A Survey on Separable Reversible Data Hiding in Encrypted Images

Mithu Varghese
PG student, Computer Science
Thejus Engeering College
Thrissur,India

Teenu S Jhon
Asst.Prof ,Computer Science Department
Thejus Engineering College
Thrissur,India

ABSTRACT
Data security and data integrity are the two challenging areas for research. So many research is progressing on the field like internet security. The requirement of secure transmission of data is important in our life. The transmission should be more secure when channel/network is too noisy/fraudulent. Image transmission is one of the application that must be securely transmitted over the fraudulence network. Secure transmission of image is required in various fields like medical/telemedicine, military etc. When it is desired to send the confidential important secure data over an insecure and bandwidth-constrained channel it is customary to encrypt as well as compress the cover data and then embed the confidential/important/secure data into that cover data. For achieving this facility there are various data hiding techniques, compression techniques, encryption/ decryption techniques available. Here is a review on different data hiding techniques in encrypted image.

Keywords
Digital images, Reversible data hiding, Separable reversible data hiding.

1. INTRODUCTION
Digital images has increased rapidly on the Internet. Security becomes increasingly important for many applications, confidential transmission, video surveillance, military and medical applications. 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. Compression also help to reduce the storage space. The protecting digital images can be done with encryption or data hiding algorithms. Since few years, a problem is to try to combine compression, encryption and data hiding in a single step. A new challenge consists to embed data in encrypted images. We can embed data in an encrypted image by using an irreversible approach of data hiding. Since the entropy of encrypted image is maximal, the embedding step, considered like noise, is not possible by using standard data hiding algorithms.. As a result of the availability of powerful image processing software packages such as Photoshop, anyone can easily modify such digital media for any reason and create unconscious forgeries. How to prevent a medical image from being maliciously altered, that is, detecting the tampered parts, has become an important issue. In order to safeguard digital images, image authentication schemes are the most widely used method. Generally, the authentication codes are usually derived from the prominent features of the medical image and are directly embedded into the image. However, the embedding procedure will distort the images. This distortion may cause the modified medical images to be unable to be used for further diagnosis.. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption That is to say, the method must have the ability to restore the original content after the extraction of the authentication codes. Therefore, it is an important challenge to develop a reversible data-hiding scheme for medical images encrypted images in order to remove the embedded data during the encryption step.

Jun Tian[1] developed a simple and efficient reversible data-embedding method for digital images in which he explored the redundancy in the digital content to achieve reversibility. For security, the bit stream can be encrypted by the Advanced Encryption Standard (AES) algorithm prior to embedding. . It do not include any results with a PSNR higher than 44 dB. Sergio Vicente,D. Pamboukian and Hae Yong Kim [2] invented the technique that selects a set of low visibility pixels and uses the Golomb code to compress the predictions of these pixels. But the resulting watermarked image may not present high visual quality. It can't apply for very small images. Zhenfei Zhao and et.al [3] showed a reversible data hiding method for natural images. Zhicheng Ni and et.al [4] studied a reversible data hiding algorithm, which can recover the original image without any distortion from the marked image after the hidden data have been extracted. This algorithm does not work in an image having an exactly horizontal histogram. Chia-Chen Lin et. al [5] propose a DCT-based reversible data hiding scheme. Ching-Yu Yanga et al. [6] propose a reversible data hiding by coefficient-bias algorithm .X. Zhang [67 propose Non Separable reversible data hiding in encrypted image. None of these methods are separable from data hiding and image extraction. Xinpeng Zhang [8] introduce a new method called separable reversible data hiding in encrypted images.It can be seen that the performance of the this separable scheme is significantly better than non separable method.

1.1 Reversible data hiding
Additional message are embed into some cover media, such as military or medical images, in a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message is called reversible data hiding.

General signal processing typically takes place before encryption or after decryption. Sometimes the content owner does not believe in the provider of the service , in such cases ability to provide manipulating the plain content secret is undesirable. So manipulation on encrypted data when keeping the plain content is allowed. Due to the limited channel resource a channel provider without any knowledge of the cryptographic key may compress the encrypted data ,when the secret data to be transmitted. In order to ensure the privacy the content owner should encrypt the data when it share a secret image with other person. Some information's such as the

origin information, image notation or authentication data,are want to be added within the encrypted image by a channel administrator who does not know the original image content. At receiver side it may be also expected that the original content can be recovered without any error after decryption and retrieve of additional message. That means a reversible data hiding scheme for encrypted image is desirable. Data hiding is the process of hiding the data into cover media. That is, the data hiding process links a set of the embedded data and a set of the cover media data. In most cases of data hiding, the original image becomes distorted due to data hiding and cannot be inverted back to the original media. That is, cover media has permanent distortion even after the hidden data have been removed. In some applications, such as medical diagnosis and law enforcement it is desired that the original cover media can be recovered efficiently with no loss. The marking techniques satisfying this requirement are referred to as reversible, lossless, distortion-free or invertible data hiding techniques.

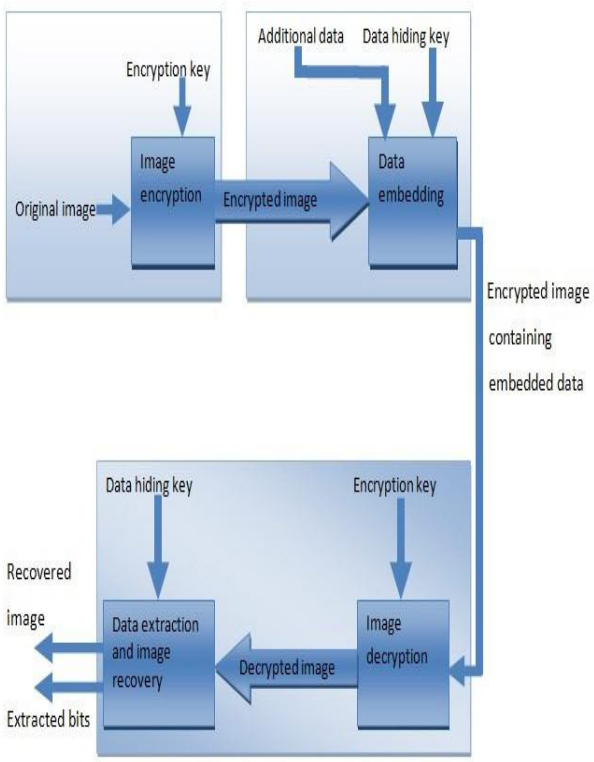

Fig 1 Non Separable reversible data hiding in encrypted image [10].

1.2 Separable reversible data hiding

Separable reversible data hiding, the name its self indicates that it is a separable reversible data technique .That is it is reversible data technique but which is separable. The separable means which is able to separate .The separation of activities i.e. extraction of original cover image and extraction of payload is done in this method. This separation requires some basic cause to occur. In separable data hiding key explained by Xinpeng Zhang the separation exists according to keys.

At the receiver side, there are three different cases are encountered. The separation of extracting the data and getting the cover media come to be exists. That's why it is called as separable reversible data hiding.

1.3 Compression

Compression of encrypted data has become considerable research interest in recent years. The traditional way of securely and efficiently transmitting redundant data is to first compress the data to reduce the redundancy, and then to encrypt the compressed data to mask its meaning. At the receiver side, the decryption and decompression operations are orderly performed to recover the original data. However, in some application scenarios, a sender needs to transmit some data to a receiver and hopes to keep the information confidential to a network operator who provides the channel resource for the transmission. That means the sender should encrypt the original data and the network provider tend to compress the encrypted data without any knowledge of the cryptographic key and the original data. There are Several techniques for compressing/decompressing encrypted data have been developed. When it is desired to transmit redundant data over an insecure and bandwidth-constrained channel, it is customary to first compress the data and then encrypt. Mark Johnson and et.al has examined the possibility of first encrypting a data and then compressing it, such that the compressor does not have knowledge of the encryption key. The encrypted data can be compressed using distributed source coding principles, because the key will be available at the decoder. They showed that under some conditions the encrypted data can be compressed to the same rate as the original, unencrypted data could have been compressed .

2. LITERATURE REVIEW

Jun Tian[1] developed a data-embedding method for reversible data-embedding. It was very simple and efficient method .In order to get the reversibility he explored the redundancy in the digital content. This data-embedding method for digital images by considering the redundancy is very simple as well as efficient. This reversible data-embedding method can be applied to digital audio and video as well. The method is based on difference expansion (DE).Difference expansion (DE) is based on finding the differences of neighboring pixel values. From these values select some difference values and find the difference expansion (DE). The original content restoration information, a message authentication code, and additional data (which could be any data, such as date/time information, auxiliary data, etc.) will all be embedded into the difference values. Both the payload capacity limit and the visual quality of embedded images are among the best in the literature. As a basic requirement, He achieved the policy that quality degradation on the image after data embedding should be low. In a digital image, one can select some expandable difference values of pixels, and embed one bit into each of them. To extract the embedded data and restore the original values, the decoder needs to know which difference values have been selected for the DE. To facilitate it need to embed such location information, such that the decoder could access and employ it for decoding. For this purpose, it will create and embed a location map, which contains the location information of all selected expandable difference values. Furthermore, the decoder needs to know where (from which difference values) to collect and decode the location map. After the DE, the expanded difference value might not be expandable. On the decoder side, to check whether is expandable does not tell whether the original has been selected for the DE during embedding. The expanded difference value is changeable, so the decoder could examine each changeable difference value. As with many image processing techniques, the encoder serves for the decoder, in the DE method, the encoder will take all changeable

difference values as the embedding area, so that the decoder will use the same data to decode. During data embedding, it will modify all changeable difference values, by either adding a new LSB (via the DE) or modifying its LSB. To guarantee an exact recovery of the original image, it will also embed the original values of those modified LSBs. In brief, the date-embedding DE algorithm consists of six steps: calculating the difference values, partitioning difference values into four sets, creating a location map, collecting original LSB values, data embedding by replacement, and finally an inverse integer transform. But the data extraction is not separable from the image extraction. Data can only compressed by lossless compression techniques. For security, the bit stream can be encrypted by the advanced encryption standard (AES) algorithm prior to embedding. Where AES is slow compared to RC4 algorithm.It do not include any results with a PSNR higher than 44 dB.

Sergio Vicente,D Pamboukian and Hae Yong Kim [2] invented the technique based on Golomb code . In order to compress the predictions of the pixels that selects a set of low visibility pixels. For to compress the predictions of the pixels it uses the Golomb code . This compressed data and the net payload data are embedded into the image. In order to create space for storing the hidden data the technique use Golomb code to compress the predictions of low visibility pixels. This technique has many potential practical uses, including lossless authenticated FAX transmission and reversible content protection of binary document databases The technique was applied to several kinds of binary images and, in average, only 453 pixels were compressed to get space to store 128 bits of net payload data. If the prediction is good, the predicted value and the true value should be the same with probability higher than 50%. Store zero when the predictions correct and one when it is wrong, subsequences of zeros will be longer (in most cases) than subsequences of ones, what makes the compression possible. The Golomb code is a good compression algorithm for this kind of sequence. As the DBPs' neighborhoods are not modified during the insertion, the predictions can be reconstructed in the extraction. The vector of predictions (0s and 1s), together with the neighborhoods of DBPs, allows recovering the original DBPs' values.The advantages of reversibly embedding the DS over appending it are obvious. First, there is no extra information (besides the image itself) to be stored or transmitted. Second, any lossless format conversion, such as changing the format from TGA to BMP, does not erase the embedded information. Third, the presence of a reversible authentication is less noticeable than the ostensibly appended DS. But the resulting watermarked image may not present high visual quality, because the concept "low visibility pixel" does not apply to this kind of image. It can't apply for very small images, because there is not enough space to store the payload and the compressed information and random noise images with similar amounts of black and white pixels, because the prediction is very difficult.

Zhenfei Zhao and et.al [3] showed a reversible data hiding method for natural images. Due to the similarity of neighbor pixels' values most differences between pairs of adjacent pixels are equal or close to zero. A histogram is constructed based on these difference statistics. In the data embedding stage, a multilevel histogram modification mechanism is employed. As more peak points are used for secret bits modulation, the hiding capacity is enhanced compared with those conventional methods based on one or two level histogram modification. Moreover, as In the data extraction and image recovery stage, the embedding level instead of the peak points and zero points is used. He proposes a reversible data hiding scheme based on histogram modification. Its principle is to modify the histogram constructed based on the neighbor pixel differences instead of the host image's histogram. Many peak points exist around the bin zero in this histogram due to the similarity of adjacent pixel values. Besides, many zero points exist in both sides of the bin zero. Here the peak point refers to the height of histogram bin with the largest statistical value (i.e., the count falling in the corresponding bin), and the zero point means the histogram bin with zero value. In our case, all the differences are classified into levels of [−255, 255] and each level corresponds to a histogram bin. Hence it is reasonable to modify the histogram with a multilevel mechanism for hiding more secret data. In decoder, the host image pixels are recovered one by one. That is, each pixel is recovered aided by its previously recovered neighbor. Meanwhile, the secret data is extracted from the marked adjacent pixels' differences.

Zhicheng Ni and et.al [4] studied a reversible data hiding algorithm, which can recover the original image without any distortion from the marked image after the hidden data have been extracted. This algorithm utilizes the zero or the minimum points of the histogram of an image and slightly modifies the pixel grayscale values to embed data into the image. It can embed more data than many of the existing reversible data hiding algorithms. They proved analytically and shown experimentally that the peak signal-to-noise ratio (PSNR) of the marked image generated by this method versus the original image is guaranteed to be above 48 dB. The computation of this technique is quite simple and the execution time is rather short. Although this lossless data hiding technique is applied to still images, it is also applicable to videos which consist of a sequence of images. Instead, the key issue is if the histogram has maximum and minimum points, i.e., if the histogram changes up-and-down enough. An extreme example in which this algorithm does not work is an image having an exactly horizontal histogram .

Chia-Chen Lin et. al [5] propose a DCT-based reversible data hiding scheme. Their proposed layer-1 strategy considers some areas not used by Chang et al.'s scheme, which call layer-2 data embedding. This method applied Tian's pixel expansion method to design their layer-1 data embedding strategy Their experimental results confirm that the hiding capacity provided by combining this strategy with Chang et al.'s is higher than that provided by the Chang et al. approach alone. Moreover, the image quality of stego-images with this scheme remains above 30 dB for most test images, which is better than the best image quality offered by Changet al.'s scheme. Finally, the security and reversibility of Chang et al.'s scheme is unaffected when their layer-2 scheme is combined with our proposed layer-1 scheme.

Ching-Yu Yanga et al. [6] propose a reversible data hiding by coefficient-bias algorithm . A simple lossless data hiding method based on the coefficient-bias algorithm by embedding bits in both spatial domain and frequency domain is consider. In spatial domain, each pixel in a host image is first subtracted from the block-mean. Then, a stego image is generated by embedding a large amount of bits (or the primary message) in the mean-removed blocks via the coefficient-bias algorithm. To provide an extra security and robustness, the stego-image is transformed to frequency domain by integer wavelet transform (IWT). A secondary watermark is hidden in the low-high (LH) and high-low (HL) subbands of IWT domain by the this algorithm. Simulations show that both the perceptual quality and hiding capacity are not bad. Moreover,

the resultant images introduced by the this method are tolerant of the attacks such as JPEG2000, JPEG, brightness, and inverting.

X. Zhang [7] presented a practical scheme satisfying the requirements. A content owner encrypts the original image using an encryption key, and a data-hider embeds additional data into the encrypted image using a data-hiding key yet he does not know the original content. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key.Image encryption involves generation of encryption key and generation of pseudo-random sequence. Encryption key is 128 bit value. It is generated randomly by using the random function. The random function generates the random key in an uniformly distributed function. Instead Pseudo random sequence consists of random bits generated using the encryption key. In our system, RC-4 algorithm is used to create the pseudo- random sequence using the 128-bit encryption key. It is represented as sequence of bytes (An array of bytes). The number of bytes generated should be equal to the number of pixels in the input image provided the pixels are represented as 8-bit values. If the pixels are represented as 16-bit values then the number bytes in pseudo-random sequence should be double the number of pixels.

This scheme made of three stages. Image encryption,data embedding, data, extraction and image-recovery. Image encryption can done by simply X-OR the bits of pixel and random function. In Data embedding Segment the encrypted image into nonoverlapping blocks sized by s × s .Then Pseudo-randomly divide the s2 pixels into two sets S0 and S1. Then check the additional bit to be embedded is 0 or 1.If it 0 then flip 3 LSB bit of S1.If it is 1 then flip 3 LSB bit of S0. In data extraction and image-recovery XOR the encrypted pixel and random bit obtain from encryption key. Then segment the decrypted image into blocks with the data-hiding key. Then Divide the pixels in each block into two sets. And check which one is original. Then concatenate the extracted bits and collect the recovered blocks.

In this scheme, the activity of data extraction is not separable from the activity of content decryption. In other words, the additional data must be extracted from the decrypted image, so that the principal content of original image is opened before data extraction, and, if someone has the data-hiding key but not the encryption key, he is not able to extract any information from the encrypted image containing additional data. It PNR value calculated nearby 37.9.This is low PSNR value compared to other methods. Error rate is large especially for high capacity cases.

In order to overcome the problems within reversible data hiding techniques Xinpeng Zhang [8] introduce a new method called separable reversible data hiding in encrypted images. This scheme is made up of image encryption, data embedding and data-extraction/image-recovery phases. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image.

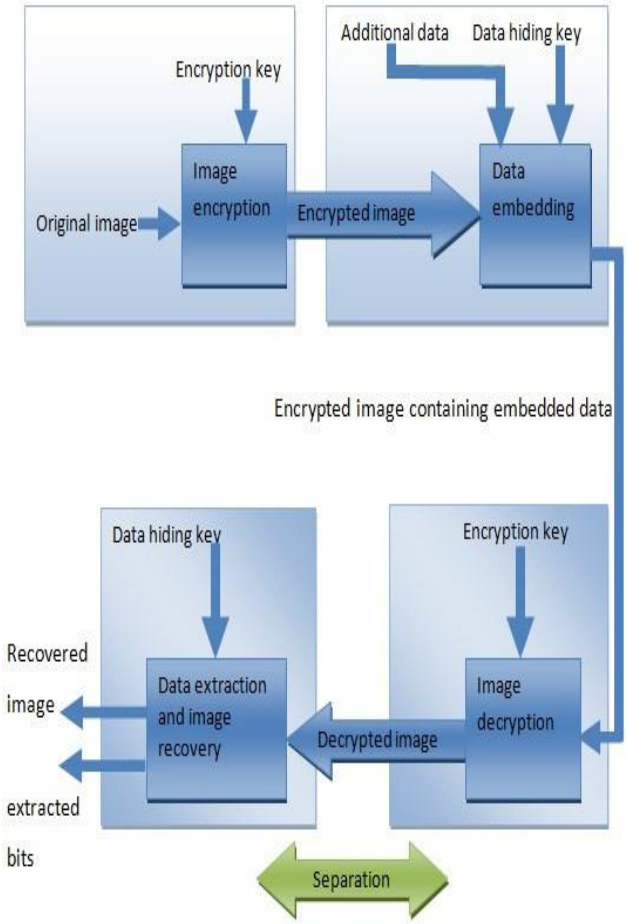

Fig 2 Separable reversible data hiding in encrypted image [10].

This method [8] provides higher PSNR. Higher PSNR means better quality. Since the spa-tial correlation is exploited for the content recovery, the rate-distortion performance in a smoother image is better. It can be seen that the performance of the this separable scheme is significantly better than nons eparable method .He[8] also compared the proposed scheme with the non separable method (Xinpeng Zhang) over 100 images sized 2520 *3776, people. When meeting the perfect recovery condition, this scheme has an average 203% gain of embedded data amount with same PSNR value in directly decrypted image, or an average gain of 8.7 dB of PSNR value in directly decrypted image with same embedded data amount.

3. CONCLUSION

Here is a review on different data hiding techniques in encrypted image.AS we seen so far none of the reversible method can separate data extraction and image recovery. Separable reversible data hiding in encrypted image, which consists of image encryption, data embedding and data-extraction/image-recovery phases. In the first phase, the content owner encrypts the original uncompressed image using an encryption key. Although a data-hider does not know the original content, can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. With an encrypted image containing additional data, the receiver may extract the

additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large. If the lossless compression method is used for the encrypted image containing embedded data, the additional data can be still extracted and the original content can be also recovered since the lossless compression does not change the content of the encrypted image containing embedded data. However, the lossy compression method in compatible with encrypted images generated by pixel permutation is not suitable here since the encryption is performed by bit-XOR operation. In the future, a comprehensive combination of image encryption and data hiding compatible with lossy compression deserves further investigation.

4. REFERENCES

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

[2] Sergio vicente d. pamboukian1 and hae yong kim,(2011) "reversible data hiding and reversible authentication watermarking for binary images"

[3] Zhenfei Zhao (2011), Reversible data hiding based on multilevel histogram modification and sequential recovery," Int. J. Electron. Commun. (AEÜ) *65 814–826*

[4] Zhicheng Ni Yun-Qing Shi, Nirwan Ansari, and Wei Su (2011) , "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol, vol. 16, no. 3, Mar 2006,pp. 354-362.

[5] Chia-Chen Lin, Pei-Feng Shiu, "DCT-based Reversible Data Hiding Scheme" , JOURNAL OF SOFTWARE, VOL. 5, NO. 2, FEBRUARY 2010

[6] Ching-Yu Yanga,Wu-Chih Hua and Chih-Hung Lin, "Reversible Data Hiding by Coefficient-bias Algorithm", Journal of Information Hiding and Multimedia Signal Processing, Volume 1, Number 2, April 2010.

[7] X. Zhang,(2011) "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258.

[8] Xinpeng Zhang, (2013) "Separable Reversible Data Hiding in Encrypted Imag", IEEE transactions on information forensics and security, vol. 7, NO. 2, APRIL 2012.

[9] T.Bianchi, A . Piva and M Barni "On the implementation of the discrete Fourier transform in the encrypted domain"IEEE Trans.Inform Forensics security,vol.4,no 1,pp,86-97,feb.2009

[10] Vinit Agham and Tareek Pattewar, A Survey on Separable Reversible Data Hiding techniques", IMACST: VOLUME 4 NUMBER 1 MAY 2013

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

[12] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption andwatermarking in video compression," IEEE Trans. Circuits Syst. VideoTechnol., vol. 17, no. 6, pp. 774–778, Jun. 2007.

[13] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, andA. Neri, "A commutative digital image watermarking and encryptionmethod in the tree structured Haar transform domain," Signal Processing:Image Commun., vol. 26, no. 1, pp. 1–12, 2011.

[14] D. Kundur and K. Karthik, "Video fingerprinting and en4ryption principlesfor digital rights management," Proceedings IEEE, vol. 92, no.6, pp. 918–932, Jun. 2004.

[15] X. Zhang, "Reversible data hiding in encrypted image," IEEE SignalProcess. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

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

[17] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE\Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.

[18] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," IEEE Trans. Image Process., vol. 14, no.2, pp. 253–266, Feb. 2005.

[19] W. Hong, T.-S. Chen, Y.-P. Chang, and C.-W. Shiu, "A high capacityreversible data hiding scheme using orthogonal projection and predictionerror modification," Signal Process., vol. 90, pp. 2911–2922, 2010.

[20] C.-C. Chang, C.-C. Lin, and Y.-H. Chen, "Reversible data-embeddingscheme using differences between original and predicted pixel values,"IET Inform. Security, vol. 2, no. 2, pp. 35–46, 2008.

[21] A. Mayache, T. Eude, and H. Cherifi, "A comparison of image qualitymodels and metrics based on human visual sensitivity," in Proc. Int.Conf. Image Processing (ICIP'98), Chicago, IL, 1998, vol. 3, pp.409–413.

[22] Z. Wang and A. C. Bovik, "A universal image quality index," IEEESignal Process. Lett., vol. 9, no. 1, pp. 81–84, Jan. 2002.