11 June, 2020

SRM UNIVERSITY AP
Andhra Pradesh

Reversible Data Hiding on Encrypted Images

By:

- Rakush Rimal (AP17110010129)
- Ramesh Yadav (AP17110010131)
- Cyrus Maharjan (AP17110010130)

Guided By:

- Dr. Manikandan V. M, SRM AP

Reversible data hiding in Encrypted Images

Abstract

In this project, we propose a scheme of data hiding in encrypted images. In the encryption phase, the original data is encrypted into images by using the stream cipher. Then the additional data is embedded into the image by modifying a small portion of encrypted data. It is based on the pixel redundancy within each block. The majority of the encrypted image is kept unchanged, the quality of the decrypted image is acceptable. In the receiver phase, the image is successfully extracted from the encrypted image with the help of an encryption key. The receiver can further recover the original plaintext image without any error by using the data hiding key. With an encrypted image containing additional data, one may first decrypt it using the encryption key, and the decryption version is similar to the original image. Then, by using the data hiding key, the user can recover the original data without loss. According to the data hiding key, with the help of spatial correlation in a natural images, the embedded data can be successfully extracted, and the original image can be perfectly recovered without loss.

Introduction

Encryption is defined as the process of encoding messages or information in such a way that the unauthorized user can't read it. Encryption denies the message content to the interceptor. Usually, encryption is used when one needs to keep his/her data private. In encryption, the message or information, which is called plaintext, is encrypted using an encryption algorithm, which creates cipher text and that cipher text should be decrypted to get the original message. Generally, an encryption scheme uses a pseudo-random encryption key generated by an algorithm. Such an algorithm is necessary for the decryption of the message because, without it, any party will be able to crack the code and access the data. Although, for a well-designed encryption scheme, large computational resources and skills are required. An authorized user can easily decrypt the message with the help of an encryption key, but the unauthorized users can't decrypt, it as they won't know the key. The encryption mechanism has not only made the transfer of data and information through the internet faster and easier, but also helped to maintain the

integrity and confidentiality of the information. There are many transmission media to transfer the data to destination like e-mails; at the same time, it may be easier to modify and misuse the valuable information through hacking. So, in order to transfer the data securely to the destination without any modifications, there are certain approaches like cryptography and steganography.

Data is hidden in the encrypted images by allocating memory before encryption. It is used to recover the original data without any loss or errors. It is basically used in the medical institutes, military institutes and law forensics, where the distortion of the original image is not permitted. In this process, the first thing we need to do is select the small portion of the image for embedding of data and reserve the memory space in the image. This sort of reservation is beneficial because it saves time for creating space for data on time. The next step is image encryption, in which the image is encrypted. There are a number of methods for encryption of images, such as image partition, in which an image is divided into two parts. Then the first part is reversibly embedded into the second part. That is, the least significant bits are firstly embedded in the second part. Then separable reversible data hiding is used for the process of data hiding. A data-hiding key is used to compress the least significant bits of the encrypted image by the data-hider to create a sparse space to adjust or accommodate some additional data. This additional data is restored back in image to get image with original quality at the receiver's end. At the receiver end, two tasks are carried out viz. data extraction & image recovery. But, to extract the original cover from the encrypted image, an additional task known as image restoration needs to be carried out. In this additional step, the original key contents are restored in the image. With an encrypted image containing extra data, if a user at the receiver's end has the key for decryption, he can extract the data even if he does not know the image content to extract the additional data. If the receiver has the encryption key, s/he can decrypt the received encrypted data to get an image that is similar to the original data but won’t be exact due to the embedded additional data. If the user at the receiver's end has both the encryption as well as the decryption key then he/she can extract the extra data as well as the original image error free by using the spatial correlation in normal image when the amount of additional data is not large.

Block Diagram:

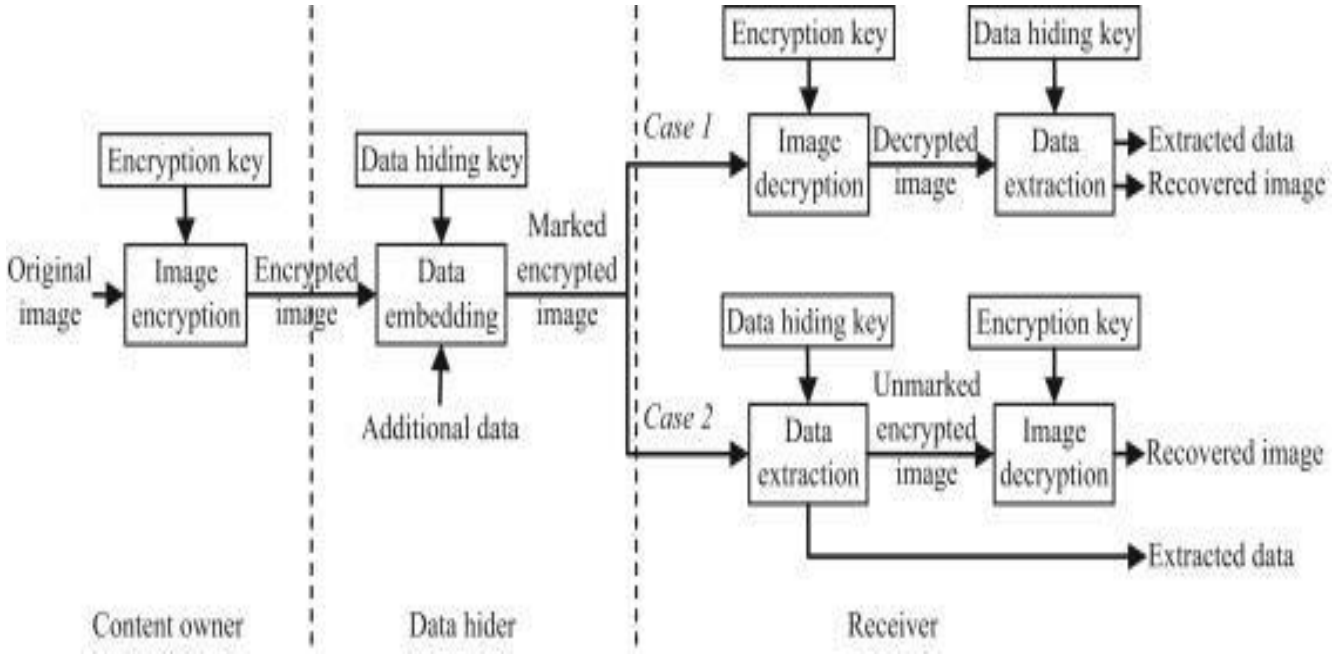


Fig. 1 Block diagram of RDH

Objective

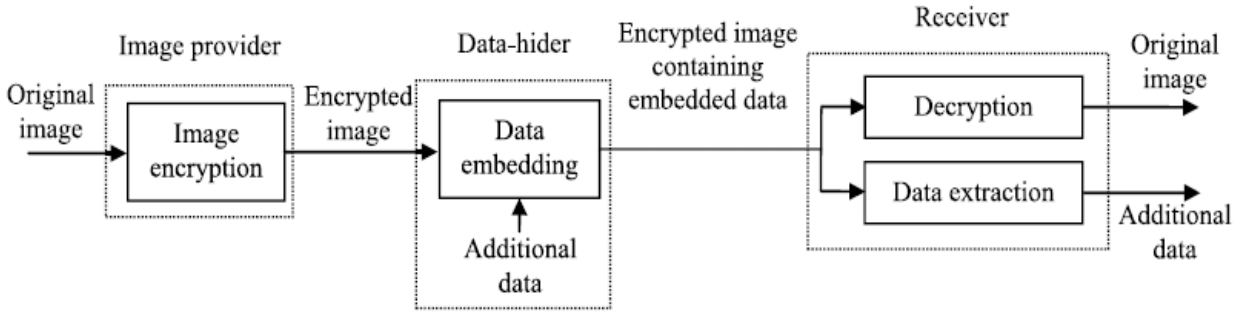
Objective of this project is to improve the security of information or data in which we will be able to hide our data and to increase the volume of hidden data in an image The technique of reversible data hiding is capable of recovering the data embedded and original image from stego image without distortion. Also provide an efficient data hiding technique and image encryption in which the data and the image can be retrieve independently. Restoring the original image after extraction of data from the stego image in which the data is hidden. E.g., in medical image it is required that the image is losselessly reconstructed after extraction of data. Content authentication to verify the authentication of the multimedia e.g., to verify the authenticity of a bank check transmitted over the internet. A watermarked image id deemed to be authentic if pixel values in the stego image are not altered after embedding the data.

Literature Review

In the last two decades, data hiding has received much attention from the research community. Previously research has been done on both data hiding and encryption. Encryption is one of the important ways of privacy protection of the data. Currently, research is being done in the existing combination of data hiding and encryption schemes. This was stated by Lian et al[1], Cancellaro et al [2] and Schmitz et al respectively in their research papers. Lian et al [1] used intra-prediction mode (current block is predicted from the edge of neighboring block) to encrypt cover domain and signs of Discrete Cosine Transform (DCT) coefficients. In the process, the watermark is embedded into the amplitudes of DCT coefficients. Cancellaro et al [2] could successfully encrypt and watermark the higher and lower bit planes of cover data in the transform domain. As only partial encryption is involved both the schemes result in leakage of partial information. In addition to this, the watermarked version is not considered for the partitioning original cover. Embedded data is irreversible.

RDH methods studied in the above-mentioned works are done for the plaintext domain, where the extra bits are embedded into the original unencrypted multimedia data with more focus on signal processing over the encrypted domain. This creates scope for the investigation of embedded additional data in the encrypted domain in a reversible manner. The content owner can encrypt the media data before transmission for securing a multimedia file before sharing with the receiver. In various applications, a channel administrator can add an extra message like original information, image rotation, or authentication data within the encrypted media. In the administration of medical images when they are to be encrypted for protecting patient privacy, the administrator can embed 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 of RDH in Encrypted Domain (RDH-ED). The principal aim of the 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

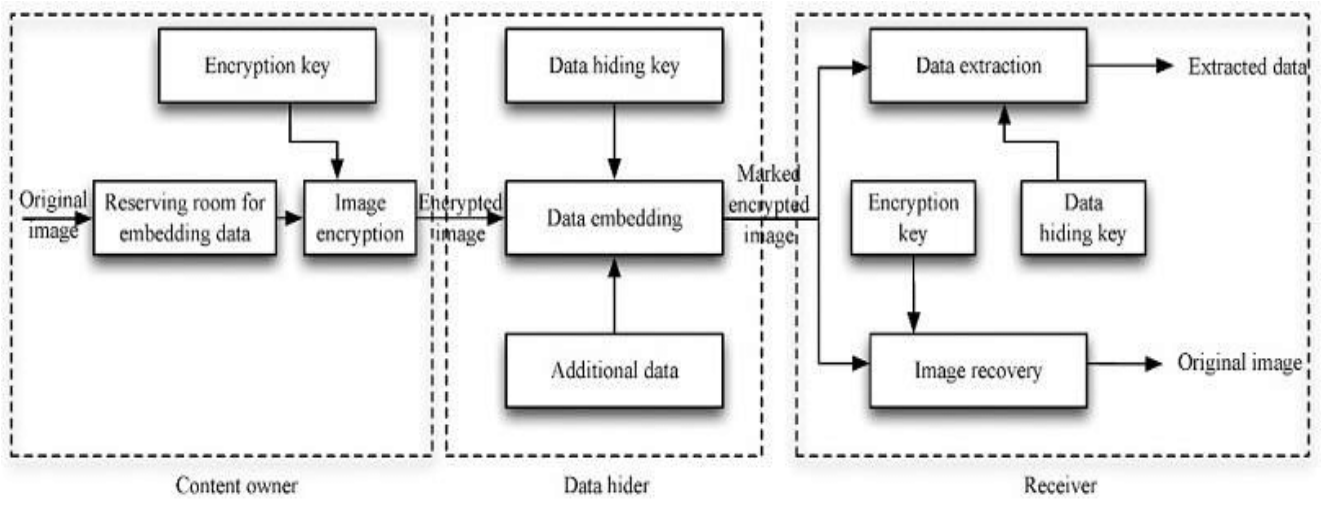
the plain text without errors.



Reversible Data Hiding in Encryption Domain has three blocks in the RDH-ED Content owner, Data-hider, and Receiver. Encryption of original media to the principal content can be done by the content owner with processing and without processing after selecting the encryption key. Data hider takes the help of a data hiding key for embedding additional bits into encrypted media for security purposes. The receiver has three options: the first option is used to decrypt the marked encrypted media to obtain appropriate media. The second option deals with extracting the additional embedded bits. Then lies the third option generating recovered media with a 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)



a) Vacating Room After Encryption (VRAE)

In VRAE method, original image content is encrypted using a standard cipher with an encryption key. Then an encrypted image is submitted to the data hider by the content owner to embed additional bits of data into the encrypted image by losslessly vacating the room with a data hiding key. From the receiver point of view, an authorized third party or content owner can retrieve the embedded data and recover the original image from the encrypted image with the help of data hiding and encryption key.

In [3] 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 [4] is in interesting study utilized a side match algorithm for higher embedded payload 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 neighboring 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 [5] and Hong et al [6] played a key role in enhancing the performance by improvising flipping ratio and unbalanced bit flipping. Liao et al [7], 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 [8] experimented by flipping only a 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 the image is recovered to a larger extent.

Chen et al [9] observed that the RDH scheme for an encrypted signal is developed by taking digital images as an illustration for description. While encrypting 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 affected 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 [10] 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.

b) Vacating Room Before Encryption (VRBE).

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 [11], Zhang et al [12], Cao et al [13] and Shiu et al [14] 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 easy and natural making way for a new "vacating room before encryption (VRBE)" framework.

Ma et al [11] proved that traditional RDH methods 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 preprocessing image. Data hiders will have an opportunity to use the positions of vacating LSBs in the encrypted image to obtain a large payload of 0.5bpp. Zhang et al [12] 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 preprocessing before encrypting the content.

Proposed Algorithm

Algorithm 1: Proposed data hiding scheme

Input	:	A grayscale image I having size of $R \times C$ pixels, an encryption key K, a secret message bit sequence D.
Output	:	An encrypted image E having size of $R \times C$ pixels which contain the hidden secret message D.
Step 1	:	Generate a pseudo-random integer matrix M having size of $R \times C$ by using the encryption key K
Step 2	:	Do the bitwise XOR operation between the pixels in the original image I and the integer values from M to get the encrypted image E'
Step 3		Initialize a matrix E with 0' having size of $R \times C$ to keep the final encrypted image with hidden secret message.
Step 4	:	Divide the encrypted image E' into non-overlapping blocks of size $B \times B$ pixels.
Step 5	:	Consider one unprocessed block C at a time from E' by traversing the image in column-wise linear order.
Step 6	:	Consider all the pixels in C and classify them into two different categories, say $S0$ and $S1$ in such a way that half of the pixels will go into $S0$ and the other half of the pixels will go into $S1$.
Step 7	:	Consider the next bit T from the secret message D
Step 8	:	If T is equal to 0 then flip all the three least significant bits (LSB) of $S0$ pixels, otherwise flip all the three LSBs of $S1$ to get a modified image block C'.
Step 9	:	Place the modified image block C' in the corresponding position at E.
Step 10		Repeat step 5 to step 9 until all the blocks in the image E' are processed. After this we will get a final encrypted image E which contains the hidden secret message
Step 11	:	Output the final encrypted image E

Algorithm 2: Proposed data extraction and image recovery scheme		
Input	:	An encrypted image E having size of $R \times C$ pixels which contains some hidden message, a decryption key K.
Output	:	The recovered image I having size of $R \times C$ pixels and the extracted secret message D.
Step 1	:	Generate a pseudo-random integer matrix M having size of $R \times C$ by using the decryption key K.
Step 2	:	Do the bitwise XOR operation between the pixels in the encrypted image E and the integer values from M to get the partially decrypted image I'
Step 3		Initialize a matrix I with 0' having size of $R \times C$ to keep the final recovered image.
		Initialize an empty list D to keep the extracted secret message bits.
Step 4	:	Divide the partially decrypted image I' into non-overlapping blocks of size $B \times B$ pixels.
Step 5	:	Consider one unprocessed block C at a time from I' by traversing the image in a column-wise linear order.
Step 6	:	Consider all the pixels in C and classify them into two different categories, say $S0$ and $S1$ in such a way that half of the pixels will go into $S0$ and the other half of the pixels will go into $S1$.
Step 7		Find a new image block $V0$ from C by flipping all the three LSBs of $S0$ pixels in C.
Step 8		Find a new image block $V1$ from C by flipping all the three LSBs of $S1$ pixels in C.
Step 9		Find the smoothness measure $M0$ from the image block $V0$
Step 10		Find the smoothness measure $M1$ from the image block $V1$
Step 11	:	If $M0$ is less than $M1$ then extract bit value 0 from the current image block C, and the recovered image block will be $V0$. Similarly, if $M1$ is less than $M0$ then extract bit value 1 from the current image block C, and the recovered image block will be $V1$. Keep appending the extracted bit value 0/1 to the extracted secret message bit sequence D.

Step 12	:	Place the recovered image block *V0 or V1* in the corresponding position of the recovered image *I.*
Step 13		Repeat step 5 to step 9 until all the blocks in the image *E'* are processed. After this we will get a final encrypted image *E* which contains the hidden secret message
Step 14	:	Output the recovered image *I* and the extracted secret message bit sequence *D.*

Experimental Results

The experimental study of the proposed scheme is carried out on the standard images obtained from well-known images such as Peppers, Baboon, Airplane, Boat and Lake. During the experimental study, all the images were converted into grayscale images of 512×512 pixels, and pseudo-random bits have been used as the secret message.

Three efficiency parameters are used for analyzing the efficiency of the proposed scheme:

- Embedding Rate: The number of bits that can be embedded per pixel in an image. The embedding rate will be measured as bits per pixels (bpp). The reversible data hiding schemes with high embedding rate is the good choice.

- Bit Error Rate (BER): The number bits extracted wrongly from the image at the receiver side will be considered as the bit error rate. Ideally, the bit error rate should be 0 for a reversible data hiding scheme.

- Peak Signal to Noise Ratio (PSNR): The PSNR between original image and the recovered image is a parameter helps us to measure the efficiency of image recovery process. If the recovered image is exactly same as the original image, the PSNR will be α.

The PSNR and BER obtained from the proposed scheme while using the well-known images.

- **For Peppers:**

- ER= 1/ (32*32)
- PSNR= 39.0075
- SSIM= 0.9930

- **For Baboon:**
  - ER= 1/ (32*32)
  - PSNR= 50.8976
  - SSIM= 0.9987
- **For Airplane:**
  - ER= 1/ (32*32)
  - PSNR= 39.6530
  - SSIM= 0.9947
- **For Boat:**
  - ER= 1/ (32*32)
  - PSNR= 43.0487
  - SSIM= 0.9971
- **For Lake:**
  - ER= 1/ (32*32)
  - PSNR= 54.3884
  - SSIM= 0.9995

Conclusion

Our proposed reversible data hiding technique is able to embed about 5–80 kb into a 512×512×8 grayscale image while guaranteeing the PSNR of the marked image versus the original image to be above 48 db. In addition, this algorithm can be applied to virtually all types of images. Furthermore, this algorithm is quite simple, and the execution time is rather short. Therefore, its overall performance is better than many existing reversible data hiding algorithms. It is expected that this reversible data hiding technique will be deployed for a wide range of applications in the areas such as secure

medical image data systems, and image authentication in the medical field and law enforcement, and the other fields where the rendering of the original images is required or desired.

REFERENCE

[1] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital water marking and steganography. Morgan Kaufmann, 2007.

[2] W.Bender, W.Butera, D.Gruhl, R.Hwang, F.J.Paiz and S.Pogreb, "Applications for data hiding" IBM systems journal, vol.39, no. 3.4,pp. 547-568, 2000.

[3] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Reversible data hiding," in Proceedings. International Conference on Image Processing. 2. IEEE, 2002, pp. II–II.

[4] Y.-Q. Shi, X. Li, X. Zhang, H.-T. Wu, and B. Ma, "Reversible data hiding: advances in the past two decades," IEEE access, vol. 4, pp.3210–3237, 2016

[5] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, "Hiding in medical images: a new high capacity and reversible data hiding technique," Journal of biomedical informatics, vol. 66, pp. 214–230, 2017.

[6] W. Zhang, H. Wang, D. Hou, and N. Yu, "Reversible data hiding in encrypted images by reversible image transformation," IEEE Transactions on multimedia, vol. 18, no. 8, pp. 1469–1479, 2016

[7] J. Wang, J. Ni, X. Zhang, and Y.-Q. Shi, "Rate and distortion optimiza-tion for reversible data hiding using multiple histogram shifting," IEEE transactions on cybernetics, vol. 47, no. 2, pp. 315–326, 2016.

[8] F. Huang, J. Huang, and Y.-Q. Shi, "New framework for reversible data hiding in encrypted domain," IEEE transactions on information forensics and security, vol. 11, no. 12, pp. 2777–2789, 2016.

[9] S. Xiang and X. Luo, "Reversible data hiding in homomorphic encrypted domain by mirroring ciphertext group," IEEE transactions on circuits and systems for video technology, vol. 28, no. 11, pp. 3099–3110, 2017.

[10] L. Xiong, Z. Xu, and Y.-Q. Shi, "An integer wavelet transform based scheme for reversible data hiding in encrypted images, "Multidimensional Systems and Signal Processing, vol. 29, no. 3, pp. 1191–1202,2018.

[11] X. Zhang, "Reversible data hiding in encrypted image," IEEE signal processing letters, vol. 18, no. 4, pp. 255–258, 2011.

[12] C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Circular interpretation on histogram for reversible watermarking," in IEEE Int. Multimedia Signal Process. Workshop, France, Oct. 2001, pp. 345–350.

[13] Y. Q. Shi, Z. Ni, D. Zou, and C. Liang, "Lossless data hiding: fundamentals,

algorithms and applications," in IEEE Int. Symp. Circuits Syst., Vancouver, Canada, May 2004, pp. 33–36.

[14] M. Goljan, J. Fridrich, and R. Du, "Distortion-free data embedding," in Proc. 4th Inf. Hiding Workshop, Pittsburgh, PA, Apr. 2001, pp. 27–41.

[15] G. Xuan, J. Zhu, J. Chen, Y. Q. Shi, Z. Ni, and W. Su, "Distortionless data hiding based on integer wavelet transform," IEE Electron. Lett., vol. 38, no. 25, pp. 1646–1648, Dec. 2002.

[16] A. R. Calderbank, I. Daubechies, W. Sweldens, and B. Yeo, "Wavelet transforms that map integers to integers," Appl. Comput. Harmonic Anal., vol. 5, no. 3, pp. 332–369, 1998.

[17] I. Daubechies and W. Sweldens, "Factoring wavelet transforms into lifting steps," J. Fourier Anal. Appl., vol. 4, pp. 247–269, 1998.