IORD Journal of Science & Technology
E-ISSN: 2348-0831
Volume 3, Issue 3 (MAR-APRIL 2017) PP07-12
IMPACT FACTOR 1.719
www.iord.in

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

Mr. Nayankumar G. Hargule
P.G. Student
Department of Computer Science & Engineering
Vidarbha Institute of Technology, Nagpur
nayankumarhargule69@gmail.com

Prof. Pravin G. Kulurkar
H.O.D
Department of Computer Science & Engineering
Vidarbha Institute of Technology, Nagpur
pravinkulurkar@gmail.com

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.

1. 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.

2. Proposed Scheme

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.

A. Image Encryption

In this phase, the image provider encrypts a plaintext image using the public key of probabilistic cryptosystem p_k. For each pixel value $m(i, j)$, where (i, j) indicates the pixel position, the image provider calculates its ciphertext value

$$c(i, j) = E[p_k, m(i, j), r(i, j)]$$

where E is the encryption operation and $r(i, j)$ is a random value. Then, the image provider collects the ciphertext values of all pixels to form an encrypted image.

Actually, the proposed scheme is capitable with various probabilistic public-key cryptosystems, such as Paillier [21] and Damgård–Jurik cryptosystems [25]. With Paillier cryptosystem [21], for two large primes p and q, calculate $n = p \cdot q$, $\lambda = \text{lcm}(p - 1, q - 1)$, where lcm means the least common multiple. Here, it should meet that $\gcd(n, (p - 1) \cdot (q - 1)) = 1$, where gcd means the greatest common divisor. The public key is composed of n and a randomly selected integer g in Z_{*n^2}, while the private key is composed of λ and

$$\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$$

where

$$L(x) = (x - 1)/n$$

In this case, implies

$$c(i, j) = g^{m(i, j)} \cdot (r(i, j))^n \bmod n^2$$

where $r(i, j)$ is a random integer in Z_{*n}. The plaintext pixel value can be obtained using the private key

$$m(i, j) = L((c(i, j))^{\lambda} \bmod n^2) \cdot \mu \bmod n.$$

As a generalization of Paillier cryptosystem, Damgård–Jurik cryptosystem can also be used to encrypt the plaintext image. Here, the public key is composed of n and an element g in $Z_{*n^{s+1}}$ such that $g = (1 + n)^j \cdot x \bmod n^{s+1}$ for a known j relatively prime to n and x belongs to a group isomorphic to Z_{*n}, and we may choose d as the private key when meeting $d \bmod n \in Z_{*n}$ and $d = 0 \bmod \lambda$. Then, the encryption in (1) can be rewritten as

$$c(i, j) = g^{m(i, j)} \cdot (r(i, j))^{n^s} \bmod n^{s+1}$$

where $r(i, j)$ is a random integer in $Z_{*n^{s+1}}$. By applying a recursive version of Paillier decryption, the plaintext value can be obtained from the ciphertext value using the private key. Note that, because of the probabilistic property of the two cryptosystems, the same gray values at different positions may correspond to different ciphertext values.

B. Data Extraction and Image Decryption

After receiving an encrypted image containing the additional data, if the receiver knows the data-hiding key, he may calculate the *k*th LSB of encrypted pixels, and then extract the embedded data from the *K* LSB-layers using wet paper coding. On the other hand, if the receiver knows the private key of the used cryptosystem, he may perform decryption to obtain the original plaintext image. When Paillier cryptosystem is used, (4) implies

$$c(i, j) = g^{m(i, j)} \cdot (r(i, j))^n + \alpha \cdot n^2$$

where α is an integer. By substituting into, there is

$$c\_(i, j) = g^{m(i, j)} \cdot (r(i, j) \cdot r\_(i, j))^n \bmod n^2.$$

Since $r(i, j) \cdot r\_(i, j)$ can be viewed as another random integer in Z^*_n, the decryption on $c\_(i, j)$ will result in the plaintext value

$$m(i, j) = L((c\_(i, j))^\lambda \bmod n^2) \cdot \mu \bmod n.$$

Similarly, when Damgård–Jurik cryptosystem is used

$$c\_(i, j) = g^{m(i, j)} \cdot (r(i, j) \cdot r\_(i, j))^{n^s} \bmod n^{s+1}.$$

The decryption on $c\_(i, j)$ will also result in the plaintext value. In other words, the replacement of ciphertext pixel values for data embedding does not affect the decryption result.

C. Reversible Data-Hiding Scheme

This section proposes 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.

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

3.The Wavelet Transform

Wavelets are signals which are local in time and scale and generally have an irregular shape. A wavelet is a waveform of effectively limited duration that has an average value of zero. The term 'wavelet' comes from the fact that they integrate to zero; they wave up and down across the axis. Many wavelets also display a property ideal for compact signal representation: orthogonality. This property ensures that data is not over represented. A signal can be decomposed into many shifted and scaled representations of the original mother wavelet. A wavelet transform can be used to decompose a signal into component wavelets. Once this is done the coefficients of the wavelets can be decimated to remove some of the details. Wavelets have the great advantage of being able to separate the fine details in a signal. Very small wavelets can be used to isolate very fine details in a signal, while very large wavelets can identify coarse details. In addition, there are many different wavelets to choose from. Various types of wavelets are: Morlet, Daubechies, etc. [9, 10]. One particular wavelet may generate a more sparse representation of a signal than another, so different kinds of wavelets must be examined to see which is most suited to image compression.

A wavelet function Ψ(t) has two main properties,

$$\int_{-\infty}^{0} \Psi = (t)dt\ 0;$$

That is, the function is oscillatory or has wavy appearance.

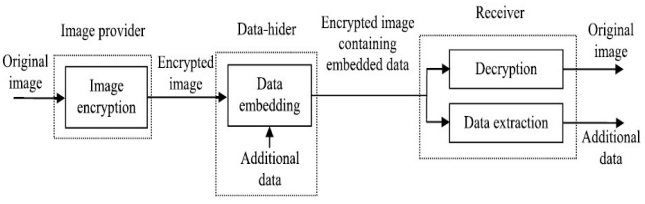
$$\int_{-\infty}^{0} |\Psi(t)|^2 dt < \infty;$$

That is, the most of the energy in Ψ(t) is confined to a finite duration.

IORD Journal of Science & Technology
E-ISSN: 2348-0831
Volume 3, Issue 3 (MAR-APRIL 2017) PP07-12
IMPACT FACTOR 1.719
www.iord.in

4. Proposed Compression Method using DWT

This section illustrates the proposed 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.



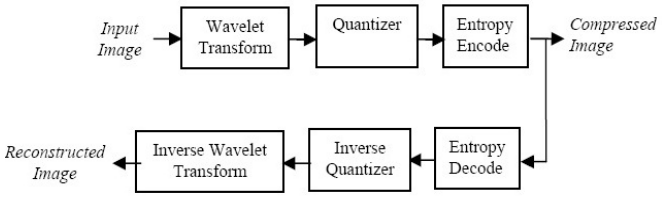


Fig: The structure of the wavelet transform based compression

The steps of the proposed compression algorithm based on DWT are described below:

I. Decompose
Choose a wavelet; choose a level N. Compute the wavelet. Decompose the signals at level N.

II. Threshold detail coefficients
For each level from 1 to N, a threshold is selected and hard thresholding is applied to the detail coefficients.

III. Reconstruct
Compute wavelet reconstruction using the original approximation coefficients of level N and the modified detail coefficients of levels from 1 to N.

5. Experimental Results

Based on the above chapters we have discussed what is histogram and we have seen the basic concept of the embedding a data into a image with the reference of the histogram shifting. So initially starting with the experiment we have chosen two images as shown below, one of the image is bitmap of size 256X256 i.e. Cover Image.bmp and the other one is bitmap of size 32 X 32 i.e. the Secret Image.bmp.

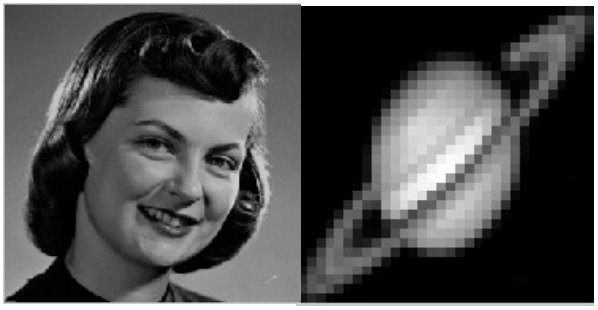


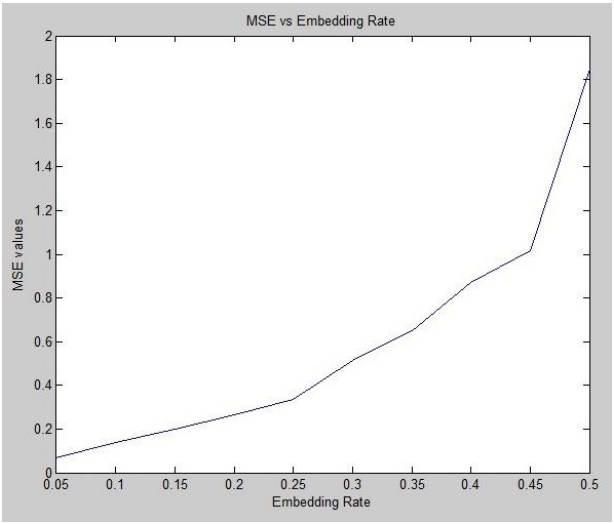
Fig:. (a) Cover images. (b) Secret Image

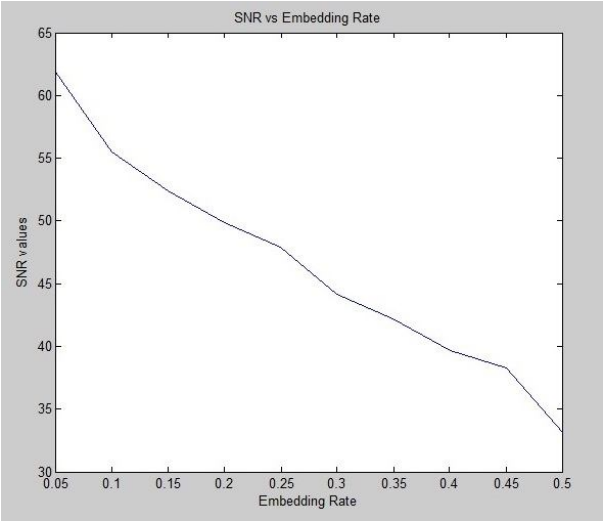
The two images used in the experiment are being called into MATLAB workspace as shown above. The both the images doesn't show much change in their visual apperance but the the embedded image has data embedded into it which can be observed with the help of Bits per pixel (BPP). If we plot a graph between the PSNR and the BPP we can clearly see that what amount of data is hidden in the original image along with the density.

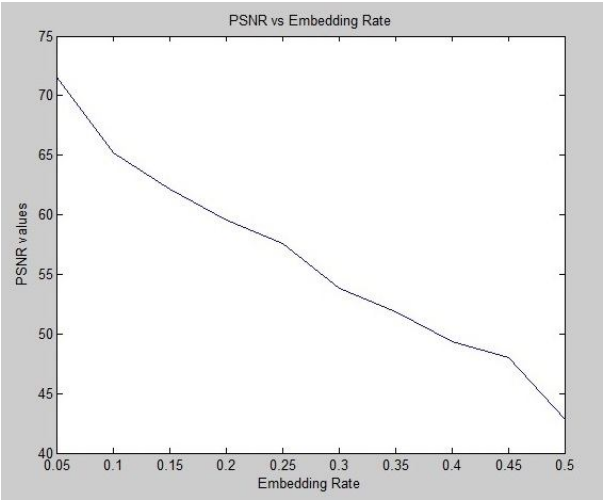
Fig:. (a) Original image (b) Data Hidden Image (c) Final Encrypted Image

Fig:. (a) Encrypted Image (b) Final Decrypted Image (c) Hidden Image

Simulation Results in MATLAB it will ask the bits per pixel range to provide so as per the BPP the density of the embedded data would be hidden inside image. With the histogram shifting method distortion is less when the embedded code rate BPP is less.







The above results indicates the embedding rate (BPP) versus PSNR (dB) which shows that as the embedding rate goes on increasing that will lead decrease in PSNR that means the image will have more distortion as compared to the original image.

With the combined scheme, we implemented the histogram shrink operation with a value of parameter δ, and encrypted the pixels using Paillier cryptosystem. Then, we embedded the first part of additional data into the ciphertext pixel values by the reversible embedding method, and embedded the second part of additional data into the K LSB-planes of the ciphertext pixel values by the lossless embedding method. When having the encrypted image containing the additional data, we first extracted the second part of additional data from the LSB-planes of ciphertext pixel values. After decryption, we further extracted the first part of additional data and recovered the original plaintext image in the plaintext domain. Here, the payloads of the two parts of additional data are same as the payloads of reversible and lossless schemes, respectively, and the quality of directly decrypted image is same as that of reversible scheme.

6. Conclusion

This paper proposes lossless, reversible, and combined data hiding schemes for ciphertext images encrypted by discrete wavelet transform (DWT) and 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.

7. 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.