A Grayscale Image Steganography Based upon Discrete Cosine Transformation

Chin-Chen Chang[1], Pei-Yu Lin[2], and Jun-Chou Chuang[3]

[1]Department of Information Engineering and Computer Science,
Feng Chia University, Taichung 40724, Taiwan.
ccc@cs.ccu.edu.tw

[2]Department of Information Communication,
Yuan Ze University, Chung-Li 32003, Taiwan.
pagelin3@gmail.com.tw

[3]Department of Computer Science and Communication Engineering,
Providence University, Taichung 433, Taiwan.
lzchung@pu.edu.tw

Journal of Digital
Information Management

ABSTRACT: *In this paper, a simple image steganography for secure communication is proposed. Our scheme is based on the discrete cosine transformation (DCT) technique. By using DCT, the most significant information of each DCT secret block can be embedded into the non-significant parts of each DCT cover block. To improve the image quality of the cover image, a quantization factor is used. According to our experiments, the proposed method outperforms the VQ-Based and the HVS-Based image hiding schemes in terms of the image quality of the stego image and the extracted secret image.*

Categories and Subject Descriptors
I.3.3 [Picture/Image Generation]*:* I.3.5 [Image Processing and Computer Vision]: Image Display **I.6.8** [**Discrete Event]**

General Terms: Image hiding schemes, Steganography, Discrete cosine transformation (DCT)

Keywords: Information systems, Steganography, Discrete Cosine Transformation, Human visual system

Received: 23 March 2009; Revised 16 August 2009; Accepted 21 October 2009

1. Introduction

Steganography is a camouflage technique used to hide secret data. Among all multimedia data on the Internet, images are the most popular; therefore, many researchers use digital images as the carrier medium [1-6]. The original image in which we intend to hide the secret image is called the cover image, and the image after embedding is called the stego image. The stego image, which looks like a regular image, can avoid attracting undesired attention during transmission given that there is little distortion between the cover image and the stego image.

Chen et al. [7] have proposed a VQ-based image hiding scheme that employs the vector quantization (VQ) technique [8, 9] to compress the gray-level secret image and embed the results into the gray-level cover image using least significant bits (LSB) substitution. Their scheme can hide a great deal of compressed data, and the quality of the stego image is quite impressive. However, their VQ-Based scheme is time-consuming.

In [10], Chang and Hwang proposed an HVS-based image hiding scheme using the human visual system (HVS) and the dynamic LSB replacement technique. Their scheme extracts some of the most significant bits (MSB) from each pixel of the secret image and puts them into the least significant bits (LSB) of each pixel of the cover image. The HVS is used to determine the number of embedded bits for each cover pixel in the embedding procedure. Thus, each cover pixel can be dynamically replaced with a different number of secret bits. Unfortunately, the scheme requires an extra table.

To balance the encoding time and the quality of retrieved image, this article presents a DCT-based image hiding scheme that embeds one gray-level secret image into one gray-level cover image. The proposed scheme applies DCT [11, 12] for each image block and extracts the most significant DCT values from each transformed secret block. Then, the extracted significant stream is embedded into the non-significant positions of each transformed cover block. For the sake of security, the extracted significant DCT values are quantized and encrypted [14] before they are hidden into the cover image.

The remainder of this paper is organized as follows. In Section 2, we review related works, including VQ-[7] and an HVS-based [10] image hiding schemes. In Section 3, we present our proposed scheme in detail, followed by the experimental results and analysis in Section 4. Finally, Section 5 provides the conclusions.

2. Related Works

2.1 VQ-Based Image hiding Scheme

To obtain the significant medium of the gray-level secret image, Chen et al.'s scheme [7] applies the VQ technique [8, 9] to compress the gray-level secret image. The compressed data can be encrypted by the DES-like cryptosystem, and be embedded into the least significant bits (LSBs) of each cover pixel. Since the secret image is compressed by VQ, the capacity of embedded stream can be reduced. That is, the cover image can be hidden a great deal of compressed image data.

To begin with, a gray-level cover image C and the gray-level secret image S are divided into non-overlapping vectors, respectively, where $C=\{c_1, c_2, \ldots, c_m\}$ and $S=\{s_1, s_2, \ldots, s_n\}$. Here m and n are the numbers of vectors in C and S, respectively. Here, the size of each vector is k.

In the second phase, a codebook is generated from the set of vectors $\{c_1, c_2, \ldots, c_m\}$ of the cover image C, and the size of this codebook is m. Due to that the codebook is directly generated from the cover image, after hiding, the stego image will be a little different from the original cover image. To generate the same codebook in both the encoder and the decoder, they assign the value $2^{(r-1)}$ to the last r bits of each c_{ij}, and then they generate a new set of vectors $\{c'_1, c'_2, \dots, c'_m\}$. Here, c'_{ij} denotes the j-th component value of c'_i. The parameter r refers to the number of modified bits, and it is denoted as

$$r = \left\lceil \frac{2k \times b + n_c \times \left[\log_2 n_S\right]}{mc \times (m_c - 1)} \right\rceil, \tag{1}$$

where b is the number of bits used to represent the content of G and D, and $m_c \times m_c$ is the image size of C. Here G and D are two vectors in a k-dimensional space randomly generated. Equation (1) means $2k \times b \times n_c \times \left[\log_2 \mathrm{n_s}\right]$ bits of the encrypted data will be hidden into the last $m_c \times (m_c - 1)$ pixels of C.

Next, they use a transformation function to project the k-dimensional value of each vector c'_i into a one-dimensional (1-D) value. This transformation function T is as follows.

$$\mathrm{T}(c'_i) = \sum_{i=1}^{k} | c'_{ij} - G_j | \times D_j \tag{2}$$

After finishing the transformation, they sort $T(c'_1)$, $T(c'_2)$, …, and $T(c'_m)$ by their 1-D values. Let the sorted results be $\tilde{c}_1$, $\tilde{c}_2$, …, and $\tilde{c}_m$, where $\tilde{c}_i \le \tilde{c}_{i+1}$. Here $\{\tilde{c}_1, \tilde{c}_2, \dots, \text{and } \tilde{c}_m\}$ is the codebook. The codebook will be used to compress each secret block.

In the third phase, for each s_i, they search for a closest vector $\tilde{c}_h$ from $\{\tilde{c}_1, \tilde{c}_2, \dots, \tilde{c}_m\}$ by using the Euclidean distance and then record the index h into I_q, where $1 \le h \le m$, and $1 \le q \le n$. Let $\{I_1, I_2, \dots, I_n\}$ be the encoding results. In order to protect the $\{I_1, I_2, \dots, I_n\}$, a simple operation ⊕ "exclusive-OR" is used to encrypt the indices. Furthermore, they use a DES-like cryptosystem to encrypt the relative information k, n, G and D. Finally, these encrypted data are hidden into the last r bits of each cover pixel of C. The major strength of this scheme is that the size of the secret image can be larger than that of the cover image. However, the large codebook searching is time-consuming. The image quality of extracted secret image is around 32 dB and leaves plenty of room for improvement.

2.2 HVS-Based Image hiding Scheme

The main idea of [10] is to hide the most significant bits (MSBs) of each secret image pixel into the least significant bits (LSBs) of each cover image pixel. In order to control the image quality of the stego image in perceptibility, the human visual system (HVS) is adopted in their scheme. To protect the secret image, a partial encryption strategy is included to encrypt the significant information.

In the partial encryption phase, only the first three significant bits of each pixel of the secret image are encrypted by using the DES-like cryptosystem. For a gray-level image, each pixel p can be represented by 8 bits $p = b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0$ in the binary form, where $b_i \in \{0,1\}$. The three MSBs are b_7, b_6, and b_5, and the remaining five bits are called the five LSBs. The scheme collects the three MSBs of each pixel in secret image and encrypts them. Let the encryption result of p be $p' = b'_7 b'_6 b'_5 b_4 b_3 b_2 b_1 b_0$.

In the mixing procedure, they use the torus automorphism technique [15] to scramble all secret image pixels, and then the mixed secret image is embedded into the cover image pixel by pixel. In the embedding procedure, a threshold mechanism built upon the human visual system is used to determine the number of bits in each cover pixel to be replaced. For example, given a cover image C with $H_c \times W_c$ pixels and an encrypted, mixed secret image S with $H_s \times W_s$ pixels. Here, $H_s \times W_s \le H_c \times W_c$. Suppose that $S_i = s_{i7}\, s_{i6} \dots s_{i0}$ is a secret pixel and $C_i = c_{i7}\, c_{i6} \dots c_{i0}$ is a cover pixel, where $S_i \in S$ and $C_i \in C$. For each pixel, the r MSBs of S_i are embedded into the r LSBs of C_i, where $r \in \{3, 4, 5\}$ and $i = 1, 2, \dots, H_s \times W_s$. The hiding order in the embedding process is from left to right and top to bottom.

In order to achieve dynamic bit-replacement while keeping the visual quality of each cover pixel under control, the HVS with a threshold T is used to determine the maximum number of LSBs of C_i to be replaced by the same number of MSBs of S_i. The hiding capacity of each cover pixel can be increased to $x_i + r$, where $x_i \in \{0, 1, 2, 3\}$ for $i = 1, 2, \dots, H_s \times W_s$. Unfortunately, their scheme also needs to maintain an extra table to record x_i, and the size of this table is $2 \times H_s \times W_s$. Chang and Hwang's scheme needs to maintain an extra table, which means more storage space has to be taken.

3. The Proposed Method

To achieve better image quality on both the stego image and the extracted secret image without extra storage space, the proposed DCT-based approach hides the most significant DCT coefficients of each DCT secret block into non-significant parts of each DCT cover block. The embedding procedure and extracting procedure are introduced in Subsections 3.1 and 3.2, respectively.

3.1 The Embedding Procedure

Given a gray-level cover image C and a gray-level secret image S of $N \times N$ pixels. Both the images are first divided into equal-sized, non-overlapping blocks, where $C = \{c_1, c_2, \dots, c_{((N \times N)/(8 \times 8))}\}$ and $S = \{s_1, s_2, \dots, s_{((N \times N)/(8 \times 8))}\}$. Here, the block is 8×8 pixels. We apply the discrete cosine transformation (DCT) technique to transform each block into coefficients. The two-dimensional transformation of DCT and IDCT (inverse DCT) are defined as follows:

$$F(u,v) = \frac{C(u)C(v)}{4} \sum_{i=0}^{7} \sum_{j=0}^{7} f(i,j) \cos\left(\frac{(2i+1)u\pi}{16}\right) \cos\left(\frac{(2j+1)v\pi}{16}\right). \tag{3}$$

$$F(i,j) = \frac{1}{4} \sum_{u=0}^{7} \sum_{v=0}^{7} C(u)C(v) f(u,v) \cos\left(\frac{(2i+1)u\pi}{16}\right) \cos\left(\frac{(2j+1)v\pi}{16}\right). \tag{4}$$

Here, $c(u) = c(v) = 1/\sqrt{2}$ for u, $v = 0$; otherwise, $c(u) = \mathrm{c}(v) = 1$. Note that $f(i, j)$ is the pixel value in the spatial domain, and $F(u, v)$ is the DCT coefficient in the frequency domain. Let $\{c'_1, c'_2, \cdots, c'_{((N \times N)/(8 \times 8))}\}$ be the transformation result of O and $\{s'_1, s'_2, \cdots, s'_{((N \times N)/(8 \times 8))}\}$ be the transformation result of S.

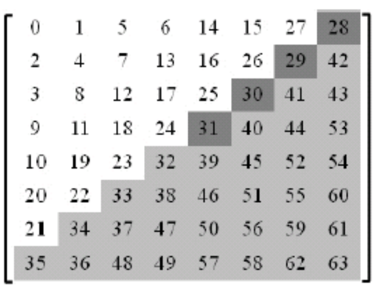
For an 8×8 DCT block, the coefficient located in the (0, 0) position is called the direct current (DC), and the remaining 63 coefficients are called the alternate current (AC). The DC value is the most significant value of this block, and the coefficients located in the low-frequency subband (upper-left positions) contain most of the energy of the DCT block. The remaining energy of the DCT block aggregates near the middle-frequency subband. The energy located in the high-frequency is insignificant, and the coefficient values are almost zero. Therefore, even though we only use the coefficients located in the low-frequency subband, the reconstructed block will be similar to its original.

Taking advantage of the energy distribution property of DCT, we extract L coefficients (one DC value and (L-1) AC values) as the significant information for each secret block s_i'. Each coefficient is extracted in zigzag order. As more coefficients are used, the reconstructed block becomes more similar to the original block. Since the DC and AC values of the edge blocks are usually relatively large, hiding them directly into the DCT cover block would degrade the quality of the stego image. In order to retain the image quality, we employ a quantization factor Q to quantize the L coefficients of each s_i'. Here, the value of the quantization factor is user defined. A small quantization factor can help obtain satisfactory quality of the extracted secret image, but the quality of the stego image will be degraded. On the contrary, a large quantization factor can help archive good quality of stego image but will distort the quality of the extracted secret image.

Considering the original DC value, the maximum value of DC is equal to 2040 ((1/8)×(255×8×8)) when the values of all gray pixels f(0, 0) are 255. By applying quantization, we can use only $[\log_2(2040/Q)]$ bits to represent the quantized DC value. For a DCT block, the DC value is the most significant. To protect the significant quantized DC value, the partial encryption strategy [14] is employed to encrypt all DCs. We encrypt the quantized DC value of s_i' by applying the DES-like cryptosystem [16] with a secret key SK_d. Moreover, to resist the image statistics attack, we then scramble the processed blocks of the secret image by the torus automorphism [15] with a secret key SK_a. Let $\{s_1'', s_2'', \cdots, s''_{((N\times N)/(8\times 8))}\}$ be the permutation result.

In the embedding phase, each s_i'' is sequentially embedded into the corresponding cover DCT block c_i', for i=1, 2, …, (N×N)/(8×8). Observing the DCT domain, the coefficients located at the middle-frequency subband are less significant. We embed the L significant coefficients of s_i'' into the middle-frequency subband and avoid distorting the quality of cover image. The first (64-(L+P-1)) DCT coefficients of c_i' are used to preserve the fidelity of c_i' and remain unchanged. The remaining (L+P-1) DCT coefficients of c_i' are used to embed the L significant coefficients of s_i'' in zigzag order. Here P=[log2(2040/Q) /2] refers to the number of coefficients used to hide the encrypted DC value.

To embed the quantized/encrypted DC value, we start form the zigzag position (64-(L+P-1)) and sequentially select P coefficients of c_i'. Those P coefficients of c_i' can be used to hide the quantized/encrypted DC value of s_i''. Here, we divide the DC value into P segments. That is, each segment consists of two bits. These P segments are embedded into the last two LSBs of the selected coefficients of c_i' using LSB substitution technique. Continuous (L-1) coefficients in the zigzag position (64-(L-1)) of c_i' are directly replaced with (L-1) AC values of s_i'', respectively. Consider the example in Figure 1. When L is 33 wand Q is 10, the initial hiding position is 28 (=64-(L+P-1)), and P is 4. The four dark blocks whose position numbers range from 28 to 31 are used to hide a quantized and encrypted DC value; positions 32 to 63 (gray blocks) are used to hide the quantized AC values.



0	1	5	6	14	15	27	28
2	4	7	13	16	26	29	42
3	8	12	17	25	30	41	43
9	11	18	24	31	40	44	53
10	19	23	32	39	45	52	54
20	22	33	38	46	51	55	60
21	34	37	47	50	56	59	61
35	36	48	49	57	58	62	63

Figure 1. An example of selecting the initial hiding position

Suppose that the set $\{\tilde{c}_1, \tilde{c}_2, \ldots, \tilde{c}_{((N\times N)/(8\times 8))}\}$ is the hiding result. We perform the IDCT on each c_i to obtain a stego image $\tilde{C}$. The stego image $\tilde{C}$ can be directly transmitted to the receiver via an open channel. Here, the parameters L, Q, SK_d, and SK_a are the secret information for the authorized receiver.

3.2 The Extracting Procedure

To extract the gray-level secret image from the received stego image $\tilde{C}$, the decoder needs the following information: a parameter L, a quantization factor Q, and two secret keys SK_d and Sk_a. In the secret extraction phase, it is exactly the inverse of the embedding phase. The N×N-pixel stego image is first divided into non-overlapping 8×8-pixel stego blocks, and then DCT is used to process each stego block. Because those DCT stego blocks have been scrambled, we apply the inverse mixing procedure with a secret key SK_a to re-permute the above blocks. For each re-permute bocks $\tilde{c}_i$, we can extract $[\log_2(2040/Q)]$ bits form the last two LSBs of the selected P coefficients at zigzag position (64-(L+P-1)). Collect these $[\log_2(2040/Q)]$ bits for all blocks, the DES-like cryptosystem with a secret key SK_d is performed to decode them and then generate the original DC value. Subsequently, we can obtain the remaining (L-1) AC values by extracting the (L-1) coefficients at the zigzag position (64-(L-1)) continuously.

With the extracted DC value and (L-1) AC values, the inverse quantization with a quantization factor Q is applied to each secret block. Finally, the 8×8 IDCT is used to decrypted all secret block to learn the constructed secret image $\tilde{S}$.

4. Experimental Results and Analysis

The gray-level images were used as either cover images or secret images with size 512×512 pixels as shown in Figure 2 . The PSNR (peak signal to noise rate) and the human visual system are used in this paper to evaluate the image quality. The PSNR formula is described as follows:

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right)dB\,. \tag{5}$$

The mean square error (MSE) of an image with N×N pixels is defined as

$$MSE = \frac{1}{N\times N}\sum_{i=1}^{N\times N}\left(p_i - p_i'\right)^2\,, \tag{6}$$

where p_i is the original pixel value and p_i' is the processed pixel value.

To demonstrate the proposed scheme, we embed secret images Boat, Jet, and Peppers into cover image Lena as shown in Figures 3(a), (c), and (e), respectively. From the visual perception of these stego images, the proposed scheme can

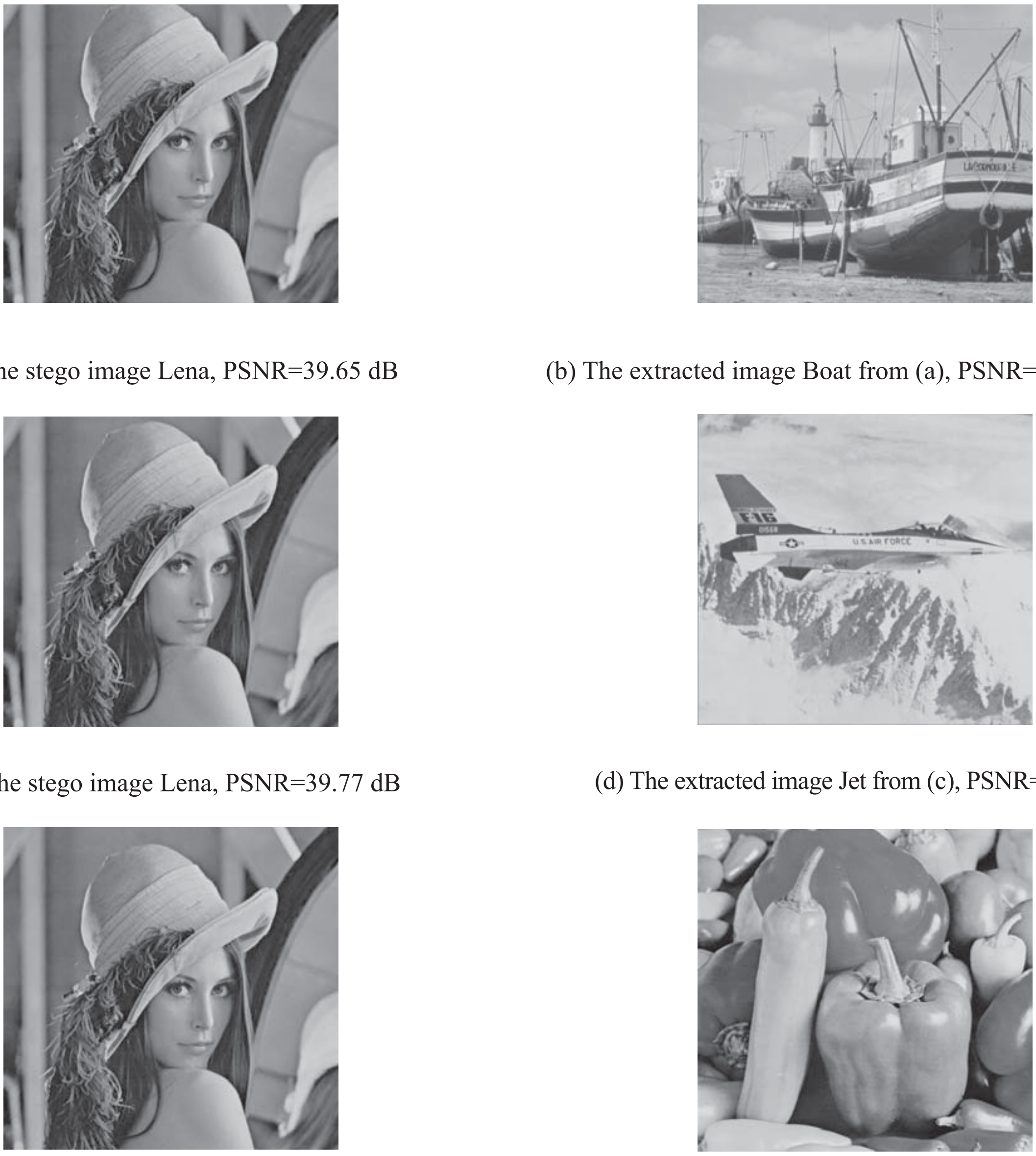
(a) Boat (b) Jet (c) Lena (d) Peppers

Figure 2. The test images

successfully camouflage secret images from intruders. The PSNR values of the stego images are 39.65 dB, 39.77 dB, and 40.00 dB, respectively. Without the loss of generality, it is difficult for people to distinguish the original image from the stego image when the PSNR value is larger than 35 dB. In Figure 3, we can see that the quality of the stego image is satisfactory. An authorized receiver can later extract the secret image from the corresponding stego image. The extracted secret image is shown in Figures 3(b), (d), and (f). The visual quality of the extracted images is satisfactory. Consequently, the proposed scheme can camouflage a secret image into a cover image with satisfactory quality.

The qualities of both the stego image and the extracted secret image depend on parameters L and Q. With a larger L, more significant DCT coefficients are extracted from each secret block, and the reconstructed secret image will be more similar to the original image. However, a large L value decreases the quality of the stego image, because more secret data are embedded into the stego image. Hence, it is a trade-off between the stego image perceptibility and the extracted secret image quality.

The quantization factor Q is the other important parameter. As we use a small quantization factor to quantize the significant coefficient of secret image, more fidelity of the secret image can be preserved. Hence, a small quantization factor is helpful to reconstruct the quality of the extracted secret image. However, the quality of the stego image degrades when the quantization factor gets too smaller, and it may cause a tremble effect on the embedded image. Since we directly replace the coefficients of the cover image with the coefficients of secret image, large coefficients will influence the quality of the stego image. To understand the tremble effect, Figure 4 shows the embedding results of stego images at different quantization factors (Q=1, 10, and 20). We can see that Figure 2(a) has a tremble effect when the quantization factor is smaller than 5. After we select a larger quantization factor, this effect is removed. According to the results, a good quantization factor should be 10 for balancing the qualities of the stego image and the extracted secret image.



(a) The stego image Lena, PSNR=39.65 dB

(b) The extracted image Boat from (a), PSNR=36.28 dB

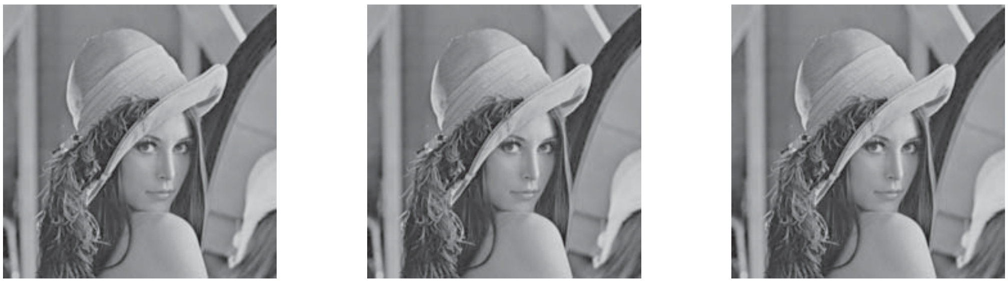
(c) The stego image Lena, PSNR=39.77 dB

(d) The extracted image Jet from (c), PSNR=37.25 dB

(e) The stego image Lena, PSNR=40.00 dB

(f) The extracted image Peppers from (e), PSNR=36.98 dB

Figure 3. The results of cover image Lena, Q = 10



(a) Q=1, PSNR=23.31 dB (b) Q=10, PSNR=39.77 dB (c) Q=20, PSNR=41.43 dB

Figure 4. The stego images with different quantization factors

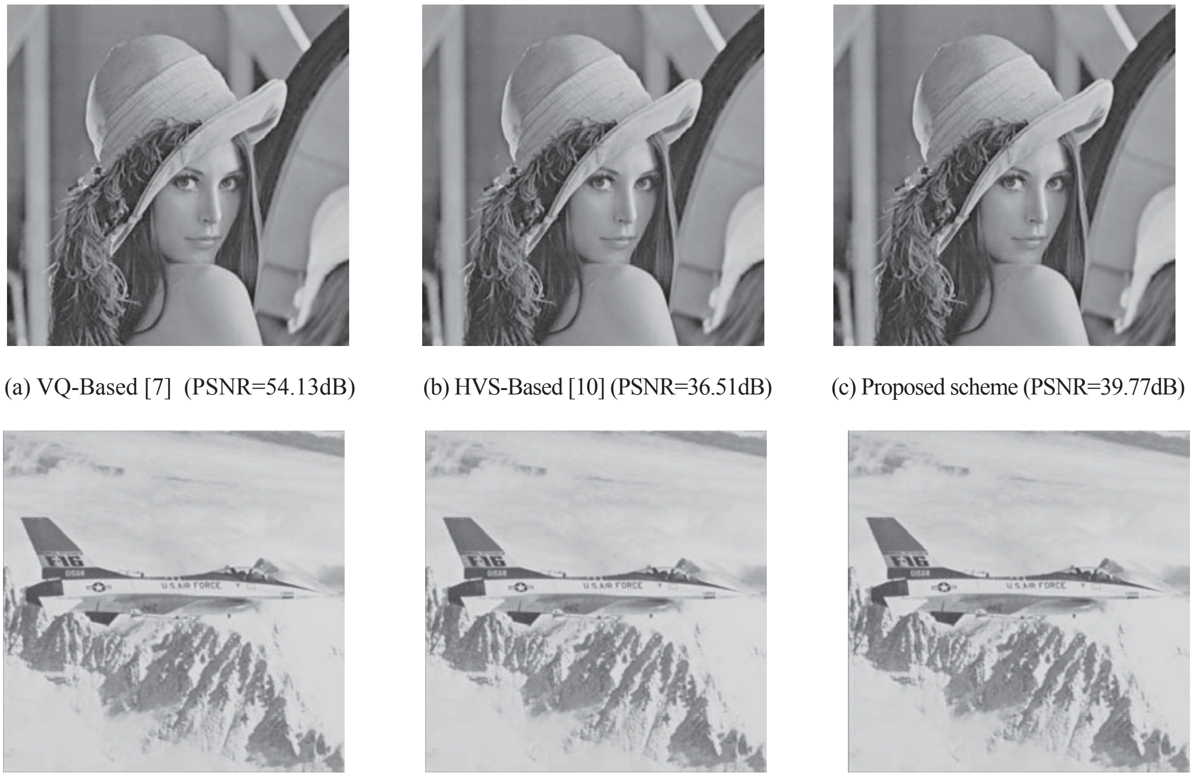
To demonstrate the performance of the proposed scheme, we conducted several experiments to compare the proposed approach with related methods. Here, the two important parameters Q and L were set as 10 and 33, respectively. In the first experiment, the VQ-based scheme [7], HVS-based scheme [10], and the proposed scheme were used to hide one gray-level secret image into one gray-level cover image. Table 1 details the experimental results. As far as the PSNR of the extracted secret image is concerned, the proposed method is better than the VQ-based scheme and the HVS-based scheme. Even though the VQ-based scheme can obtain a higher stego image PSNR value, the image quality of the extracted image is unsatisfactory.

To compare the proposed scheme with [7, 10] in terms of visual quality, we used these schemes to hide a secret image Jet into a cover image Lena. The stego images are shown in Figures 5(a), (b), and (c), and the corresponding extracted secret images are shown in Figures 5(d), (e), and (f). According to Figures 5(a) through (c), the stego PSNRs of [7, 10] and the proposed scheme are around 54.14 dB, 36.36 dB, and 39.11 dB, respectively. Generally, if the PSNR value is less than 35 dB, some important signal characteristics may be lost. While the PSNR value is less than 30 dB, the quality is unacceptable [17]. That is, it is difficult for people to distinguish the original image from the processed image when the PSNR value is larger than 35 dB. Figures 5(d) through (f) show that the visual quality of the reconstructed secret image of the proposed scheme is far better than that of [7, 10]. The experimental results demonstrate that the stego image and the secret image extracted by our scheme can achieve better PSNR values and good visual quality.

Table 2 shows the performance comparison among related schemes [7, 10] and the proposed scheme. The VQ-based scheme proposed by Chen et al. must search for the closest codeword from a large codebook, making it time-consuming. As for our scheme, we employ the DCT technique to transform each image block into a DCT block, so the encoding time is a litter longer than that of the HVS-based scheme but faster than the VQ-based scheme. In [10], they can dynamic embed extra secret bits x_i into the cover pixel according to the human visual system. The quality of the stego image is depends on threshold T. However, [10] needs to maintain

Cover image (512×512)	**Secret image (512×512)**	**VQ-based [7] (*r*=2)**		**HVS-based [10] (*NL*=3, *T*=16)**		**Ours (*Q*=10, *L*=33)**	
		Stego	**Extracted**	**Stego**	**Extracted**	**Stego**	**Extracted**
Boat	Boat	54.12	N/A	36.57	34.45	37.92	36.28
	Jet	54.14	32.57	36.47	33.91	38.01	37.25
	Lena	54.13	33.23	36.78	34.87	38.26	37.58
	Peppers	54.13	32.56	36.55	34.48	38.17	36.98
Jet	Boat	54.14	30.81	36.55	33.89	39.07	36.28
	Jet	54.15	N/A	36.81	33.12	39.26	37.25
	Lena	54.14	32.54	36.63	34.27	39.56	37.58
	Peppers	54.15	30.27	36.51	34.04	39.41	36.98
Lena	Boat	54.14	31.21	36.73	34.03	39.65	36.28
	Jet	54.13	31.96	36.51	33.50	39.77	37.25
	Lena	54.14	N/A	36.78	34.40	40.18	37.58
	Peppers	54.15	32.36	36.63	34.15	40.00	36.98
Peppers	Boat	54.16	30.92	35.62	34.44	38.92	36.28
	Jet	54.15	32.37	35.47	33.94	39.05	37.25
	Lena	54.16	33.71	35.72	34.90	39.36	37.58
	Peppers	54.16	N/A	35.55	34.57	39.23	36.98
	Average	54.14	32.04	36.36	34.18	39.11	37.02

Table 1. Performance comparison in terms of the PSNR values of the stego image and the extracted secret image



(a) VQ-Based [7] (PSNR=54.13dB) (b) HVS-Based [10] (PSNR=36.51dB) (c) Proposed scheme (PSNR=39.77dB)

(d) VQ-Based [7] (PSNR=31.96dB) (e) HVS-Based [10] (PSNR=33.50dB) (f) Proposed scheme (PSNR=37.25dB)

Figure 5. (a)-(c) are the stego images produced by different image hiding schemes, and (d)-(f) are the retrieved secret images by different hiding schemes

	VQ-based [7]	**HVS-based [10]**	**Ours**
Embedded domain	Spatial domain	Spatial domain	Frequency domain
Encoding time	Time consuming	Fast	Medium
Quality adaptable	No	Yes	Yes
Extra storage	No	Yes	No
Image quality of stego image	Good	Low	Medium
Image quality of retrieved image	Low (≈32 dB)	Medium (≈34 dB)	Good (≈37 dB)

Table 2. Performance comparison among the VQ-based scheme, the HVS-based scheme, and the proposed scheme

an extra table with size $2\times H_s\times W_s$ to record the increased bits x_i, which reduces embedding capacity. Compared to [10], the quantization factor Q of the proposed is adaptable and can be set according to the decoder's demand without extra storage.

Image quality is an important requirement for evaluating the performance of image hiding approaches. The scheme [7] can obtain better stego image quality, but the quality of the extracted secret image is unsatisfactory (around 32 dB). The article [10] can achieve better quality than [7] at around 34 dB. To balance the qualities of the stego image and the reconstructed image, we extract the most significant coefficients of the secret image using DCT and then embed it into the less significant coefficients of the cover image. Therefore, the proposed scheme can preserve the quality of the extracted secret image (near 37 dB). Thus, the proposed scheme can obtain better stego image quality and better extracted secret image quality.

The security of our proposed scheme is analyzed as follows. In the partial encryption phase, we apply a DES-like cryptosystem to encrypt all DC values; therefore, the encrypted DC values are secure. Without the key SK_d, it is extremely difficult for anyone to decode the encrypted DC values. Here, we only protect the DC values, because they are the most important. Surely, the security can be improved if we encrypt all secret DCT coefficients. However, since the values of the quantized AC coefficients are usually small, the encryption process may cause the AC coefficients to become too large. Thus, we only protect the DC value of the block, but the remaining AC values may give away the block's information. A complex image block usually contains large AC values, whereas a smooth block does not. An attacker can observe the variation of AC values of each block to obtain an image. To remedy this problem, we use torus automorphism to scramble all of the embedded blocks. Even if the attacker knows the variation of each block, they still cannot figure out the relationships since each block has been re-permuted.

5. Conclusions

This paper provides an image camouflage approach for concealing a secret image into a cover image. To balance qualities of the stego image and the reconstructed secret image, the proposed scheme utilizes the property of DCT subbands to embed the most significant coefficients of the secret block into the non-significant coefficients of the cover block. Because significant data are embedded into non-significant positions, we can make the changes less perceptible. Moreover, the encoder can adjust the qualities of the stego image and the reconstructed image by setting the quantization factor. For security, partial encryption and torus automorphism are applied. Experiments demonstrate that the proposed scheme can achieve satisfactory PSNR value and better quality of the reconstructed secret images than that the VQ- and HVS-based schemes. To preserve the fidelity of the secret image, further research should aim to restore the lossless secret image. That is practical to protect the valuable secret image, such as military and medical images.

References

[1] Hsu, C. T., Wu, J. L. (1999). Hidden digital watermarks in images, *IEEE Transactions on Image Processing*, 8 (1) 58-68.

[2] Chang, C. C., Lin, P. Y. (2008). A color image authentication method using partitioned palette and morphological operations, *IEICE Transactions on Information and Systems*, E91-D (1) 54-61.

[3] Lin, P. Y., Lee J. S., Chang, C. C. (2009). Distortion-free secret image sharing mechanism using modulus operator, *Pattern Recognition*, 42 (5) 886-895.

[4] Chang, C. C., Lin, P. Y., Yeh, J. S. (2009). Preserving robustness and removability for digital watermarks using subsampling and difference correlation, *Information Sciences*, 179 (13) 2283-2293.

[5] Lin, P. Y., Lee, J. S., Chang, C. C. (2009). Dual digital watermarking for internet media based on hybrid strategies, *IEEE Transactions on Circuits and Systems for Video Technology*, 19 (8) 1169-1177.

[6] Chang, C. C., Lin, P. Y., Zang, H., Li, M. C. (2010). A sudoku-based secret image sharing scheme with reversibility, *Journal of Communications*, 5 (1) 5-12.

[7] Chen, T. S., Chang C. C., Hwang, M. S. (1998). A virtual image cryptosystem based upon vector quantization, *IEEE Transactions on Image Processing*, 7 (10) 1485-1488.

[8] Gray, R. M. (1984). Vector quantization, *IEEE ASSP Magazine*, 4-29.

[9] Chang, C. C., Lu, T. C., Ya, J. B. (2007). VQ codebook searching algorithm based on correlation property, *Fundamenta Informaticae*, 76 (1-2) 39-57.

[10] Chang, C. C., Hwang, K. F. (2001). Hiding images using dynamic bit-replacement and human visual system, *In*: *Distributed Multimedia Databases: Techniques and Applications* (T. K. Shin, ed.) Chapter 16, Idea Group Publishing, USA, 190-205.

[11] Cox, I. J., Kilian, J., Leighton, F. T., Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia, *IEEE Transactions on Image Processing*, 6 (12) 1673-1687.

[12] Chang, C. C., Chuang J. C., Chen, T. S. (2002). Recognition of image authenticity using significant DCT coefficients quantization, *Informatica*, 26 (4) 359-366.

[13] Chang, C. C., Lin, P. Y. (2008). Adaptive watermark mechanism for rightful ownership protection, *Journal of Systems and Software*, 81 (7) 1118-1129.

[14] Cheng, H., Li, X. (2000). Partial encryption of compressed images and videos, *IEEE Transactions on Image Processing*, 48 (8) 2439-2451.

[15] Voyatzis, G., Pitas, I. (1996). Applications of toral automorphisms in image watermarking, *In*: *Proceedings of IEEE International Conference on Image Processing (ICIP'96)*, 2. p.237-240.

[16] DES encryption standard (DES). (1997). National Bureau of Standards (U.S.), Federal Information Processing Standards Publication 46, National Technical Information Service, Springfield, VA.

[17] Kyriakopoulos, K., Parish, D. J. (2007). A live system for wavelet compression of high speed computer network measurements, *In*: *Proceeding of Passive and Active Network Measurement*, Lecture Notes in Computer Science, Springer Berlin / Heidelberg, V. 4427, p. 241-244.