A Steganography Method for Digital Images using Coefficient Analysis

Po-Yueh Chen[1] Yue-Chi Tseng[2]
Department and Graduate Institute of Computer Science and Information Engineering,
Chaoyang University of Technology[1]
Graduate Institute of Networking and Communication Engineering,
Chaoyang University of Technology[2]
168 Gifeng E. Rd., Wufeng,Taichung County, Taiwan
pychen@mail.cyut.edu.tw[1] s9330615@mail.cyut.edu.tw[2]

Abstract

In this paper, performing image steganography on frequency domain in stead of space domain is analyzed. Image steganography is a new data hiding scheme which protects the essential information embedded in an image. The object is to hide as many bits as possible while maintaining certain image quality (in terms of Peak Signal-to-Noise-Ratio, PSNR). By embedding the essential information in the high frequency parts of the DWT coefficients and keep the low frequency part unchanged, we can exploit the characteristic of DWT and protect the embedded information more securely since human eyes are much less sensitive to high frequency signals.

Keywords: Steganography, DWT, Security

1. Introduction

In this highly digitalized world, the internet serves as an important role for data transmission and sharing. However, since it is a world-wide and publicized medium, some confidential data might be stolen, copied, modified, or destroyed by an unintended observer. Therefore, security problems become an essential issue. Encryption is a well-know procedure for secure data transmission. The frequently used encryption methods include RSA [1], and DES (Data Encryption Standard) [2]. Although these two methods do achieve certain security effects, they make the secret messages unreadable and unnatural. These unnatural messages usually attract some unintended observers' attention. This is the reason a new security approach called "steganography" [3] arises.

For example, steganography may select an image as the medium to hide the secret messages without perceptibly destroying the original image. The selected image is called the "cover-image". The embedded secret data can be of any types, such as images, texts, voices, or just binary codes. The cover-image with the secret message embedded is called the "stego-image". Since the stego-image looks almost the same as the cover image, only the intended receivers are aware of the existence of hided messages. Hence, malicious hackers are kept away from the embedded image. For higher security requirements, we can encrypt the message data before embedding them in the cover-image to provide further protection.

Data hiding methods using images can be categorized into two types, the spatial-domain methods and the frequency-domain one [4]. Applying spatial-domain approaches, the secret messages are embedded in the image pixels directly. They are easy and fast, yet less tolerant to noises. Applying frequency-domain approaches, the sender transform the cover-image into frequency-domain coefficients before embedding secret messages in it. These methods are more complex and slower than the spatial-domain ones. However, they are more secure and tolerant to noises.

We propose in this paper a new frequency-domain approach based on the motivations stated below. When applying Discrete Wavelet Transform (DWT) on an image, 4 sub-bands (namely, LL, HL, LH, and HH sub-bands) are obtained. Since human eyes are much more sensitive to the low frequency part (the LL sub-band), we can hide the secret messages in the other 3 sub-bands to maintain better image quality (in terms of Peak Signal-to-Noise-Ratio, PSNR). Furthermore, the fact that 4 sub-bands are of the same size makes it convenient to embed/extract the messages according to the corresponding coefficients positions. Exploiting this self-similarity characteristic of DWT coefficients, we do not need extra information to keep a track of embedded messages locations. For the security issue, we design a specific embedding procedure so that the secret messages cannot be reconstructed by just assembling the Least Significant Bits (LSBs) [5] of DWT coefficients.

The rest of this paper is organized as follows. Section 2 reviews the relative bibliography and theoretical background. In section 3, the proposed method is described in details step by step. Section 4 demonstrates the experiment results. Finally, the discussions and conclusions are provided in Section 5.

2. Related works

The most frequently used steganography method is the technique of LSB (Least Significant Bits) substitution. The basic concept of LSB substitution is to embed the confidential data at the rightmost bits (bits with smallest weightings) so that the embedding procedure will not significantly affect the original pixel value. The mathematical representation for LSB method is:

$$x_i' = x_i - x_i \bmod 2^k + m_i \qquad (1)$$

In equation (1), x_i' represents the i th pixel value of the stego-image and x_i represents that of the original cover-image. m_i represents the decimal value of the i th block in the confidential data. The number of LSBs to be substituted is k. The extraction process is to copy the k-rightmost bits directly. Mathematically the extracted message is represented as:

$$m_i = x_i' \bmod 2^k \qquad (2)$$

Hence, a simple permutation of the extracted m_i gives us the original confidential data. This method is easy and straightforward. However, when the capacity is greatly increased, the PSNR decreases a lot and hence poor stego-image quality results. Furthermore, the confidential data might be easily stolen by simply extracting the k-rightmost bits directly.

In [6], the authors proposed to use LSB substitution method first. Supposed the ith pixel value of the original image is p_i and the ith pixel value with embedded messages is p_i'. They calculate the difference value as $\delta_i = p_i' - p_i$ and then further segment it into three intervals:

Interval 1 : $2^{k-1} < \delta_i < 2^k$

Interval 2 : $-2^{k-1} \leq \delta_i \leq 2^{k-1}$

Interval 3 : $-2^k < \delta_i < -2^{k-1}$

where k is the number of embedding bits. According to the interval where δ_i lies in, the authors modify p_i' to form the stego-pixel p_i''. Although this method increases the image quality, we have to refer to extra information before extracting the confidential data. It cannot be extracted out from p_i'' directly.

In [7], a spatial domain approach, the authors proposed exploiting the correlation between neighboring pixels for determining the bit number to be embedded at certain specific pixel. Employing the variance between neighboring pixels, it is convenient to estimate whether a pixel is located in edge areas or not. If the pixel is located in edge areas, we can embed more data there than in smooth areas. The approach is categorized into 3 kinds of side match: two-side, three-side, and four-side. As shown in Fig.1, to estimate where a pixel is located in (a smooth area or an edge area), pixels are classified as white or grey. White blocks are the input pixels and gray ones are the neighboring (reference) pixels for correlation estimation.

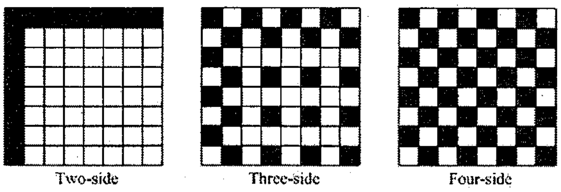


Fig. 1. Three kinds of side-match proposed in [7]

Since the messages are embedded mostly in the edge areas (where the human eyes are less sensitive to), the method increases the image quality (PSNR). However, when cover-images have large smooth areas the capacity becomes very small.

In [8], the authors proposed a frequency domain approach for image steganography. In the system, data hiding (embedding) is realized in bit planes of sub-band wavelets coefficients obtained by using the Integer Wavelet Transform (IWT). To increase data hiding capacity while keeping the imperceptibility of the hidden data, the replaceable IWT coefficient areas are defined by a complexity measure used in the Bit-Plane Complexity Segmentation Steganography (BPCS). To make the proposed system robust enough to some distortion caused by non-ideal communication channel, an Error Control Coding scheme is employed, which can reduce the Bit Error Rate (BER) of extracted hidden data when the stego-image encounters some channel distortion.

Although this lossless data hiding method can reduce the Bit Error Rate of extraction, its high computational complexity cost more processing time. Moreover, since most secret keys have to be embedded before message embedding, the capacity of this method is significantly constrained.

3. Proposed method

In this section, we propose a new frequency domain method for image steganography. The merit is to increase image quality by hiding the messages in HL, LH, and HH sub-bands while keeping LL sub-band invariant. Overview of the proposed method is briefly introduced as follows. At first, the cover-image is transformed into frequency-domain. Haar-DWT [9], the simplest DWT is applied to obtain 4 sub-bands. Secondly, determine how many bits should be embedded in a DWT coefficient according to the magnitude of that coefficient. After the secret messages are embedded, the slightly modified DWT coefficients are transformed back to spatial domain. The resulted stego-image is hence ready for quality evaluation. To extract secret messages from the stego-image, we just perform the algorithm in the opposite direction. The detailed description for both embedding and extraction is provided in the following 2 sub-sections step by step.

3.1 Embedding procedure

Suppose C is the original 8-bit gray-level cover-image of $M_C \times N_C$ pixels. It is denoted as:

$$C = \{x_{ij} \mid 1 \le i \le M_C, 1 \le j \le N_C, x_{ij} \in \{0,1,...,255\}\}$$

S is the n-bit secret message represented as:

$$S = \{s_i \mid 1 \le i \le n, s_i \in \{0,1\}\}$$

Step 1: Apply DWT on C to obtain the frequency-domain matrix H. The 4 sub-bands obtained are denoted as H_{LL}, H_{HL}, H_{LH} and H_{HH} (All 4 sub-bands have the same size of $M_C/2 \times N_C/2$).

Step 2: Normalizing coefficients in H_{HL}, H_{LH}, and H_{HH} sub-bands. After the DWT, coefficients in H_{HL}, H_{LH}, and H_{HH} sub-bands range from -510 to 510. However, in Step 3, it would be more convenient for us to determine the number of embedding bits if the coefficients range is constrained within [-255, 255] (so that the maximum number of embedding bits is 3). Hence, we perform the equation below to achieve normalization.

$$N = \frac{C_{1ij}}{510} = \frac{C_{2ij}}{255} \qquad (3)$$

In equation (3), C_1 represents the original coefficient value in H_{HL}, H_{LH}, and H_{HH} sub-bands and C_2 represents the coefficient value after normalization. A numerical example is demonstrated in Fig. 2.

$$\begin{array}{|c|c|c|c|}\hline -31 & -94 & 66 & 18 \\ \hline -65 & 3 & 90 & 15 \\ \hline 330 & 216 & 2 & 21 \\ \hline -175 & 144 & -21 & 25 \\ \hline \end{array} \quad \Rightarrow \quad \begin{array}{|c|c|c|c|}\hline -15.5 & -47 & 33 & 9 \\ \hline -32.5 & 1.5 & 45 & 7.5 \\ \hline 165 & 108 & 1 & 10.5 \\ \hline -87.5 & 72 & -10.5 & 12.5 \\ \hline \end{array}$$

Fig. 2. An example of normalization

Step 3: Determine the bits of embedding by the formula listed below:

$$n_{ij} = \left\lfloor \frac{1}{2} \log_2 |C_{ij}| \right\rfloor \qquad (4)$$

As we can see in equation (4), the bit number to be embedded at position (i,j) , n_{ij}, increases with the coefficient magnitude C_{ij} which represents the DWT coefficient value at position (i,j) in H_{HL}, H_{LH}, and H_{HH} sub-bands (for example, if $|C_{ij}| < 4$ we embed 1 bit of secret message at position (i,j)).

Step 4: According to the calculated n_{ij} and the Raster-scan order (as shown in Fig. 3.), embed the secrete message coefficient by coefficient.

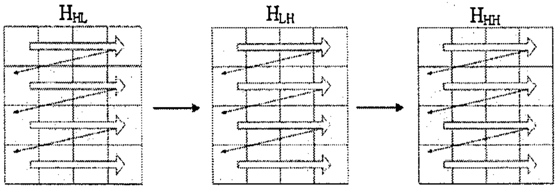


Fig. 3. The embedding order

Step 5: After embedding all message bits, we obtain the slightly modified coefficients matrix H'. By performing the inverse DWT (IDWT) on H', the stego-image E is obtained. However, due to the LSB substitutions, some pixels in E are not integers ranging from 0 to 255. As shown in Fig. 4, we employ a so-called "Key matrix"- K to record the 4 possible non-integer situations (0.0, 0.25, 0.5 and 0.75). The rounded pixel values of E are used to show the stego-image. In order to perfectly reconstruct the secret message bits, K is necessary in the extracting procedure.

$$E = \begin{bmatrix} 173\ \underline{.75} \\ 174\ \underline{.0} \\ 174\ \underline{.25} \\ 174\ \underline{.5} \\ 174\ \underline{.75} \\ 175\ \underline{.0} \end{bmatrix} \Rightarrow K = \begin{bmatrix} \underline{11} \\ \underline{00} \\ \underline{01} \\ \underline{10} \\ \underline{11} \\ \underline{00} \end{bmatrix}$$

Fig. 4. Generation of the Key matrix

Step 6: The rounded version of E, denoted as F, is then stored in a specific image file format while K is filled in the unused tags (for example, the "Description" tag in TIFF format and the "Comment" tag in JPG format). The whole file of the stego-image is then ready for transmission.

3.2 Extracting Procedure

The message extracting is explained as follows. The 8-bit gray-level stego-image of $M_F \times N_F$ pixels is represented as:

$$F = \{y_{ij} \mid 1 \le i \le M_F, 1 \le j \le N_F, y_{ij} \in \{0,1,...,255\}\}$$

Step 1: Extract the Key Matrix from file tag of F as:
$K = \{k_{ij} \mid 1 \le i \le M_F, 1 \le j \le N_F, k_{ij} \in \{00, 01, 10, 11\}\}$
Transform all elements of K into 0, 0.25, -0.5 and -0.25 to form K', which is represented as:
$K' = \{k'_{ij} \mid 1 \le i \le M_F, 1 \le j \le N_F, k'_{ij} \in \{0, 0.25, -0.5, -0.25\}\}$

Step 2: Obtain matrix H' by performing DWT transform on E (which is calculated by F + K', as illustrated in Fig. 5).

$$E\begin{bmatrix}173.75\\174.0\\174.25\\174.5\\174.75\\175.0\end{bmatrix} = K'\begin{bmatrix}-0.25\\0\\0.25\\-0.5\\-0.25\\0\end{bmatrix} + F\begin{bmatrix}174\\174\\174\\175\\175\\175\end{bmatrix}$$

Fig. 5. Reconstruction of E, the accurate matrix

Step 3: Normalize coefficients in H_{HL}, H_{LH}, and H_{HH} sub-bands. Equation (3) is performed.

Step 4: Determine the bits of extracting:

$$n'_{ij} = \left\lfloor \frac{1}{2}\log_2 \left|\mathrm{H}'_{ij}\right| \right\rfloor \tag{5}$$

In equation (5), n'_{ij} represents the number of bit supposed to be extracted (it is actually the same as the n_{ij} in embedding phase) and H'_{ij} represents the high frequency DWT coefficients.

Step 5: According to the calculated n'_{ij} and the Raster-scan order (as shown in Fig. 3.), extract the secrete message bits coefficient by coefficient.

Step 6: At last, cascade the extracted bits and form the whole message bit stream S.

4. Simulation results

In this section we demonstrate the simulation results for the proposed scheme. The performance of the proposed method is compared with those in literature [5], [6], [7] and [8] using Matlab 7.0 for programming.

Four TIFF formatted images "Airplane" (254Kbyte), "Baboon" (258Kbyte), "Boat (256Kbyte), "Lenna" (258Kbyte) are employed as the cover-images. All of them are size of 512×512, 8-bit gray-level images as shown in Fig. 6.

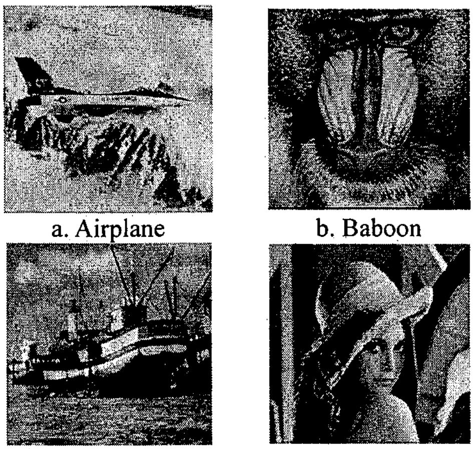

a. Airplane b. Baboon
c. Boat d. Lenna

Fig. 6. Four cover-images

The secret message S applies pseudo-random numbers and is denoted as:
$S = \{s_i \mid 1 \le i \le 900^2, s_i \in \{0,1\}\}$
The performance in terms of capacity (in bit) and PSNR (in dB) are demonstrated for the method in the following sub-sections for performance evaluation.

We employ a pseudo random number generator to produce the secret message bits. The peak signal to noise ratio (PSNR) is used for image quality evaluation. The PSNR of an 8-bit gray-level images is defined as :

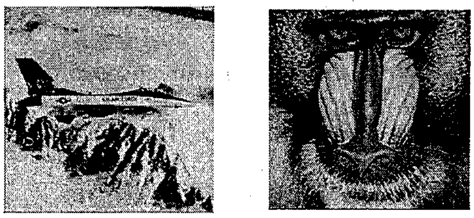
$$PSNR = 10\log_{10}\frac{255^2}{MSE}, \tag{6}$$

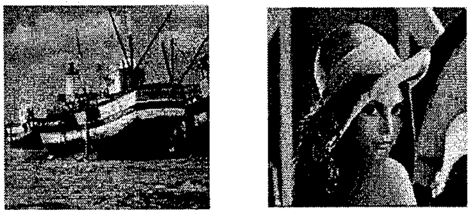
where $MSE = (\frac{1}{M_C \times N_C})\sum_{i=1}^{M_C}\sum_{j=1}^{N_C}(x_{ij} - y_{ij})^2$

x_{ij} and y_{ij} represent the pixel values of the original cover-image and that of the stego-image respectively. The simulation results are exhibited case by case as follows.

4.1 Performance of the proposed method

Four resulted stego-images are show in Fig. 7. And Table1 exhibits the PSNR of the most capacity in the method of four images.


a. Airplane b. Baboon



c. Boat d. Lenna

Fig. 7. Four stego-images

Table 1.Capacity and PSNR of 4 images in proposed method

Image	Capacity	PSNR	File size
Airplane	405,382	48.82	366KB
Baboon	484,135	47.36	366KB
Boat	415,865	48.68	365KB
Lenna	403,802	49.03	367KB
Average	427,296	48.47	366KB

4.2 Performance analysis and comparison

To evaluate the efficiency of the proposed scheme, we employ similar capacity values for all methods and compare the resulted PSNR values as follows. Please refer to Table 2 and Table 3. However, algorithm proposed in [8] is not straightforward to implement and we adopt the results claimed by the authors for comparison as show in Table 4.

Table 2. Comparison with literature [5] and [6]

Case		[5]	[6]	Proposed
Image	Capacity	PSNR	PSNR	PSNR
Airplane	405,382	45.26	47.54	48.82
Baboon	484,135	44.49	46.72	47.36
Boat	415,865	45.03	47.45	48.68
Lenna	403,802	45.30	47.49	49.03

Table 3. Comparison with literature [7]

Images	Boat		Lenna	
Methods	Capacity	PSNR	Capacity	PSNR
Two-sided	413,342	39.42	389,004	41.22
proposed	413,342	48.71	389,004	51.11
Three-sided	271,367	44.32	267,242	45.03
proposed	271,367	51.39	267,242	53.92
Four-sided	166,832	47.85	164,538	48.18
proposed	166,832	53.60	164,538	55.31

Table 4. Comparison with literature [8]

Case		[8]	proposed
Image	Capacity	PSNR	PSNR
Airplane	327,680	40.94	51.35
Baboon	327,680	40.78	51.13
Boat	327,680	40.41	50.79

5. Discussions and Conclusions

In addition to the simulation results displayed in the previous section, we further discuss the message capacity issue, image quality issue, and security issue of the proposed method. Conclusive remarks are provided in the final subsection.

5.1 Discussions

Considering the capacity issue, three 256×256 sub-bands (HL, LH and HH) are available for embedding and the average capacity reaches around 427,296 bits. It is a satisfactory amount for many practical applications.

For quality issue, after transforming the image into frequency domain by DWT, we obtained 4 sub-bands with different importance. The proposed method reserves the coefficients in LL sub-band, the most important ones for an image, and hence increases the PSNR of the resulted stego-image. The other sub-bands stand for horizontal edges, vertical edges, and diagonal edges. Slight modifications on these edge parts of an image do not induce serious degradation in image quality. Considering the worst case in which 3 LSBs in the LH, HL and HH sub-bands are all complemented. That means the new coefficient value differs from the original one by 7. In this worst case, the calculated PSNR is 46.31dB which is still an acceptable value.

For security issue, no user can extracting the secret message S without the knowledge of equation (5) and the embedding order. In addition, the "Key matrix" forms a secure protection as well. Without properly using the "Key matrix", one cannot reconstruct the precise E matrix and its corresponding DWT coefficients. Even somehow the precise E is available, no secret messages can be retrieved directly from the k-rightmost LSBs of the pixels since our method apply frequency domain embedding. Hence, the proposed method does provide satisfactory security.

5.2 Conclusions

In this paper, we proposed a novel and secure image steganography method utilizing the features obtained from DWT coefficients. Quality of embedded images is increased because the secret messages are embedded in the high frequency sub-bands which human eyes are less sensitive to. According to the simulation results, the proposed approach provides fine image quality and enough embedding capacity. Furthermore, respectable security is maintained as well since no message can be extracted without the "Key matrix" and the decoding rules.

Reference

[1] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communication of the ACM*, Vol. 21, no.2, pp.120-126, 1978.

[2] DES Encryption Standard (DES), "National Bureau of Standard (U.S.)", *Federal Information Processing Standards Publication 46, National Technical Information Service*, Springfield, VA, 1997.

[3] B. Pfitzmann, "Information hiding terminology," *Proc. First Workshop of Information Hiding Proceedings, Cambridge, U.K., Lecture Notes in Computer Science*, Vol.1174, pp. 347-350, 1996.

[4] C. C. Chang, T. S. Chen, and L. Z. Chung, "A steganographic method based upon JPEG and quantization table modification," *Information Sciences*, vol. 141, pp. 123-138, 2002.

[5] W. Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for data hiding," *IBM Syst. J. 35 (3-4)*, pp. 313-336, 1996.

[6] C. K. Chan, L. M. Cheng, "Hiding data in image by simple LSB substitution," *Pattern Recognition*, Vol. 37, pp. 469-471, 2003.

[7] C. C. Chang., H. W. Tseng., "A Steganographic method for digital images using side match," Pattern Recognition Letters, Vol. 25, pp. 1431-1437, Jun. 2004.

[8] S. Torres, M. Nakano, H. Perez, "An Image Steganography Systems Based on BPCS and IWT," 16th International Conference on Electronics, Communications and Computers, pp. 51-56, 2006.

[9] Po-Yueh Chen and En-Chi Liao, "A New Algorithm for Haar Wavelet Transform," 2002 IEEE International Symposium on Intelligent Signal Processing and Communication System, pp453-457, 2002.