International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Reversible Data Hiding In Encrypted Images by Reserving Room before Encryption

Veena N Bhat[1], Navin Y[2]
[1]M.E VLSI Design, JCT college of engineering and technology, Pichanur , Coimbatore , Tamil Nadu, India[1].
[2]Assistant Professor, Department of E C E, JCT college of engineering and technology, Pichanur, Coimbatore,Tamil Nadu, India[2]

Abstract: Reversible data hiding (RDH) in images is a technique, by which the original cover can be lossless recovered after the embedded message is extracted. This important technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed. Recently, more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be lossless recovered after embedded data is extracted while protecting the image content's confidentiality. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. In this paper, we propose a novel method by reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. Experiments show that this novel method can embed more than 10 times as large payloads for the same image quality as the previous methods.
Keywords: reversible data hiding, image encryption, privacy protection.

I. INTRODUCTION

In recent years, the amount of digital images has increased rapidly hence the protection of multimedia data is becoming very important for many applications, e.g., confidential transmission, video surveillance, military and medical applications. Nowadays, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over networks. To decrease the transmission time, the data compression is necessary. The protection of this multimedia data can be done with encryption or data hiding algorithms.

Since few years, a new problem is trying to combine in a single step, compression, encryption and data hiding. So far, few solutions have been proposed to combine image encryption and compression. Two main groups of technologies have been developed for this purpose. The first one is based on content protection through encryption. There are several methods to encrypt binary images or gray level images. In this group, proper decryption of data requires a key. The second group bases the protection on digital watermarking or data hiding, aimed at secretly embedding a message into the data. These two technologies can be used complementary and mutually commutative. In this approach the digital signature of the original image is added to the encoded version of the original image. The encoding of the image is done using an appropriate error control code.

Nowadays, a new challenge consists to embed data in encrypted images. Previous work proposed to embed data in an encrypted image by using an irreversible approach of data hiding. The challenge was to find an encryption method robust to noise. Since the entropy of encrypted image is maximal, the embedding step, considered like noise, is not possible by using standard data hiding algorithms. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. Recent reversible data hiding methods have been proposed with high capacity but these methods are not applicable on encrypted images. In this paper proposes a method for the data hiding in encrypted images and in order to remove the embedded data during the decryption step and also decode the cover image.

In this framework "vacating room after encryption (VRAE)", 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 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 encrypted version according to the encryption key.

Since lossless vacating room from the encrypted images is relatively difficult and sometimes. By reverses 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)". The content owner first reserves enough space on original image and then convert 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.

The proposed method in this project is a framework same as the reserving room before encryption. In the previous method the data embedded can be available without any error after the decryption of the encoded data. But the cover that is the image which containing the data cannot be effectively rebuild. That is the major drawback of the frame woke mentioned previously. To overcome this, in this project the reversible data hiding scheme is replaced by rationale rhombus method. It is the best technique to use in RDH. The algorithm used for rational rhombus method is simple and it provide cover image without any loss.

II. REVERSIBLE DATA HIDING

Reversible or lossless data hiding techniques hide data in a host signal (for example, an image) and allow 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.

Tian's difference expansion technique previously had the highest embedding capacity and the lowest distortion in image quality. His method divides the image into pairs of pixels and uses each legitimate pair for hiding one bit of information. Therefore, his embedding capacity is at best 0.5 b/pixel. The combined use of the rhombus prediction scheme, sorting, histogram shift method, and, as result, small size of location map produces relatively superior results compared to existing schemes.

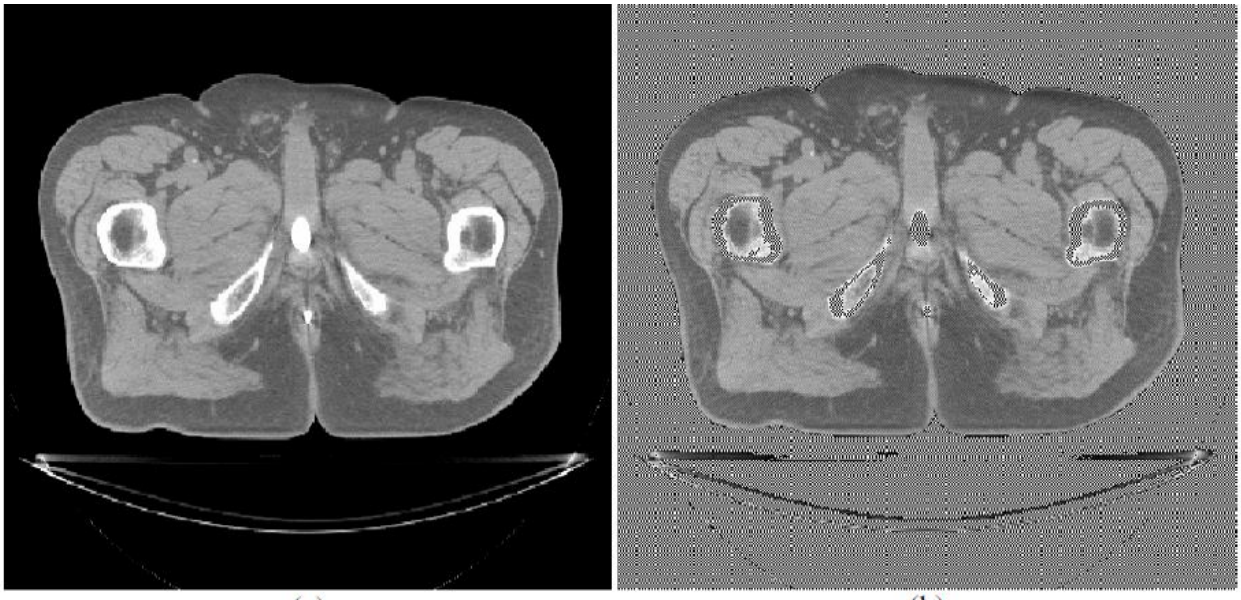
Data hiding, often referred to as digital watermarking, has recently been proposed as a promising technique for information assurance. Owing to data hiding, however, some permanent distortion may occur and hence the original cover medium may not be able to be reversed exactly even after the hidden data have been extracted out. Following the classification of data compression algorithms, this type of data hiding algorithms can be referred to as lossy data hiding. It can be shown that most of the data hiding algorithms reported in the literature are lossy. Here, let us examine three major classes of data hiding algorithm. With the most popularly utilized spread-spectrum watermarking techniques, either in DCT domain or block 8x8 DCT domains, round off error and/or truncation error may take place during data embedding. As a result, there is no way to reverse the stego media back to the original without distortion. For the least significant bit-plane (LSB) embedding methods, the bits in the LSB are substituted by the data to be embedded and the bit-replacement is not memorized. Consequently, the LSB method is not reversible. With the third group of frequently used watermarking techniques, called quantization index modulation (QIM), quantization error renders lossy data hiding.

In applications, such as in law enforcement, medical image systems, it is desired to be able to reverse the stego-media back to the original cover media for legal consideration. In remote sensing and military imaging, high accuracy is required. In some scientific research, experimental data are expensive to be achieved. Under these circumstances, the reversibility of the original media is desired. The data hiding schemes satisfying this requirement can be referred to as lossless. The terms of reversible, or invertible also used frequently. These techniques, like their lossy counterparts, insert information bits by modifying the host signal, thus induce an embedding distortion. Nevertheless, they also enable the removal of such distortions and the exact- lossless- restoration of the original host signal after extraction of embedded information.

One major element of this algorithm is that that it is based on the patchwork theory. That is, within each zone, the mass centre vector's orientation is determined by all the pixels within this zone. Consequently, the algorithm is robust to image compression to certain extent. Another major element of this algorithm lies in that it uses modulo-256 addition to avoid overflow and underflow, thus achieving reversibility. Consequently, however, as pointed out, this algorithm will suffer from the salt-and-pepper noise. In the stego-medical image, the severe salt-and-pepper noise is clear. The PSNR of stego image versus the original image is below 10 dB when 476 information bits are embedded into this 512x512 image. Not only for medical image, the salt-and-pepper noise may be severe for colour images as well. We have applied this algorithm to eight JPEG2000 test colour images. There are four among the eight images that suffer from severe salt-and-pepper noise, while the other four some less severe salt-and-pepper noise. The PSNR

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

can be as low as less than 20 dB when severe noise exists when 1412 information bits are embedded into a colour image of 1536x1920x24. From the above investigation, it can be concluded that all reversible data hiding algorithms based on modulo-256 addition to avoid overflow and underflow, say, in and cannot be applied to many real applications, and hence should be avoided.



(a) (b)

Fig 1. Original medical image and Stego-image with severe salt-and-pepper noise

A. Reversible Data Hiding: Principles, Techniques

Data hiding are a group of techniques used to put a secure data in a host media (like images) with small deterioration in host and the means to extract the secure data afterwards. For example, steganography can be named. Steganography is one such pro-security innovation in which secret data is embedded in a cover. But, this paper will get into reversible data hiding. Reversible data-hidings insert information bits by modifying the host signal, but enable the exact (lossless) restoration of the original host signal after extracting the embedded information. Sometimes, expressions like distortion-free, invertible, lossless or erasable watermarking are used as synonyms for reversible watermarking. In applications, such as in law enforcement, medical image systems, it is desired to be able to reverse the stego-media back to the original cover media for legal consideration.

Lossless data embedding techniques may be classified into one of the following two categories: Type I algorithms employ additive spread spectrum techniques, where a spread spectrum signal corresponding to the information payload is superimposed on the host in the embedding phase. At the decoder, detection of the embedded information is followed by a restoration step where watermark signal is removed, i.e. subtracted, to restore the original host signal. Potential problems associated with the limited range of values in the digital representation of the host signal, e.g. overflows and underflows during addition and subtraction, are prevented by adopting modulo arithmetic. Payload extraction in Type-I algorithms is robust. On the other hand, modulo arithmetic may cause disturbing salt-and-pepper artefacts. In Type II algorithms, information bits are embedded by modifying, e.g. overwriting, selected features (portions) of the host signal -for instance least significant bits or high frequency wavelet coefficients-. Since the embedding function is inherently irreversible, recovery of the original host is achieved by compressing the original features and transmitting the compressed bit-stream as a part of the embedded payload. At the decoder, the embedded payload- including the compressed bit-stream- is extracted, and original host signal is restored by replacing the modified features with the decompressed original features. In general, Type II algorithms do not cause salt-and-pepper artifacts and can facilitate higher embedding capacities, albeit at the loss of the robustness of the first group.

Similarly, the sequence “111111” becomes “110111” if bit 0 is inserted, and becomes “110011” if bit 1 is inserted. However, the papers do not describe clearly how to identify the modified pixels in the extraction process. The image boundaries may change with the watermark insertion. Moreover, let us suppose that a sequence “001000” (located near to an image boundary) was found in the stego image. The papers do not describe how to discriminate between an unmarked “001000” sequence and an originally “000000”

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

sequence that became “001000” with the insertion of the hidden bit 0.

III. REVERSIBLE DATA HIDING TECHNIQUE BY RESERVING ROOM BEFORE ENCRYPTION

The proposed method in this project is a framework same as the reserving room before encryption. In the previous method the data embedded can be available without any error after the decryption of the encoded data. But the cover that is the image which containing the data cannot be effectively rebuild. That is the major drawback of the frame woke mentioned previously. It is illustrated in below Fig 2.

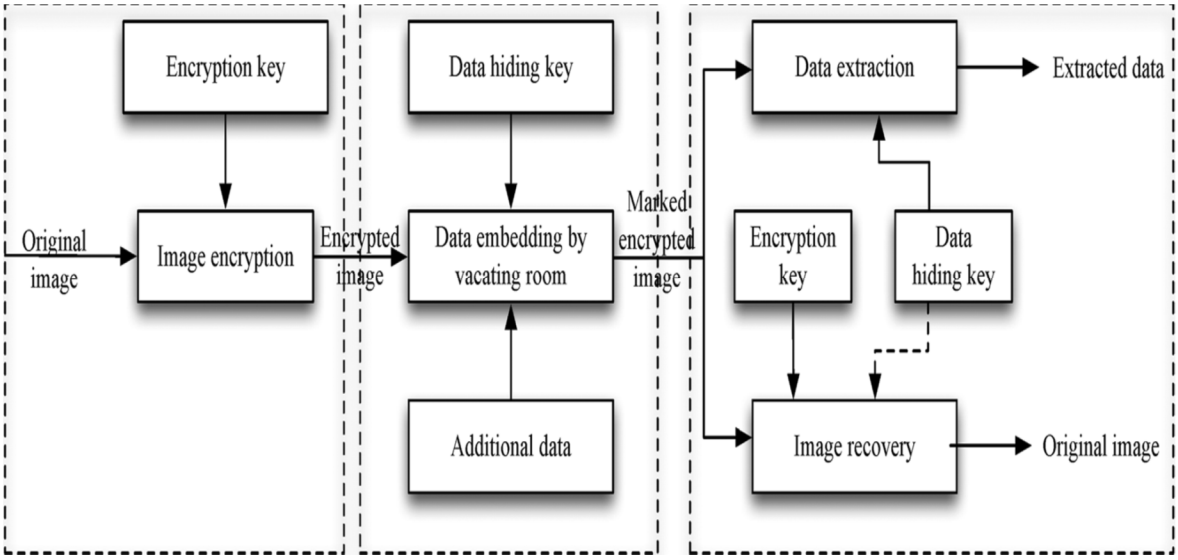


Fig 2. Vacating room after encryption

To overcome this, in this project the reversible data hiding scheme is replaced by rationale rhombus method. It is the best technique to use in RDH. The algorithm used for rational rhombus method is simple and it provide cover image without any loss. The block diagram of the proposer framework in this project is shown in the Fig 3.

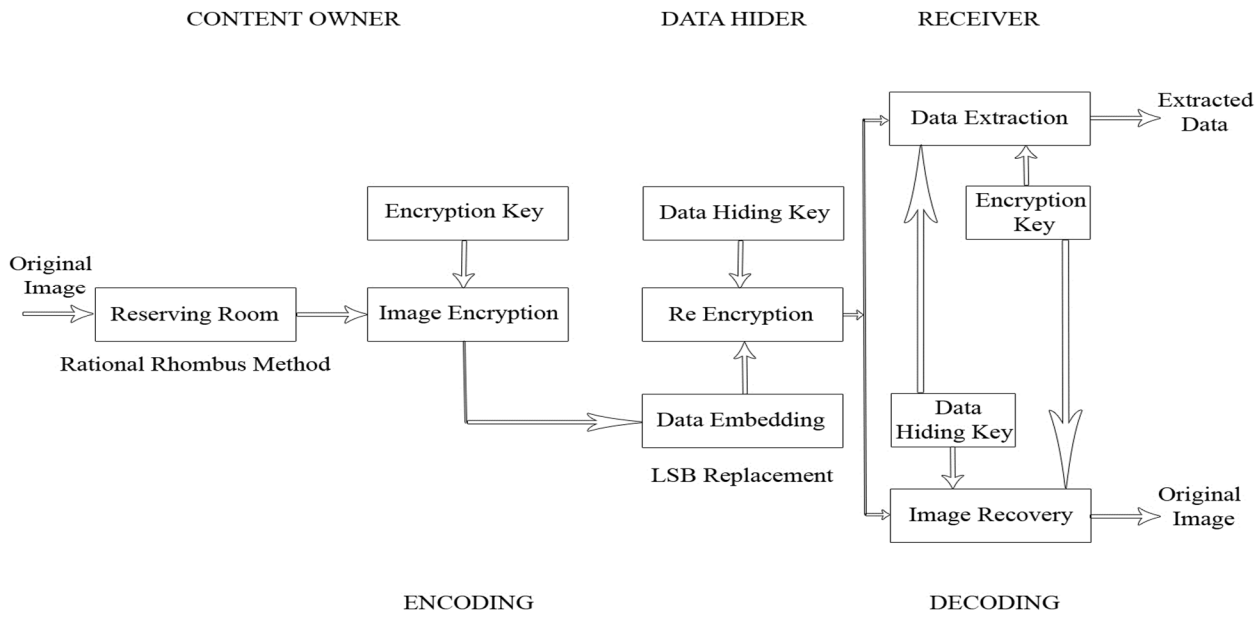


Fig 3 Modified block diagram

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Elaborate a practical method based on this Framework, which primarily consists of four stages: generation of encrypted image, data hiding in encrypted image, data extraction and image recovery. The reserving operation adopt in the proposed method is the modification made in this project. Rationale rhombus method is used to establish the RDH approach. For the secret data hiding the simple method LSB replacement is used.

A. Generation Of Encrypted Image

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 A and B; then, the LSBs of A are reversibly embedded into B using rationale rhombus algorithm so that LSBs of A can be used for accommodating messages.

B. Image Partition

The operator here for reserving room before encryption is a standard RDH technique, so the goal of image partition is to construct a smoother area B, on which rationale rhombus algorithms can achieve better performance. To do that, without loss of generality, assume the original image C is a gray-scale image with its size M x N, it is divided in to two equal sized images. In this the B part has the smoother area to apply the RDH technique. The LSBs of the pixels of A where the data is hiding is stored.

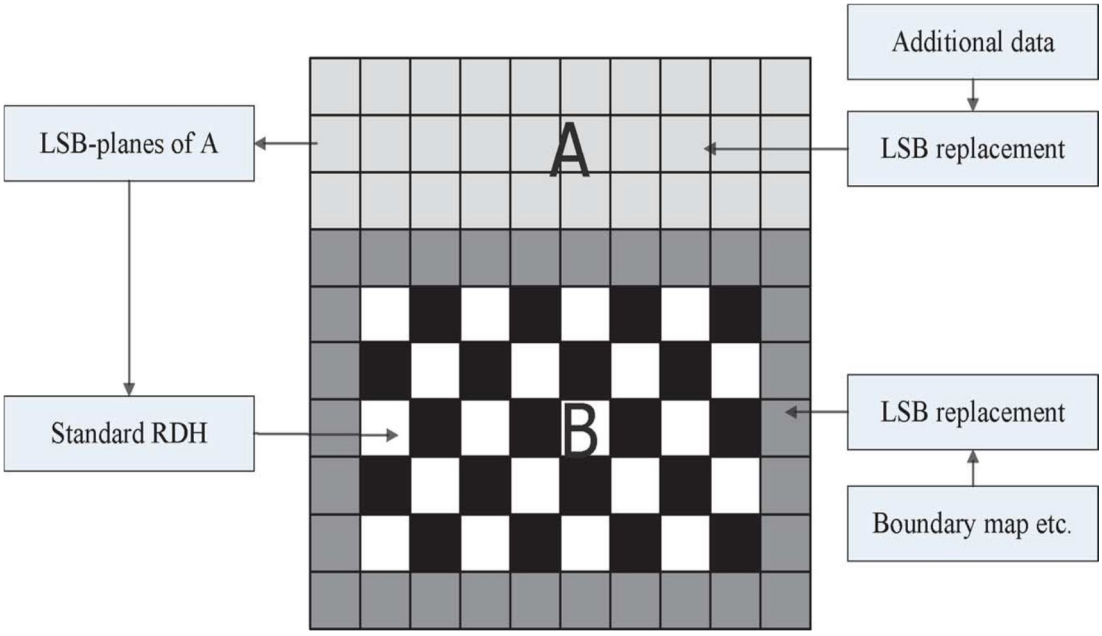


Fig 4 Image partition and embedding process

C. Self-Reversible Embedding

The goal of self-reversible embedding is to embed the LSB-planes of A into B by employing rationale rhombus algorithm.

D. Image Encryption

After rearranged self-embedded image and reserving rooms the encryption is done with the help of encryption key .It is an 8 bit key. In this the encryption is done by XORing the image with the key. Finally, we embed 10 bits information into LSBs of first 10 pixels in encrypted version of A to tell data hider the number of rows and the number of bit-planes he can embed information into. After image encryption, the data hider or a third party cannot access the content of original image without the encryption key, thus privacy of the content owner being protected.

E. Data Hiding In Encrypted Image

Once the data hider acquires the encrypted image, he can embed some data into it, although he does not get access to the original image. The embedding process starts with locating pixels in which the data can embed in the encrypted version of image. Since the

data hider has the locations where the data can be embedded it is effortless for the data hider to read bits information in LSBs of encrypted pixels. After knowing how many bit-planes and rows of pixels he can modify, the data hider simply adopts LSB replacement to substitute the available bit-planes with additional data. Finally, the data hider encrypts according to the data hiding key to formulate encrypted image containing data.

F. Data Extraction and Image Recovery

Since data extraction is completely independent from image decryption, the order of them implies two different practical applications. 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. The order of data extraction before image decryption guarantees the feasibility of our work in this case. When the database manager gets the data hiding key, he can decrypt the LSB-planes of A 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 updated 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.

IV. ALGORITHMS

A. Rationale Rhombus Algorithm

Rationale rhombus method used to store the LSB values of the pixel of the A portion of the image. Rationale rhombus method is implemented here to effectively hide and make is available in the decoding time. In an image the adjacent pixels have the pixel value in less difference. So while considering a rhombus in the pixels the pixel cantered by the four pixels has the average value of the four pixels. This technique is used to develop the rationale rhombus algorithm. These pixels are classified as Cross and Dot. Dots are the four pixels used to find the average value and its value is not changed in this method. Cross is the pixel where the data is hiding and is modified with the following algorithm. Henceforth, this scheme will be called the Cross embedding scheme.

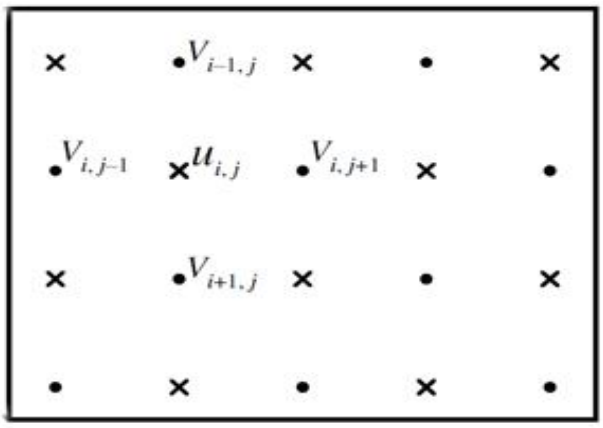


Fig 5 Prediction pattern

In order to predict the pixel value of position ui, j in Fig.4.1, four neighbouring pixels "Dots" are used.

vi, j−1, vi+1, j, vi, j+1, and vi−1, j.

Ui,j is used as the Cross to store the data. The five pixels including ui, j comprises a cell which is used to hide one bit of data.

The encoder of the Cross embedding scheme for a single cell is as follows.

Center pixel ui, j of the cell can be predicted from the four neighbouring pixels

vi, j−1, vi+1, j, vi, j+1, and vi−1, j.

The predicted value u'i, j is computed as follows:

$$u'_{i,j} = [v_{i,j-1} + v_{i+1,j} + v_{i,j+1} + v_{i-1,j} / 4]$$

Based on the predicted value u'i, j and original value ui, j, the prediction error "E" is computed as

$$E = u_{i,j} - u'_{i,j}$$

$$M = 2E$$

This prediction error can be expanded to hide information as

$$H = M + bit$$

Where H is the prediction error after expansion called modified prediction error. The bit is the hiding data.
After data hiding, the original pixel value ui, j is changed to Ui, j as

$$Ui, j = H + u'i, j$$

The decoding procedure for the Cross embedding scheme for a single cell is an inverse of the encoding scheme. During data hiding, pixels from the Dot set are not modified, so the predicted values u'i, j is also not changed. Using the predicted value u'i, j and the modified pixel value Ui, j, and the decoder can exactly recover the embedded bit and original pixel value.

The modified prediction error is computed as

$$H = Ui, j – u'i, j$$

The embedded bit value is computed as

$$bit = H \bmod 2$$

The original prediction error is computed as

$$M = H – bit$$
$$E = M / 2$$

The original pixel's value is computed as

$$ui, j = u'i, j + E$$

Note that the two sets (the Cross set and Dot set) are independent of each other. Independence means changes in one set do not affect the other set, and vice versa. Pixels from the Dot set are used for computing predicted values u'i, j, whereas pixels from the Cross set ui, j are used for embedding data. The order of hiding data in cells is not important and can be changed. Sorting reorders cells according to the magnitudes of local variance and enables hiding data in cells with small prediction errors. Thus, sorting can significantly improve the data embedding scheme.

B. LSB Replacement Algorithm

In this algorithm embed the each bit of the data in the least significant bits places of the original image. The embedding of the data is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with embedding bits. The extraction of the data is performed by extracting the least significant bit of each of the selected image pixels. If the extracted bits match the inserted bits, then the stored is detected. The extracted bits do not have to exactly match with the inserted bits. A correlation measure of both bit vectors can be calculated. If the correlation of extracted bits and inserted bits is above a certain threshold, then the extraction algorithm can decide that the data is detected.

IV.CONCLUSION

Reversible data hiding (RDH) in encrypted images is a topic drawing attention because of the privacy-preserving requirements from cloud data management. Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to proposed method which is by reserving room before encryption. Thus the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effortless. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. Furthermore, this novel method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images.

REFERENCES

[1] Kede Ma, Wei. Zhang, Xianfeng Zhao, "Adaptive Fingerprint Image Enhancement with emphasis on preprocessing of Data" IEEE trans. On information forensics and security, vol,8 No.3 , march 2013.
[2] D.M. Thodi and J. J. Rodriguez, "Reversible Watermarking Algorithm" IEEE Trans.Image Process., vol. 16,no. 3, pp. 721–730, Mar. 2007.
[3] J. Tian, "Watermarking using simple LSB Technique" Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890, Dec. 2009.
[4] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding" Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354, April 2012.
[5] X. L. Li, B. Yang, and T. Y. Zeng, "Reversible Data Hiding: Principles, Techniques" IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, December.2013.

[6] W. Hong, T. Chen, and H.Wu, "Image Processing using smooth ordering of its patches " IEEE Image process. Lett.,vol. 19, no. 4, pp. 199–202, Apr. 2014.
[7] J. Fridrich, M. Goljan, and D. Rui, "Comparison Between Two Watermarking Algorithms Using Dct Coefficient, And Lsb Replacement " IEEE Trans. Consum. Electron., Vol. 3971, pp. 197, Feb. 2013.
[8] W. Hong, T. Chen, and H.Wu, "Reversible Image Watermarking using Interpolation" IEEE Image process. Lett.,vol. 19, no. 4, pp. 199–202, Apr. 2012.
[9] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers" vol. 21, no. 6, pp. 2991–3003, June. 2012