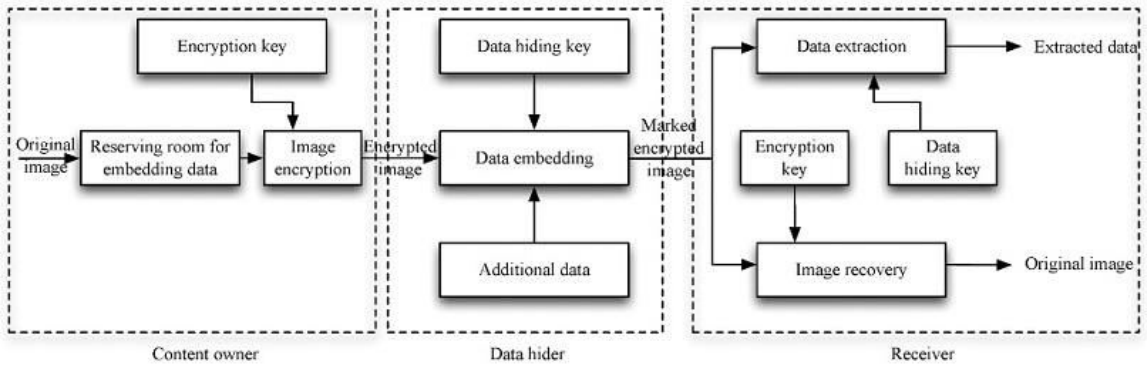

Figure-4. Vacating room before encryption [69].

New RDH technique for encrypted images is futile as lossless vacating room from the encrypted image is not only difficult but also inefficient. Ma *et al* [70], Zhang *et al* [71], Cao *et al* [72] and Shiu *et al* [73] found in their studies that reversing the order of the encryption and vacating room prior to the image encryption at the content owner side, RDH task in encrypted image appears to be more easier and natural making way for a new "vacating room before encryption (VRBE)" framework as shown in Figure-4.

Ma *et al* [70] proved that traditional RDH method can be used to create digital images with the help of embedding LSBs of some pixels into other pixels. Encrypted image is generated by encrypting the pre processing image. Data hider will have an opportunity to use the positions of vacating LSBs in the encrypted image to obtain large payload of 0.5bpp. Zhang *et al* [71] projected a new model based on prediction technique where some pixels are calculated by the remaining pixels before encryption and also predicting some errors is possible. Then prediction errors are encrypted and a standard encryption algorithm is applied to the remaining pixels. Additional data is embedded by moving the encrypted histogram of predicted errors instead of embedding data in the encrypted images directly. In VRBE work cannot support this kind of embedding as it is necessary for the content owner to execute the task of additional pre processing before encrypting the content.

9. CONCLUSIONS

This paper focused on some data hiding methods. The methods in each work have different level of applications. Each method has its own advantages and disadvantages. The current models have little scope for efficient security. It is quite essential to develop effective system for data embedding and data recovery in lossless manner without scope for any distortion. This survey paper addressed on Reversible Data Hiding (RDH) techniques. In the spatial domain of RDH technique, the digital images in JPEG domain are experiencing some lossy compression. They are the RDH methods in the spatial domain. The image quality like MSE and PSNR value are measured by analysing different RDH contrast enhancement methods. Encrypting images in Reversing

data hiding is a new concept by vacating room after encryption and before encryption. The RDH in encrypted domain was excellent security performance without loss of data compared with other security methods. It is expected to increase the security level by using audio and video as the cover media in the future research on RDH.

REFERENCES

[1] J. Fridrich. 2009. Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge, U.K.: Cambridge Univ. Press.

[2] R.H. Chan, F.R. Lin, K.M. Yeung. 2001. A frequency domain based watermarking scheme with spatial repetition coding. Proceedings of the 5th World Multi-conference on Systemic, Cybernetics and Informatics. VI: 35-40, Orlando.

[3] M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg and K. Ramchandran. 2004. On compressing encrypted data. IEEE Trans. Signal Process. 52(10): 2992-3006.

[4] W. Liu, W. Zeng, L. Dong, and Q. Yao. 2010. Efficient compression of encrypted grayscale images. IEEE Trans. Image Process. 19(4): 1097-1102.

[5] X. Zhang, G. Feng, Y. Ren and Z. Qian. 2012. Scalable coding of encrypted images. IEEE Trans. Image Process. 21(6): 3108-3114.

[6] M. Deng, T. Bianchi, A. Piva, and B. Preneel. 2009. An efficient buyer-seller watermarking protocol based on composite signal representation. in Proc. 11th ACM Workshop Multimedia Secur. pp. 9-18.

[7] S. Lian, Z. Liu, Z. Ren, and H. Wang. 2007. Commutative encryption and watermarking in video compression. IEEE Trans. Circuits Syst. Video Technol. 17(6): 774-778.

[8] T. Morkel, J.H.P. Eloff and M.S. Olivier. An Overview of Image Steganography.

[9] N. Provos and P. Honeyman. 2003. Hide and seek: An introduction to steganography. IEEE Security and Privacy. 01(3): 32-44.

[10] R. Chandramouli, M. Kharrazi, N. Memon. 2004. Image Steganography and Steganalysis: Concepts and Practice. International Workshop on Digital Watermarking, Seoul.

[11] R.J. Anderson and F. A. P. Petitcolas. 2001. On the limits of the Stegnography. IEEE Journal Selected Areas in Communications. 16(4): 474-481.

[12] J. Fridrich and M. Goljan. 2002. Lossless data embedding for all image formats. in Proc. SPIE Proc. Photonics West, Electronic Imaging, Securityand Watermarking of Multimedia Contents, San Jose, CA, USA. 4675: 572-583.

[13] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker. 2007. Digital Water-marking and Steganography. San Mateo, CA, USA: Morgan Kaufmann.

[14] J. Fridrich. 2009. Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge, U.K.: Cambridge Univ. Press.

[15] Y. Q. Shi, Z. Ni, D. Zou, C. Liang, and G. Xuan. 2004. Lossless data hiding: Fundamentals, algorithms and applications. In: Proc. IEEE Int. Symp. Circuits Syst. 2: 33-36.

[16] Y. Q. Shi. 2004. Reversible data hiding. in Proc. Int. Workshop Digit. Watermarking. pp. 1-12.

[17] R. Caldelli, F. Filippini, and R. Becarelli. 2010. Reversible watermarking methods: An overview and a classification. EURASIP J. Inf. Secur. 2010(134546).

[18] J. M. Barton. 1997. Method and apparatus for embedding authentication information within digital data. U.S. Patent 5 646 997.

[19] C. W. Honsinger, P. W. Jones, M. Rabbani, and J. C. Stoffel. 2001. Lossless recovery of an original image containing embedded data. U.S. Patent 6 278 791.

[20] F. Bao, R.-H. Deng, B.-C. Ooi, and Y. Yang. 2005. Tailored reversible watermarking schemes for authentication of electronic clinical atlas. IEEE Trans. Inf. Technol. Biomed. 9(4): 554-563.

[21] G. Coatrieux, C. Le Guillou, J.-M. Cauvin and C. Roux. 2009. Reversible watermarking for knowledge digest embedding and reliability control in medical images. IEEE Trans. Inf. Technol. Biomed. 13(2): 158-165.

[22] J. Fridrich, M. Goljan, and R. Du. 2002. Lossless data embedding for all image formats. Proc. SPIE, Secur. Watermarking Multimedia Contents. 4675: 572-583.

[23] J. Fridrich, M. Goljan and R. Du. 2001. Invertible authentication. Proc. SPIE. 4314: 197-208.

[24] M. Goljan, J. J. Fridrich, and R. Du. 2001. Distortion-free data embedding for images. In: Proc. 4th Inf. Hiding Workshop. pp. 27-41.

[25] J. Fridrich, M. Goljan, and R. Du. 2002. Lossless data embedding-New paradigm in digital watermarking. EURASIP J. Adv. Signal Process. 2002(2): 185-196.

[26] G. Xuan, J. Zhu, J. Chen, Y. Q. Shi, Z. Ni and W. Su. 2002. Distortionless data hiding based on integer wavelet transform. Electron. Lett. 38(25): 1646-1648.

[27] G. Xuan, J. Chen, J. Zhu, Y. Q. Shi, Z. Ni and W. Su. 2002. Lossless data hiding based on integer wavelet transform. In: Proc. IEEE Int. Workshop Multimedia Signal Process. pp. 312-315.

[28] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Reversible data hiding. In: Proc. IEEE Int. Conf. Inf. Process., vol. 2. September 2002, pp. 157 - 160.

[29] G. Xuan *et al*. 2004. High capacity lossless data hiding based on integer wavelet transform. in Proc. IEEE Int. Symp. Circuits Syst. 2: 29-32.

[30] M. U. Celik, G. Sharma, A. M. Tekalp and E. Saber. 2005. Lossless generalized-LSB data embedding. IEEE Trans. Image Process. 14(2): 253-266.

[31] M. U. Celik, G. Sharma, and A. M. Tekalp. 2006. Lossless watermarking for image authentication: A new framework and an implementation. IEEE Trans. Image Process. 15(4): 1042-1049.

[32] G.K. Rajini, G. Ramachandra Reddy. 2015. A fractional Random Wavelet Transform Based Image Steganography. Research Journal of Applied Science, Engineering and Technology. pp. 943-951.

[33] J. Tian. 2002. Wavelet-based reversible watermarking for authentication", Proc. SPIE, vol. 4675, page no. 679 - 690, April.

[34] J. Tian. 2003. Reversible data embedding using a difference expansion. IEEE Trans. Circuits Syst. Video Technol. 13(8): 890-896.

[35] A. M. Alattar. 2004. Reversible watermark using the difference expansion of a generalized integer transform. IEEE Trans. Image Process. 13(8): 1147-1156.

[36] D. Coltuc and J. M.Chassery. 2007. Very fast watermarking by reversible contrast mapping. IEEE Signal Process. Lett. 14(4): 255-258.

[37] S. Weng, Y. Zhao, J.-S. Pan and R. Ni. 2008. Reversible watermarking based on invariability and adjustment on pixel pairs. IEEE Signal Process. Lett. 15: 721-724.

[38] C. Wang, X. Li, and B.Yang. 2010. High capacity reversible image watermarking based on integer transform. In: Proc. IEEE Int. Conf. Inf. Process. pp. 217-220.

[39] Z. Ni, Y.-Q. Shi, N. Ansari and W. Su. 2003. Reversible data hiding. in Proc.IEEE Int. Symp. Circuits Syst. pp. 912-915.

[40] Z. Ni, Y.-Q. Shi, N. Ansari and W. Su. 2006. Reversible data hiding. IEEE Trans. Circuits Syst. Video Technol. 16(3): 354-362.

[41] M. Fallahpour and M. H. Sedaaghi. 2007. High capacity lossless data hiding based on histogram modification. IEICE Electron. Exp. 4(7): 205-210.

[42] S.-K. Lee, Y.-H. Suh and Y.-S. Ho. 2006. Reversiblee image authentication based on watermarking. in Proc. IEEE Int. Conf. Multimedia Expo. pp. 1321-1324.

[43] G. Xuan, Y. Q. Shi, P. Chai, X. Cui, Z. Ni and X. Tong. 2007. Optimum histogram pair based image lossless data embedding. In: Proc. Int. Workshop Digit. Watermarking. pp 264-278.

[44] X. Li, B. Li, B. Yang and T. Zeng. 2013. General framework to histogram shifting- based reversible data hiding. IEEE Trans. Image Process. 22(6): 2181-2191.

[45] J. Fridrich, M. Goljan and R. Du. 2001. Invertible authentication watermark for JPEG images. in Proc. Int. Conf. Inf. Technol., Coding Comput. pp. 223-227.

[46] G. Xuan, Y. Q. Shi, Z. Ni, P. Chai, X. Cui and X. Tong. 2007. Reversible data hiding for JPEG images based on histogram Pairs. in Proc. Int. Conf. Image Anal. Recognit. pp. 715-727.

[47] H. Sakai, M. Kuribayashi and M. Morii. 2008. Adaptive reversible data hiding for JPEG images. in Proc. IEEE Int. Symp. Inf. Theory Appl. pp. 1-6.

[48] Q. Li, Y. Wu and F. Bao. 2010. A reversible data hiding scheme for JPEG images. in Proc. Paci_c-Rim Conf. Multimedia. pp. 653-664.

[49] T. Efimushkina, K. Egiazarian and M. Gabbouj. 2013. Rate-distortion based reversible watermarking for JPEG images with quality factors selection. in Proc. Eur. Workshop Vis. Inf. Process. pp. 94-99.

[50] J. Fridrich, M. Goljan and R. Du. 2002. Lossless data embedding for all image formats. Proc. SPIE. 4675: 572-583.

[51] C. De Vleeschouwer, J. F. Delaigle and B. Macq. 2001. Circular interpretation of histogram for reversible watermarking. in Proc. IEEE Workshop Multimedia Signal Process. pp. 345-350.

[52] C. De Vleeschouwer, J.-F. Delaigle and B. Macq. 2003. Circular interpretation of bijective transformations in lossless watermarking for media asset management. IEEE Trans. Multimedia. 5(1): 97-105.

[53] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Q. Sun and X. Lin. 2004. Robust lossless image data hiding. in Proc. IEEE Int. Conf. Multimedia Expo. pp. 2199-2202.

[54] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Q. Sun and X. Lin. 2008. Robust lossless image data hiding designed for semi-fragile image authentication. IEEE Trans. Circuits Syst. Video Technol. 18(4): 497-509.

[55] H.-T. Wu, J.-L. Dugelay and Y.-Q. Shi. 2015. Reversible image data hiding with contrast enhancement. IEEE Signal Process. Lett. 22(1): 81-85.

[56] H.-T. Wu, J. Huang and Y.-Q. Shi. 2015. A reversible data hiding method with contrast enhancement for medical images. J. Vis. Commun. Image Represent. 31: 146-153.

[57] N. Otsu. 1979. A threshold selection method from gray-level histograms. IEEE Trans. Syst., Man, Cybern. 9(1): 62-66.

[58] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli. 2004. Image quality assessment: From error visibility to structural similarity. IEEE Trans. Image Process. 13(4): 600-612.

[59] S. Lian, Z. Liu, Z. Ren and H. Wang. 2007. Commutative encryption and watermarking in video compression IEEE Trans. Circuits Syst. Video Technol. 17(6): 774-778.

[60] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. De Natale, and A. Neri. 2011. A commutative digital image watermarking and encryption method in the tree structured Haar transform domain. Signal Process, Image Commun. 26(1): 1-12.

[61] R. Schmitz, S. Li, C. Grecos, and X. Zhang. 2012. A new approach to commutative watermarking-encryption. in Proc. 13th Joint IFIP TC6/TC11Conf. Commun. Multimedia Secur. pp. 117-130.

[62] X. Zhang. 2011. Reversible data hiding in encrypted image. IEEE Signal Process. Lett. 18(4): 255-258.

[63] W. Hong, T.-S. Chen and H.-Y.Wu. 2012. An improved reversible data hiding in encrypted images using side match. IEEE Signal Process. Lett. 19(4): 199-202.

[64] J. Yu, G. Zhu, X. Li and J. Yang. 2012. An improved algorithm for reversible data hiding in encrypted image. in Proc. Int. Workshop Digit.-Forensics Watermarking. pp. 384-394.

[65] W. Hong, T.-S. Chen, J. Chen, Y.-H. Kao, H.-Y. Wu and M.-C. Wu. 2013. Reversible data embedment for encrypted cartoon images using unbalanced bit flipping. In: Proc. 4th Int. Conf. Swarm Intell. pp. 208-214.

[66] X. Liao and C. Shu. 2015. Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels. J. Vis. Commun. Image Represent. 28: 21-27.

[67] C. Qin and X. Zhang. 2015. Effective reversible data hiding in encrypted image with privacy protection for image content", J. Vis. Commun. Image Represent., vol. 31, page no. 154-164, August.

[68] Y.-C. Chen, C.-W. Shiu and G. Horng. 2014. Encrypted signal-based reversible data hiding with public key cryptosystem. J. Vis. Commun. Image Represent. 25(5): 1164-1170.

[69] Z.Qian and X.Zhang. 2016. Reversible Data Hiding in encrypted images with distributed source encoding. IEEE Trans. Circuits Syst. Video Technol. 26(4): 636-646.

[70] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li. 2013. Reversible data hiding in encrypted images by

reserving room before encryption. IEEE Trans. Inf. Forensics Security. 8(3): 553-562.

[71] W. Zhang, K. Ma and N. Yu. 2014. Reversibility improved data hiding in encrypted images. Signal Process. 94(1): 118-127.

[72] X. Cao, L. Du, X. Wei, D. Meng and X. Guo. 2016. High capacity reversible data hiding in encrypted images by patch-level sparse representation. IEEE Trans. Cybern. 46(5): 1132-1143.

[73] C.-W. Shiu, Y.-C. Chen and W. Hong. 2015. Encrypted image-based reversible data hiding with public key cryptography from difference expansion. Signal Process, Image Commun. 39: 226-233.