ijecs
open access
www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 3 March 2013 Page No. 558-568

Secure And Authenticated Reversible Data Hiding In Encrypted Images

Dr.V.Khanaa, Dr.Krishna Mohanta

Dean Info. Bharath University Chennai 600 073
Sri Lakshmi Ammal Engineering College Chennai 73
Department of Computer Sci.&Engg.

Mail:drvkannan62@yahoo.com

Abstract:-Reversible data hiding a novel technique which is used to embed additional information in the encrypted images, applies in military and medical images, which can be recoverable with original media and the hided data without loss. A number of reversible data hiding techniques were proposed in the recent years, but on analysis, all lacks in providing the security and authentication. This project proposes a novel reversible data hiding technique which work is separable, the receiver can extract the original image or extra embedded data or both according to the keys hold by the receiver. On the other hand the receiver can verify the data hided by the data hider, such that the work proposes both security and authentication. This project proposes a novel reversible data hiding technique which poses both security and authentication for additional data stored in the encrypted images. Also proposed work is separable, the receiver can extract the original image or extra embedded data or both according to the keys hold by the receiver. On the other hand the receiver can verify the data hided by the data hider, such that the work proposes both security and authentication.

This work proposes a novel scheme for separable reversible data hiding in encrypted images. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, a data-hider may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing additional data, if a receiver has the data-hiding key, he can extract the additional data though he does not know the image content. If the receiver has the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image when the amount of additional data is not too larg

INTRODUCTION

In recent years, signal processing in the encrypted domain has attracted considerable research interest. As an effective and popular means for privacy protection, encryption converts the ordinary signal into unintelligible data, so that the traditional signal processing usually takes place before encryption or after decryption. However, in some scenarios that a content owner does not trust the processing service provider, the ability to manipulate the encrypted data when keeping the plain content unrevealed is desired. For instance, when the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may tend to compress the encrypted data due to the limited channel resource. While an encrypted binary image can be compressed with a lossless manner by finding the syndromes of low-density parity-check codes [1], a lossless compression method for encrypted gray image using progressive decomposition and rate-compatible punctured turbo codes is developed in [2]. With the lossy compression method presented in [3], an encrypted gray image can be efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. When having the compressed data, a receiver may reconstruct the principal content of original image by retrieving the values of coefficients. The computation of transform in the encrypted domain has also been studied. Based on the homomorphic properties of the underlying cryptosystem, the discrete Fourier transform in the encrypted domain can be implemented [4]. In [5], a composite signal representation method packing together a number of signal samples and processing them as a unique sample is used to reduce the complexity of computation and the size of encrypted data.

There are also a number of works on data hiding in the encrypted domain. In a buyer–seller watermarking protocol [6], the seller of digital multimedia product encrypts the original data using a public key, and then permutes and embeds an encrypted fingerprint provided by the buyer in the encrypted domain. After decryption with a private key, the buyer can obtain a watermarked product. This protocol ensures that the seller cannot know the buyer's watermarked version while the buyer cannot know the original version. An anonymous fingerprinting scheme that improves the enciphering rate by exploiting the Okamoto-Uchiyama encryption method has been proposed in [7]. By introducing the composite signal representation mechanism, both the computational overhead and the large communication bandwidth due to the homomorphic public-key encryption are also significantly reduced [8]. In another type of joint data-hiding and encryption schemes, a part of cover data is used to carry the additional message and the rest of the data are encrypted, so that both the copyright and the privacy can be protected. For example [9], the intraprediction mode, motion vector difference and signs of DCT coefficients are encrypted, while a watermark is embedded into the amplitudes of DCT coefficients. In [10], the cover data in higher and lower bit-planes of transform domain are respectively encrypted and watermarked. In [11], the content owner encrypts the signs of host DCT coefficients and each content-user uses a different key to decrypt only a subset of the coefficients, so that a series of versions containing different fingerprints are generated for the users.

The reversible data hiding in encrypted image is investigated in [12]. Most of the work on reversible data hiding focuses on the data embedding/extracting on the plain spatial domain

[13]–[17]. But, in some applications, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content. And it is also hopeful that the original content should be recovered without any error after image decryption and message extraction at receiver side. Reference [12] presents a practical scheme satisfying the above-mentioned requirements and Fig. 1 gives the sketch. A content owner encrypts the original image using an encryption key, and a data-hider can embed additional data into the encrypted image using a data-hiding key though 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. In the scheme, the data extraction is not separable from the content

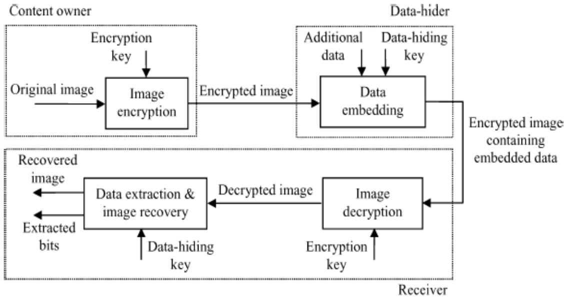


Fig. 1. Sketch of non-separable reversible data hiding in encrypted image.

I. EXISTING SYSTEM

In recent years, signal processing in the encrypted domain has attracted considerable research interest. As an effective and popular means for privacy protection, encryption converts the ordinary signal into unintelligible data, so that the traditional signal processing usually takes place before encryption or after decryption. However, in some scenarios that a content owner does not trust the processing service provider, the ability to manipulate the encrypted data when keeping the plain content unrevealed is desired. For instance, when the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may tend to compress the encrypted data due to the limited channel resource.

In some existing joint data-hiding and encryption schemes, a part of cover data is used to carry the additional message and the rest data are encrypted. For example, the intra-prediction mode, motion vector difference and signs of DCT coefficients are encrypted, while a watermark is embedded into the amplitudes of DCT coefficients. In the cover data in higher and lower bit-planes of transform domain are respectively encrypted and watermarked. In the content owner encrypts the signs of host DCT coefficients and each content-user uses a different key to decrypt only a subset of the coefficients, so that a series of versions containing different fingerprints are generated for the users. In these joint schemes, however, only a partial encryption is involved, leading to a leakage of partial information of the cover. Furthermore, the separation of original cover and embedded data from a watermarked version is not considered. In each sample of a cover signal is encrypted by a public-key mechanism and a homomorphic property of encryption is exploited to embed some additional data into the encrypted signal. But the data amount of encrypted signal is significantly expanded and the computation complexity is high. Also, the data embedding is not reversible.

In the existing Reversible techniques one can hide the secret data in one or two bits of an image. When the secret data is hided in three or more bits of the image its quality becomes low and the human eye can detect the changes in the image. Hence, its data carrying capacity and the tamper resistance or security is low. Due to the disadvantages above, the secret data is embedded in two or more bits of the image using LSB and this increases the capacity i.e) large amount of information can be embedded in the cover medium. Also, secret data is embedded using increment and decrement technique and this increases the security i.e) hacker's inability to detect the secret data. Also the quality of the stego image is much better when compared to the existing techniques.

Also In LSB, the least significant bit of each pixel for a specific color channel or for all color channels is replaced with a bit from the secret data. Although it is a simple techniques, but the probability of detecting the hidden data is high. SCC technique is an enhancement. The color channel, where the secret data will be hidden in, is cycling frequently for every bit according to a specific pattern. For example, the first bit of the secret data is stored in the LSB of red channel, the second bit in the green channel, the third bit in the blue channel and so on. This technique is more secure than the LSB but still it is suffers detecting the cycling pattern that will reveal the secret data. Also it has less capacity than the LSB.

Obviously, most of the existing data hiding techniques are not reversible. For instance, the widely utilized spread-spectrum based data hiding methods are not invertible owing to truncation (for the purpose to prevent over/underflow) error and round-off error. The well-known least significant bit (LSB) plane based schemes are not lossless owing to bit replacement without "memory." Another category of data hiding techniques, quantization-index-modulation (QIM)based schemes are not distortion-free owing to quantization error.

The newly suggested technique a novel reversible data hiding scheme for encrypted image, which is made up of image encryption, data embedding and data-extraction/image-recovery phases. The data of original cover are entirely encrypted, and the additional message is embedded by modifying a part of encrypted data. At receiver side, with the aid of spatial correlation in natural image, the embedded data are successfully extracted while the original image is perfectly recovered.

Reversible Data Hiding

We present a novel reversible (lossless) data hiding (embedding) technique, which enables the exact recovery of the original host signal upon extraction of the embedded information. A generalization of the well-known LSB (least significant bit) modification is proposed as the data embedding method, which introduces additional operating points on the capacity-distortion curve. Lossless recovery of the original is achieved by compressing portions of the signal that are susceptible to embedding distortion, and transmitting these compressed descriptions as a part of the embedded payload. A prediction-based conditional entropy coder which utilizes static portions of the host as side-information improves the compression efficiency, and thus the lossless data embedding capacity.

Data Hiding For JPEG Images

This paper proposes a lossless data hiding technique for JPEG images based on histogram pairs. It embeds data into the JPEG quantized 8x8 block DCT coefficients and can achieve good performance in terms of PSNR versus payload through manipulating histogram pairs with optimum threshold and optimum region of the JPEG DCT coefficients. It can obtain higher payload than the prior arts. In addition, the increase of JPEG file size after data embedding remains unnoticeable. These have been verified by our extensive experiments.

Digital Image Water Marking

Watermarking, which belong to the information hiding field, has seen a lot of research interest recently. There is a lot of work begin conducted in different branches in this field. Steganography is used for secret communication, whereas watermarking is used for content protection, copyright management, content authentication and tamper detection. In this paper we present a detailed survey of existing and newly proposed steganographic and watermarking techniques. We classify the techniques based on different domains in which data is embedded.

Digital Image Steganography In simple words, Steganography can be defined as the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. Though the concept of steganography and cryptography are the same, but still steganography differs from cryptography. *Cryptography* focuses on keeping the contents of a message secret, *steganography* focuses on keeping the existence of a message secret. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated The strength of steganography can thus be amplified by combining it with cryptography.

Reversible Data hiding In Encrypted Image

This work proposes a novel reversible data hiding scheme for encrypted image. After encrypting the entire data of an uncompressed image by a stream cipher, the additional data can be embedded into the image by modifying a small proportion of encrypted data. With an encrypted image containing additional data, one may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, with the aid of spatial correlation in natural image, the embedded data can be successfully extracted and the original image can be perfectly recovered.

Lossless Compression

The feasibility of lossless compression of encrypted images has been recently demonstrated by relying on the analogy with source coding with side information at the decoder. However previous works only addressed the compression of bi-level images, namely sparse black and white images, with asymmetric probabilities of black and white pixels. In this paper we investigate the possibility of compressing encrypted grey level and color images, by decomposing them into bit-planes. A few approaches to exploit the spatial and cross-plane correlation among pixels are discussed, as well as the possibility of exploiting the correlation between color bands. Some experimental results are shown to evaluate the gap between the proposed solutions and the theoretically achievable performance.

II. PROPOSEDSYSTEM

The proposed 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 shows the three cases at the receiver side.

Here propose a new reversible data embedding technique, which can embed a large amount of data (5–80 kb for a 512 x 512 x 8 grayscale image) while keeping a very high visual quality for all natural images, specifically, the PSNR of the marked image versus the original image is guaranteed to be higher.

Image Encryption

Assume the original image is in uncompressed format and each pixel with gray value falling into [0, 255] is represented by 8 bits.

$$B_{i,j,k} = b_{i,j,k} \oplus r_{i,j,k}$$

where ri,j,k are determined by an encryption key using a standard stream cipher. Then, B,i,j,k are concatenated orderly as the encrypted data. A number of secure stream cipher methods can be used here to ensure that anyone without the encryption key, such as a potential attacker or the data hider, cannot obtain any information about original content from the encrypted data.

Data Embedding

In the data embedding phase, some parameters are embedded into a small number of encrypted pixels, and the LSB of the other encrypted pixels are compressed to create a space for accommodating the additional data and the original data at the positions occupied by the parameters.

The detailed procedure is as follows According to a data-hiding key, the data-hider pseudo-randomly

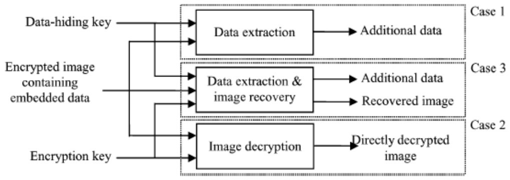


Fig. 2. Three cases at receiver side of the proposed separable scheme.

In encryption phase, the exclusive-or results of the original bits and pseudo-random bits are calculated

selects Np encrypted pixels that will be used to carry the parameters for data hiding.

Here, Np is a small positive integer, for example, Np=20. The other (N-Np) encrypted pixels are pseudo-randomly permuted and divided into a number of groups, each of which contains L pixels.

The permutation way is also determined by the data-hiding key.

For each pixel-group, collect the M least significant bits of the L pixels, and denote them as B (k,1) , B (k,2) …… B(k,M*L) where k is a group index within [1,(N-Np)/L] and M is a positive integer less than 5.

The data-hider also generates a matrix G sized (M*L – S) * M*L, which is composed of two parts. The left part is the identity matrix and the right part is pseudo-random binary matrix derived from the data-hiding key.

For each group , which is product with the G matrix to form a matrix of size (M * L-S). Which has a sparse bits of size S, in which the data is embedded and arrange the pixels into the original form and repermutated to form a original image.

Image Decryption

When having an encrypted image containing embedded data, a receiver firstly generates ri,j,k according to the encryption key, and calculates the exclusive-or of the received data and

ri,j,k to decrypt the image. We denote the decrypted bits as b1i,j,k . Clearly, the original five most significant bits (MSB) are retrieved correctly. For a certain pixel, if the embedded bit in

the block including the pixel is zero and the pixel belongs to S1, or the embedded bit is 1 and the pixel belongs to S0 , the data-hiding does not affect any encrypted bits of the pixel. So, the three decrypted LSB must be same as the original LSB, implying that the decrypted gray value of the pixel is correct. On the other hand, if the embedded bit in the pixel’s block is 0 and the pixel belongs to S0, or the embedded bit is 1 and the pixel belongs to S1 , the decrypted LSB

$$\begin{aligned} b'_{i,j,k} &= r_{i,j,k} \oplus B'_{i,j,k} \\ &= r_{i,j,k} \oplus \overline{B_{i,j,k}} \\ &= r_{i,j,k} \oplus \overline{b_{i,j,k} \oplus r_{i,j,k}} \\ &= \overline{b_{i,j,k}}, \qquad k = 0, 1, 2. \end{aligned}$$

That means the three decrypted LSB must be different from the original LSB. In this case:

$$b'_{i,j,k} + b_{i,j,k} = 1,$$

Data Extraction

If the receiver has both the data-hiding, he may aim to extract the embedded data According to the data-hiding key, the values of M,L and S, the original LSB of the Np selected encrypted pixels, and the (N-Np) * S/L - Np additional bits can be extracted from the encrypted image containing embedded data. By putting the Np LSB into their original positions, the encrypted data of the Np selected pixels are retrieved, and their original gray values can be correctly decrypted using the encryption keys. In the following, we will recover the original gray values of the other (N-Np) pixels.

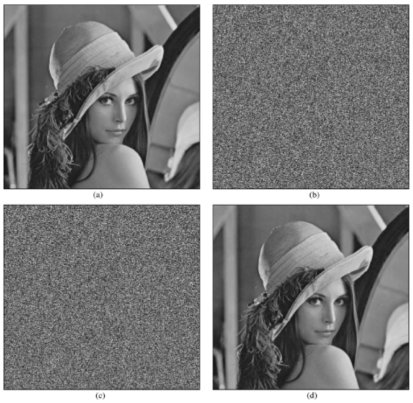


Fig. 3. (a) Original Lena, (b) its encrypted version, (c) encrypted image containing embedded data with embedding rate 0.017 bpp, and (d) directly decrypted version with PSNR 39.0 dB.

This paper proposes a novel scheme for separable reversible data hiding in encrypted image. In the proposed scheme, the original image is encrypted using an encryption key and the additional data are embedded into the encrypted image using a data-hiding key. With an encrypted image containing additional data, if the receiver has only the data-hiding key, he can extract the additional data though he does not know the image content. If he has only the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the embedded additional data. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original image without any error when the amount of additional data is not too large.

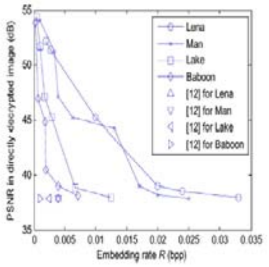


Fig. 4. Rate-PSNR comparison between the proposed scheme and the method in [12].

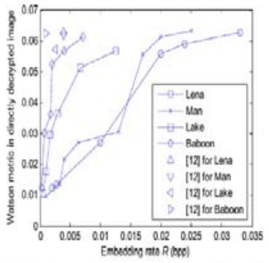


Fig. 5. Rate-Watson metric comparison between the proposed scheme and the method in [12].

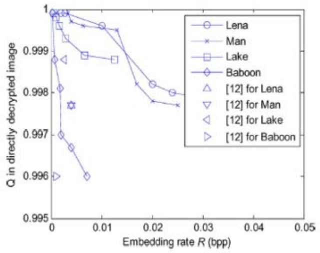
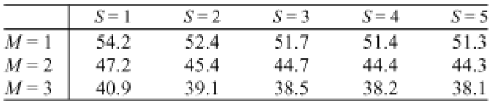


Fig. 6. Rate-Q comparison between the proposed scheme and the method in [12].

Theoretical Values

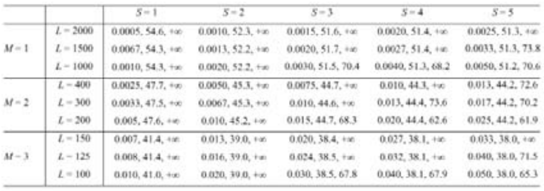
TABLE I
THEORETICAL VALUES OF PSNR (dB) WITH RESPECT TO S AND M



	$S=1$	$S=2$	$S=3$	$S=4$	$S=5$
$M=1$	54.2	52.4	51.7	51.4	51.3
$M=2$	47.2	45.4	44.7	44.4	44.3
$M=3$	40.9	39.1	38.5	38.2	38.1

Embedding Rate

TABLE II
EMBEDDING RATE R, PSNR IN DIRECTLY DECRYPTED IMAGES (dB) AND PSNR IN RECOVERED IMAGES (dB) WITH DIFFERENT PARAMETERS FOR TEST IMAGE LENA



		$S=1$	$S=2$	$S=3$	$S=4$	$S=5$
$M=1$	$L=2000$	0.0005, 54.6, +∞	0.0010, 52.3, +∞	0.0015, 51.6, +∞	0.0020, 51.4, +∞	0.0025, 51.3, +∞
	$L=1500$	0.0067, 54.3, +∞	0.0013, 52.2, +∞	0.0020, 51.7, +∞	0.0027, 51.4, +∞	0.0033, 51.3, 73.8
	$L=1000$	0.0010, 54.3, +∞	0.0020, 52.2, +∞	0.0030, 51.5, 70.4	0.0040, 51.3, 68.2	0.0050, 51.2, 70.6
$M=2$	$L=400$	0.0025, 47.7, +∞	0.0050, 45.3, +∞	0.0075, 44.7, +∞	0.010, 44.3, +∞	0.013, 44.2, 72.6
	$L=300$	0.0033, 47.5, +∞	0.0067, 45.3, +∞	0.010, 44.6, +∞	0.013, 44.4, 73.6	0.017, 44.2, 70.2
	$L=200$	0.005, 47.6, +∞	0.010, 45.2, +∞	0.015, 44.7, 68.3	0.020, 44.4, 62.6	0.025, 44.2, 61.9
$M=3$	$L=150$	0.007, 41.4, +∞	0.013, 39.0, +∞	0.020, 38.4, +∞	0.027, 38.1, +∞	0.033, 38.0, +∞
	$L=125$	0.008, 41.4, +∞	0.016, 39.0, +∞	0.024, 38.5, +∞	0.032, 38.1, +∞	0.040, 38.0, 71.5
	$L=100$	0.010, 41.0, +∞	0.020, 39.0, +∞	0.030, 38.5, 67.8	0.040, 38.1, 67.9	0.050, 38.0, 65.3

IV. CONCLUSION

In this paper, a novel scheme for separable reversible data hiding in encrypted image is proposed, 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, he can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodatethe additional data. With an encrypted image containingadditional 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 anyerror 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 isperformed by bit-XOR operation. In the future, a comprehensive combination of image encryption and data hiding compatible with lossy compression deserves further investigation

V. FUTURE ENHANCEMENT

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, thelossy compression method compatible with encrypted images generated by pixel permutation is not suitable here since the encryption performed by bit-XOR operation. In the future, a comprehensive combination of image encryption and data hiding compatible with lossy compression deserves further investigation.

The implemented a Novel Reversible method can be enhanced in future by using the following provisions

- And MLSB technique can also be applied after embedding when there is lot of change in the pixel to retain nearest to the original value
- Can be applied in networking and the keys are sent and received securely

REFERENCES

[1] 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.

[2] W. Liu, W. Zeng, L. Dong, and Q. Yao,“Efficient compression of encrypted grayscale images,”*IEEETrans. Image Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[3] X. Zhang, “Lossy compression and iterative reconstruction for encrypted image,” *IEEE Trans. Inform. Forensics Security*, vol. 6, no. 1, pp. 53–58, Feb. 2011.

[4] 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.

[5] T. Bianchi, A. Piva, and M. Barni, “Composite signal representation for fast and storage-efficient processing of encrypted signals,” *IEEE Trans. Inform. Forensics Security*, vol. 5, no. 1, pp. 180–187, Feb. 2010.

[6] N. Memon and P. W. Wong, “A buyer-seller watermarking protocol,”*IEEE Trans. Image Process.*, vol. 10, no. 4, pp. 643–649, Apr. 2001.

[7] M. Kuribayashi and H. Tanaka, “Fingerprinting protocol for images based on additive homomorphic property,” *IEEE Trans. Image Process.*, vol. 14, no. 12, pp. 2129–2139, Dec. 2005.

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

[9] S. Lian, Z. Liu, Z. Ren, and H.Wang, “Commutative encryption and watermarking in video compression,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 6, pp. 774–778, Jun. 2007.

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

[11] D. Kundur and K. Karthik, “Video finger printing and encryption principles for digital rights management,” *Proceedings IEEE*, vol. 92, no. 6, pp. 918–932, Jun. 2004.

[12] X. Zhang, “Reversible data hiding in encrypted image,” *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

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

[14] 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.

[15] 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.

[16] W. Hong, T.-S. Chen, Y.-P. Chang, and C.-W. Shiu, “A high capacity reversible data hiding scheme using orthogonal projection and prediction error modification,” *Signal Process.*, vol. 90, pp. 2911–2922, 2010.

[17] C.-C. Chang, C.-C. Lin, and Y.-H. Chen, “Reversible data-embedding scheme using differences between original and predicted pixel values,” *IET Inform. Security*, vol. 2, no. 2, pp. 35–46, 2008.

[18] A. Mayache, T. Eude, and H. Cherifi, “A comparison of image quality models and metrics based on human visual sensitivity,” in *Proc. Int. Conf. Image Processing (ICIP’98)*, Chicago, IL, 1998, vol. 3, pp. 409–413.

[19] Z. Wang and A. C. Bovik, “A universal image quality index,” *IEEE Signal Process. Lett.*, vol. 9, no. 1, pp. 81–84, Jan. 2002.