Volume 6, Issue 10, October 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Separable Reversible Data Hiding Using Discrete Wavelet Transform In Encrypted JPEG Image

Nayankumar G. Hargule*
M.Tech Student, CSE, VIT Nagpur,
Maharashtra, India

Prof. Pravin G. Kulurkar
H.O.D, CSE, VIT Nagpur,
Maharashtra, India

Abstract— Among various digital image formats used in daily life, the Joint Photographic Experts Group (JPEG) is the most popular. Therefore, reversible data hiding (RDH) in JPEG images is important and useful for many applications such as archive management and image authentication. However, RDH in JPEG images is considerably more difficult than that in uncompressed images because there is less information redundancy in JPEG images than that in uncompressed images, and any modification in the compressed domain may introduce more distortion in the host image. Furthermore, along with the embedding capacity and fidelity (visual quality), which have to be considered for uncompressed images, the storage size of the marked JPEG file should be considered. In this paper, based on the philosophy behind the JPEG encoder and the statistical properties of discrete wavelet transform (DWT) coefficients, we present some basic insights into how to select quantized DWT coefficients for RDH. Then, a new histogram shifting-based RDH scheme for JPEG images is proposed, in which the zero coefficients remain unchanged and only coefficients with values 1 and −1 are expanded to carry message bits. Moreover, a block selection strategy based on the number of zero coefficients in each 8 × 8 block is proposed, which can be utilized to adaptively choose DCT coefficients for data hiding.

Keywords: Encryption, Decryption, Reversible Data hiding, Data Recovery, Discrete Wavelet Transform.

I. INTRODUCTION

Encryption and data hiding are two effective means of data protection. While the encryption techniques convert plaintext content into unreadable cipher text, the data-hiding techniques embed additional data into cover media by introducing slight modifications. In some distortion unacceptable scenarios, data hiding may be performed with a lossless or reversible manner. Although the terms lossless and reversible have a same meaning in a set of previous references, we would distinguish them in this paper. We say a data-hiding method is lossless if the display of cover signal containing embedded data is same as that of original cover even though the cover data have been modified for data embedding. For example, in the pixels with the most used color in a palette image are assigned to some unused color indices for carrying the additional data, and these indices are redirected to the most used color. This way, although the indices of these pixels are altered, the actual colors of the pixels are kept unchanged. On the other hand, we say a data-hiding method is reversible if the original cover content can be perfectly recovered from the cover version containing embedded data even though a slight distortion has been introduced in data-embedding procedure. A number of mechanisms, such as difference expansion , histogram shift ,and lossless compression , have been employed to develop the reversible data-hiding techniques for digital images. Recently, several good prediction approaches and optimal transition probability under payload-distortion criterion have been introduced to improve the performance of reversible data hiding.

II. LITERATURE REVIEW

A number of reversible data hiding techniques have been proposed, and they can be roughly classified into three types: lossless compression based methods, difference expansion (DE) methods, and histogram modification (HM) methods. In practical aspect, many RDH techniques have emerged in recent years.

A lossless data-hiding scheme for public key-encrypted images is proposed. There are three parties in the scheme: an image provider, a data hider, and a receiver. With a cryptosystem possessing probabilistic property, the image provider encrypts each pixel of the original plaintext image using the public key of the receiver, and a data hider who does not know the original image can modify the ciphertext pixel values to embed some additional data into the encrypted image by multilayer wet paper coding under a condition that the decrypted values of new and original ciphertext pixel values must be same. When having the encrypted image containing the additional data, a receiver knowing the data-hiding key may extract the embedded data, while a receiver with the private key of the cryptosystem may perform decryption to retrieve the original plaintext image. In other words, the embedded data can be extracted in the encrypted domain, and cannot be extracted after decryption since the decrypted image would be same as the original plaintext image due to the probabilistic property. That also means the data embedding does not affect the decryption of the plaintext image.

A reversible data-hiding scheme for public-key-encrypted images. In the reversible scheme, a preprocessing is employed to shrink the image histogram, and then each pixel is encrypted with additive homomorphic cryptosystem by the image provider. When having the encrypted image, the data hider modifies the ciphertext pixel values to embed a bit-sequence generated from the additional data and error-correction codes. Due to the homomorphic property, the modification in encrypted domain will result in slight increase/decrease on plaintext pixel values, implying that a decryption can be implemented to obtain an image similar to the original plaintext image on receiver side. Because of the histogram shrink before encryption, the data-embedding operation does not cause any overflow/underflow in the directly decrypted image. Then, the original plaintext image can be recovered and the embedded additional data can be extracted from the directly decrypted image. Note that the data extraction and content recovery of the reversible scheme are performed in plaintext domain, while the data extraction of the previous lossless scheme is performed in encrypted domain and the content recovery is needless.

III. PROPOSED WORK

Here, a new data hiding technique is proposed which cannot only control the over-stretching of image but will also prevent the overflow/underflow while maintaining satisfactory visual perception

The Compression technique with pruning proposal based on discrete wavelet transform (DWT). The proposed technique first decomposes an image into coefficients called sub-bands and then the resulting coefficients are compared with a threshold. Coefficients below the threshold are set to zero. Finally, the coefficients above the threshold value are encoded with a loss less compression technique.

The compression features of a given wavelet basis are primarily linked to the relative scarceness of the wavelet domain representation for the signal. The notion behind compression is based on the concept that the regular signal component can be accurately approximated using the following elements: a small number of approximation coefficients (at a suitably chosen level) and some of the detail coefficients.

A novel scheme for separable reversible data hiding 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 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.

Result analysis with respect to SNR, PSNR, COMPRESSION RATIO.

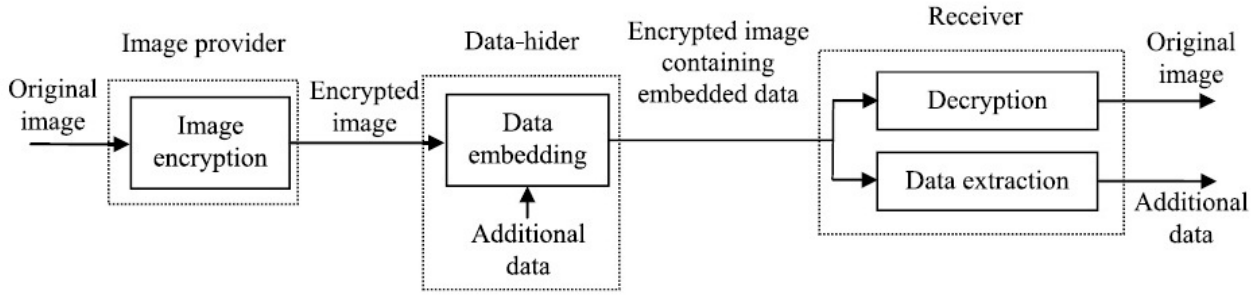

Fig. Block diagram of Separable Reversible data hiding in Encrypted Image

IV. CONCLUSION

This paper proposes lossless, reversible, and combined data hiding schemes for ciphertext images encrypted by public-key cryptography with probabilistic and homomorphic properties. In the lossless scheme, the ciphertext pixel values are replaced with new values for embedding the additional data into the LSB-planes of ciphertext pixels. This way, the embedded data can be directly extracted from the encrypted domain, and the data embedding operation does not affect the decryption of original plaintext image. In the reversible scheme, a preprocessing of histogram shrink is made before encryption, and a half of ciphertext pixel values are modified for data embedding. On the receiver side, the additional data can be extracted from the plaintext domain, and, although a slight distortion is introduced in decrypted image, the original plaintext image can be recovered without any error. Due to the compatibility of the two schemes, the data embedding operations of the lossless and the reversible schemes can be simultaneously performed in an encrypted image. Therefore, the receiver may extract a part of embedded data in the encrypted domain, and extract another part of embedded data and recover the original plaintext image in the plaintext domain.

REFERENCES

[1] Fangjun Huang, Xiaochao Qu, Hyoung Joong Kim, Jiwu Huang, "Reversible Data Hiding in JPEG Images " , *IEEE Transactions On Circuits And Systems For Video Technology*, vol. 26, no. 9, Sept 2016

[2] Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng, "Lossless and Reversible Data Hiding in Encrypted Images With Public-Key Cryptography," *IEEE Transactions On Circuits And Systems For Video Technology*, vol. 26, no. 9, sep. 2016.

[3] Fatema-Tuz-Zohra Khanam, Kyoung-Young Song, Sunghwan Kim, "A Modified Reversible Data Hiding in Encrypted Image Using Enhanced Measurement Functions", *IEEE ICUFN* 2016

[4] Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image", IEEE *Transactions On Information Forensics And Security*, vol. 7, no. 2, April 2012

[5] X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum rate prediction and optimized histograms modification for reversible data hiding," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 653–664, Mar. 2015.

[6] X. Zhang, "Reversible data hiding with optimal value transfer," *IEEE Trans. Multimedia*, vol. 15, no. 2, pp. 316–325, Feb. 2013.

[7] W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Process. Lett.*, vol. 19, no. 4, pp. 199–202, Apr. 2012.

[8] X. Li, B. Yang, and T. 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] W. Hong, T.-S. Chen, and C.-W. Shiu, "Reversible data hiding for high quality images using modification of prediction errors," *J. Syst. Softw.*, vol. 82, no. 11, pp. 1833–1842, 2009.

[10] G. Coatrieux, C. Le Guillou, J.-M. Cauvin, and C. Roux, "Reversible watermarking for knowledge digest embedding and reliability control in medical images," *IEEE Trans. Inf. Technol. Biomed.*, vol. 13, no. 2, pp. 158–165, Mar. 2009.

