ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Next Generation Method for Reversible Data Hiding

R.Narmatha[1], Mr.S.R.Sivakumar[2]

II Year M.E, Dept. of CSE, SRS College of Engineering and Technology, Salem, India[1]

Assistant Professor, Dept. of CSE, SRS College of Engineering and Technology, Salem, India[2]

ABSTRACT: Nowadays huge 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. Recent Methods such as reserving room before encryption with a traditional RDH algorithm sometimes results in error and complicated usage at the time of data extraction and/or image restoration .Hence to overcome this problem, this project propose an efficient method which uses by combining cryptographic primitives based encryption with Histogram Shifting-based RDH algorithm, a high capacity and low distortion can be achieved efficiently, and thus it is easy for the data hider to reversibly embed data in the encrypted image.

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 using the same cryptographic primitives and extract the additional data by directly reading the decrypted version.. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content. The proposed method can achieve real multi level reversibility, that is, data extraction and image recovery are free of any error. Experiments show that this method can embed more than 10 times as large payloads for the same image quality.

Index Terms—Reversible data hiding, image encryption, privacy Protection, histogram shift.

I INTRODUCTION

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. Since first introduced, RDH has attracted considerable research interest.With the advance of computer networks and signal processing, digital multimedia are spread widely through the Internet nowadays. This causes the security problem of exposing transmitted digital data on the network with the risk of being copied or intercepted illegally. In order to protect the privacy of private data, various cryptographic techniques have been proposed to encrypt these data before conducting data transmission. However, with considerable increasing of the computing powers of modern computers, the security of the data yielded by these techniques is threatened. In addition, though cryptographic techniques encrypt secret messages into unrecognizable forms before transmission, the undisguised appearances of the encrypted message would easily arouse suspicion and bring on unexpected attacks from hackers.

The development of information hiding techniques provides another solution to protecting digital media. Such techniques may be employed to embed private or secret information into cover media in such a way that the existence of the hidden information is imperceptible but known only to a pre-concerted recipient. Information like private annotations, business logos, and critical intelligence

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

can be embedded into a cover image in an invisible form so that many applications, like ownership claim of digital contents, copyright protection of media, covert communication between parties, etc., can be fulfilled. Information hiding techniques used for covert communication are often called steganography, and those for ownership or copyright protection are often called watermarking.

In the early phase, conventional steganography emphasizes exploring higher hiding capacities and pursuing lower quality degradations in watermarked images (also referred to as stego-images in the sequel). In general, a small amount of content loss will occur in the stego-image, though often imperceptible.

However, such a loss is not desirable in some applications, such as legal documentation, military reconnaissance, high-precision scientific investigation, etc., because it may lead to risks of incorrect decision making. In view of this, a type of novel data hiding technique, which is referred to as reversible, invertible, lossless, or distortion-free, has been developed in recent years. In this study, a reversible data hiding method which yields stego-images with good qualities and high data hiding capacities is proposed.

REVERSIBLE DATA HIDING TECHNIQUES

Reversible data hiding techniques can be employed to restore stego-images to their pristine states after the hidden data are extracted.

Such techniques can be classified into three groups:

1. Based on data compression
2. Based on pixel-value difference expansion
3. Based on histogram shifting .

The strategy used in the techniques of the first group is to compress message data as well as related information and embed the result directly into the cover image. A method in this group is Barton which compresses the secret message before embedding them into the bit stream of digital data. a high-capacity lossless data hiding method which quantizes each image pixel by into L-level scales, compresses the quantization residues, and embeds the secret bits as well as the compressed data into the quantified image by the least-significant-bit (LSB) substitution technique.

The second group of reversible data hiding methods aims to explore the redundancy of pixel values in images. A technique of pixel-value difference expansion by performing fundamental arithmetic operations on pairs of pixels to discover hide able space. A location map is used to indicate whether pairs are expanded or not. An enhanced pixel-value difference expansion method proposed here which used a refined location map and a new concept of expandability to achieve higher data hiding capacities while keeping the resulting image distortion as low as that yielded .

The last group of reversible data hiding methods, to which the proposed method belongs, is based on the concept of histogram shifting. Here a reversible data hiding method which shifts slightly the part of the histogram between the maximum point (also called the peak point) and the minimum point to the right side by one pixel value to create an empty bin besides the maximum point for hiding an input message. Advantages of this method include yielding superior hiding capacities and providing higher qualities in stego-images. The knowledge of the maximum point and the minimum point of the histogram is necessary for retrieving the hidden data and restoring the stego-image lossless to the original state. In addition, the coordinates of the pixels whose gray values equal to the gray value of the minimum point b need be recorded as overhead information when the value of b is not zero. Consideration of multiple pairs of maximum and minimum points was also included in the method in order to raise the data hiding capacity, at the sacrifice of the resulting stego-image quality. A problem occurs here when too many of such pairs are selected for data hiding.

In such a case, a rapid increase of the size of the overhead information, which cannot be embedded completely in the cover image, might occur. So the idea of decomposing the entire cover image into blocks and using the peak point of the histogram of each block to hide data. The technique of block division successfully improves the data hiding capacity and keeps the stego-image quality at the same level, later the concept of slightly adjusting the pixel values located at both sides of a histogram peak to embed message data.. The Peak Signal-to-Noise Ratio (PSNR) of the stego-image needs a modification in some cases. A modification of the method using several pairs of

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

peak points and minimum points instead of just one was also proposed. However, the more of such pairs are selected, the larger the decrease in the data hiding capacity becomes, because more information of the selected minimum points and the reversible points need be kept in the location map. Later used the block division technique to increase the data hiding capacity.

II. PREVIOUS ARTS

Since lossless vacating room from the encrypted images is relatively difficult and sometimes inefficient, why are we still so obsessed to find novel RDH techniques working directly for encrypted images? 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. 1(b), the content owner first reserves 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 lossless 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.

III. PROPOSED METHOD

Nowadays huge 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. Recent Methods such as reserving room before encryption with a traditional RDH algorithm sometimes results in error and complicated usage at the time of data extraction and/or image restoration .Hence to overcome this problem, this project propose an efficient method which uses by combining cryptographic primitives based encryption with Histogram Shifting-based RDH algorithm, a high capacity and low distortion can be achieved efficiently, and thus it is easy for the data hider to reversibly embed data in the encrypted image.

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 using the same cryptographic primitives and extract the additional data by directly reading the decrypted version.. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.The proposed method can achieve real multi level reversibility, that is, data extraction and image recovery are free of any error. Experiments show that this method can embed more than 10 times as large payloads for the same image quality.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

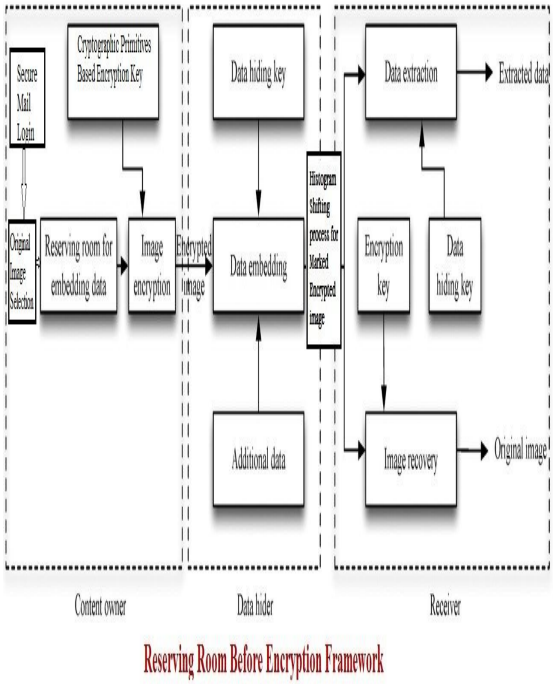
International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India



Reserving Room Before Encryption Framework

Fig 2 Framework For RRBE

A. Logging Mail by Content Sender

This module helps to log in to a mail in which this mail is configured and designed especially for sending confidential data with the Encrypted Image to another mail recipient.

B. Generation of Encrypted Image

Actually, 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 with a standard RDH algorithm so that LSBs of A can be used for accommodating messages; at last, encrypt the rearranged image to
generate its final version.

1) 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 , on which standard RDH algorithms such as [10], [11] can achieve better performance. To do that, without loss of generality, assume the original image is an 8 bits gray-scale image with its size MXN and pixels Ci,j€[0,255],1<=J<=M,1<=J<=N. First, the content owner extracts from the original image, along the rows, several overlapping blocks whose number is determined by the size of to-be-embedded messages, denoted by . In detail, every block consists of rows, where m=[1/N], and the number of blocks can be computed through n=M-m+1. An important point here is that each block is overlapped by pervious and/or subsequential blocks along the rows. For each block, define a function to measure its first-order smoothness

$$f = \sum_{u=2}^{m}\sum_{v=2}^{N-1}\left|C_{u,v} - \frac{C_{u-1,v} + C_{u+1,v} + C_{u,v-1} + C_{u,v+1}}{4}\right| \quad (1)$$

Higher relates to blockswhich contain relativelymore complex textures. The content owner, therefore, selects the particular block with the highest to be , and puts it to the front of

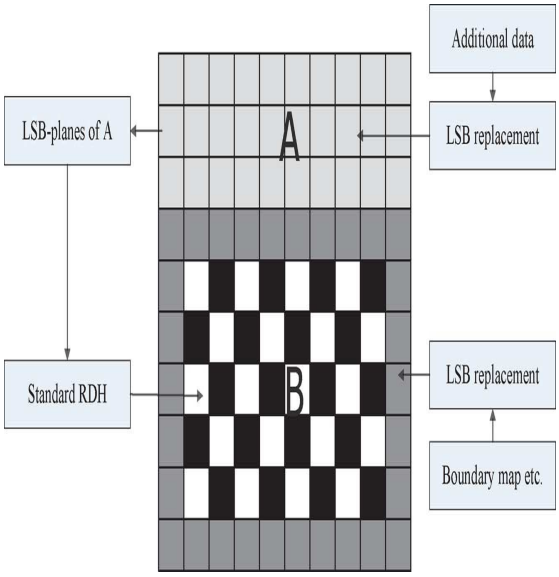


Fig 3 Illustration of image partition and embedding process.

the image concatenated by the rest part B with fewer textured areas, as shown in Fig. 3.The above discussion implicitly relies on the fact that only single LSB-plane A of is recorded. It is straightforward that

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

the content owner can also embed two or more SB-planes of A into B , which leads to half, or more than half, reduction in size of . However, the performance of , n terms of PSNR, after data embedding in the second stage decreases significantly with growing bit-planes exploited. Therefore, in this paper, we investigate situations that at most three LSB-planes of are employed and determine the number of bit-plane with regard to different payloads experimentally in the next section.

2) Self-Reversible Embedding: The goal of self-reversible embedding is to embed the LSB-planes of A into B by employing traditional RDH algorithms. For illustration, we simplify the method in [10] to demonstrate the process of self-embedding. Note that this step does not rely on any specific RDH algorithm. Pixels in the rest of image B are first categorized into two sets: white pixels with its indices i and j satisfying (i+j) mod 2=0and black pixels whose indices meet (i+j) mod 2=1 , as shown in Fig. 3. Then, each white pixel, is estimated by the interpolation value obtained with the four black pixels surrounding it as follows

$$B'_{i,j} = w_1 B_{i-1,j} + w_2 B_{i+1,j} + w_3 B_{i,j-1} + w_4 B_{i,j+1}, \quad (2)$$

where the weight wi,1<=i<=4 , is determined by the same method as proposed in [10]. The estimating error is calculated via $e_{i,j}=B_{i,j}-B'_{i,j}$ and then some data can be embedded into the estimating error sequence with histogram shift, which will be described later. After that, we further calculate the estimating errors of black pixels with the help of surrounding white pixels that may have been modified B. Then another estimating error sequence is generated which can accommodate messages as well. Furthermore, we can also implement multilayer embedding scheme by considering the modified as "original" one when needed. In summary, to exploit all pixels of , A two estimating error sequences are constructed for embedding messages in every single-layer embedding process. By bidirectional histogram shift, some messages can be embedded on each error sequence. That is, first divide the histogram of estimating errors into two parts, i.e., the left part and the right part, and search for the highest point in each part, denoted by LM and RM , respectively. For typical images, LM=-1 and RM=0. Furthermore, search for the zero point in each part, denoted by LN and RN. To embed messages into positions with an estimating error that is equal to RM, shift all error values between RM+1 and RN-1 with one step toward right, and then, we can represent the bit 0 with RM and the bit 1with RM+1 . The embedding process in the left part is similar except that the shifting direction is left, and the shift is realized by subtracting 1 from the corresponding pixel values. Suppose we should implement the embedding scheme times to accommodate additional data. In the previous x-1 single-layer embedding rounds, peak points of two error sequences are selected and utilized to embed messages as above mentioned. When it comes to the th single-layer embedding, only a small portion of messages is left to be embedded, so it is unadvisable to accommodate such little data at the expense of shifting all error values between peak points and their corresponding zero points. To deal with this issue, we can either exploit only part of error sequences which has enough peak points to embed the remaining messages while leaving the rest error sequences unchanged, or find two proper points, denoted by and , whose sum is larger, however closest to, the size of remaining messages. By shifting error values between and their corresponding zero points, messages can be embedded into and instead of peak points. Fig. 3 illustrates the idea of selecting proper points. Generally speaking, two solutions can gain significantly improvement in terms of PSNR when the length of data is relatively short, i.e., when. And the superiority of one solution over the other depends highly on statistics of natural image itself which will be discussed in the next section. The same with other RDH algorithms, overflow/underflow problem occurs when natural boundary pixels change from 255 to 256 or from 0 to . To avoid it, we only embed data into estimating error with its corresponding pixel valued from 1 to 254. However, ambiguities still arise when no boundary pixels are changed from 1 to 0 or from 254 to 255 during the embedding process. These created boundary pixels in the embedding process are defined as pseudo-boundary pixels. Hence, a boundary map is introduced to tell whether boundary pixels in marked image are natural or pseudo in extracting process. It is a binary sequence with bit "0" for natural boundary pixel,

bit "1" for pseudo-boundary pixel. Since estimating errors of marginal area of cannot be calculated via (2),

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

to make the best use of we choose its marginal area shown in Fig. 2 to place the boundary map, and use LSB replacement to embed it. The original LSBs of marginal area is assembled with messages,
i.e., LSB-planes of , and reversibly embedded into .In most cases, even with a large embedding rate, the length of boundary map is very short; thus, the marginal area of is enough to accommodate it. Meanwhile, several parameters such as , payloads embedded into the estimating errors of black pixels , total embedding rounds , start row and end row of in original image, are embedded into marginal area in a similar way. These parameters play an important role in data extraction and image recovery process.

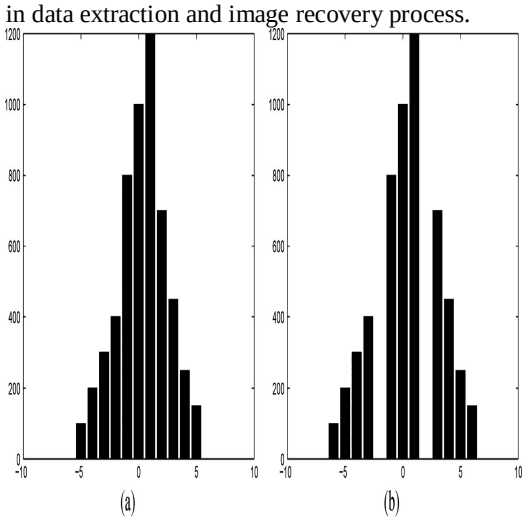


Fig 4 selection of proper points (a)original histogram (b)Shifted histogram(In this figure,length of messages is 1000 bits,LP=-2 and RP=2)

3) Image Encryption: After rearranged self-embedded image, denoted by , is generated, we can encrypts X to onstruct the encrypted image, denoted by .With a stream cipher, the encryption version of X is easily obtained. For example, a gray value X i,j ranging from 0 to 255 can be represented by 8 bits, X i,j(0),X i,j(1),.....Xi,j(7) such that

$$X_{i,j}(k) = \left\lfloor \frac{X_{i,j}}{2^k} \right\rfloor \bmod 2, \quad k = 0, 1, \ldots, 7. \qquad (3)$$

The encrypted bits Ei,j(k) can be calculated through exclusive-or operation

$$E_{i,j}(k) = X_{i,j}(k) \oplus r_{i,j}(k), \qquad (4)$$

where ri,j(k) is generated via a standard stream cipher determined by the encryption key. Finally, we embed 10 bits information into LSBs of first 10 pixels in encrypted version A of to tell data hider the number of rows and the number of bit-planes he can embed information into. Note that 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.

C. 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 the encrypted version of, denoted by A_E. Since A_E has been rearranged to the top of , it is effortless for the data hider to read 10 bits information in LSBs of first 10 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 sets a label following m to point out the end position of embedding process and further encrypts m according to the data hiding key to formulate marked encrypted image denoted by E'. Anyone who does not possess the data hiding key could not extract the additional data.

D. Data Extraction and Image Recovery

Since data extraction is completely independent from image decryption, the order of them implies two different practical applications.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

1) Case 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. 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_E and extract the additional data m 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.

2) Case 2: Extracting Data From Decrypted Images: In Case 1, both embedding and extraction of the data are manipulated in encrypted domain. On the other hand, there is a different situation that 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.

IV. CONCLUSION

A Reversible data hiding method based on histogram shifting has been proposed, which not only embeds large-volume data into cover images, but also produces stego-images with high qualities by using a strategy of hierarchical block division. The bottleneck of data-hiding-rate increasing at the block size of 8×8 found in existing methods is broken by the proposed non-recursive algorithms. And the proposed recursive versions of the algorithms enhance the performance further both in the data hiding capacity and the PSNR value, which result from the proposed scheme of recursive looking-ahead estimation of the data hiding capacity. The estimation process is a kind of optimal tree search under the quad-tree structure constructed by the hierarchical block division scheme, and so yields an optimal data hiding result under the tree structure. The experimental results show the effectiveness of the proposed method. Future researches may be directed to investigating more block division types for further improvement on the data hiding capacity, applying the histogram shifting technique to other information hiding applications, reducing the key size, eliminating the use to the location map, etc. Future work will be to continue to study the characteristics of image and data hiding methods to increase capacity, PSNR, and security. There should be deep research on increasing the size of the storing data and media data without any latency even if the size of the data increases without any limit.

REFERENCES

[1] 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.

[2] W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for reversible data hiding," in *Proc 13th Information Hiding (IH'2011),LNCS 6958*, 2011, pp. 255–269, Springer-Verlag.

[3] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers," *IEEE Trans.Image Process.*, vol. 21, no. 6, pp. 2991–3003, Jun. 2012.

[4] 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.

[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.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

[7] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3,pp. 721–730, Mar. 2007.

[8] X. L. Li, B. Yang, and T. Y. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,"*IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524–3533, Dec.2011.

[9] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Process.*, vol.89, pp. 1129–1143, 2009.

[10] L. Luo *et al.*, "Reversible imagewatermarking using interpolation technique," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 187–193,Mar. 2010.

[11] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Trans.*
Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.
[12] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC, 1996.

[13] 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.

[14] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[15] 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.