Image Hiding Based on a Hybrid Technique of VQ Compression and Discrete Wavelet Transformation

Yen-Ping Chu, Shu-Wei Guo — *Department of Computer Science National Chung Hsing University*

Yung-Kuan Chan — *Department of Management Information Systems National Chung Hsing University*

Hsien-Chu Wu — *Department of Information Management National Taichung Institute of Technology*

Abstract- *Data hiding is to embed the important or secure information into a cover image and thus a stego-image is generated. By transferring the stego-image in public computer networks, the embedded information can be successfully transferred to the receiver. This paper proposes a hybrid technique of VQ compression and discrete wavelet transformation for image hiding. The proposed method compresses the gray-level secret image with VQ compression before the secret image is hidden. Before VQ encoding, a codebook is trained such that the quality of the secret image can be better in encryption and decryption. The compressed data of the gray-level secret image is encrypted and then embedded into the DWT coefficients of the cover image. After inverse DWT calculating, the stego-image is generated. Finally, the sender only needs to transfer the stego-image, two keys, and a set of the initial codewords to the receivers. The secret image can be rebuilt with the received information. If the stego-image is destroyed, the proposed method can also recover the secret image partially.*

Keywords: Vector Quantization, Discrete Wavelet Transformation, Image Compression, Image Hiding, Steganography

1. Introduction

In recent years, computer network and multimedia technology have been developed fast. Information transmission and information sharing are more convenient. However, the security of network is usually not satisfied in common network environment. The important information is easy to be intercepted, modified, or attacked by others who are not authorized in transmission. Thus, it is an important task to avoid important information to be intercepted by unauthorized attackers in transmission. Now, most of researchers focus on how to embed secret data into all kinds of digital media [2-3, 5, 8]. Secret data can be sent to receivers by sending those media which are embedded with the secret data. Thus, when those media are intercepted by unauthorized attackers, they can only get the media but can not detect or decrypt the embedded secret data.

For digital images, image hiding means to embed the secret image into another image. The main purposes of image hiding are to hide the secret image and to avoid unauthorized attackers to use the secret image [3, 5, 8].

In recent years, more and more researchers make their efforts in image hiding field. Some related image hiding methods are proposed [3, 5]. But most of these image hiding methods focus on hiding capacity without considering robustness. This paper focuses on the robustness on resisting compression and noises. The proposed method provides a new image hiding method to compress the secret image and provides a recovery scheme to repair the secret image if the stego-image is destroyed during transmission.

In this paper, Section 2 introduces the related works. VQ compression is discussed in Subsection 2.1 and DWT is discussed in Section 2.2. The proposed method is described in Section 3. Section 4 shows the experiment results and finally, the conclusions are in Section 5.

2. Related works

VQ compression technique is an effective compression method [1-4, 6-7]. Before VQ encoding, it needs to build a codebook. The common codebook generation method is to employ LBG (Linde, Buzo and Gray) algorithm [7] to train the codebook. This section briefly describes the concepts of VQ compression technique in Subsection 2.1. In addition, DWT is described in Subsection 2.2.

2.1. VQ compression

Q is an effective lossy compression method. For encoding an image, first, VQ divides the original image I sized $n\times n$ into several non-overlapped small image blocks $B_1, B_2, ..., B_r$ such that each block has the same size $k\times k$ and $r = n \times n \big/ k \times k$. Each block B_i is then processed individually to find the closest codeword V_i from the codebook CB by calculating the minimal Euclidean distance between B_i and each codeword. Next, use the index p_i of the codeword V_i to substitute B_i. Finally, all image blocks $B_1, B_2, ..., B_r$ are transferred into indices $p_1, p_2, ..., p_r$. Thus, its compression rate is equal to $1/(k\times k)$ product the bit number of an index. Besides high compression rate, another advantage of VQ is that only the mapping blocks will be destroyed when some of the indices of the compressed image are broken.

In VQ decoding process, each index in the compressed data is processed to find the mapping

This research was supported by the National Science Council of the Republic of China under grant NSC 93-2213-E005-012

codeword in the codebook. Then the mapping codewords are combined together to become the recovered image *RI*.

2.2. DWT (Discrete Wavelet Transform)

DWT transforms an image from spatial domain into frequency domain by a series of calculating. The simplest and most frequently used method is Haar DWT. Haar DWT has two processes: vertical process and horizontal process. Suppose I is an image with $m \times n$ pixels and I_{dwt} is the transformed result of I after Haar DWT. Let $C_{i,j}$ be the pixel at the *i*-th column and *j*-th row of I and $C'_{i,j}$ be the transformed coefficient at the *i*-th column and *j*-th row of I_{dwt}. Thus, for 1-level Haar DWT $C'_{i,j}$ is defined as follows:

Vertical process:

$$C'_{i,j} = (C_{2i-1,j}+C_{2i,j})/2, \quad C_{\frac{n}{2}+i,j} = (C_{2i-1,j}-C_{2i,j})/2. \quad (1)$$

Horizontal process:

$$C'_{i,j} = (C_{i,2j-1}+C_{i,2j})/2, \quad C_{i,\frac{n}{2}+j} = (C_{i,2j-1}-C_{i,2j})/2. \quad (2)$$

For each process, the resulted image is divided into high and low frequency bands. The part of addition is in low frequency band, and the part of subtraction is in high frequency band. Low frequency band is denoted as *L*, and high frequency band is denoted as *H*. After 1-level DWT, image I_{dwt} is divided into *4* frequency bands: LL_1, HL_1, LH_1 and HH_1. LL_1 is low frequency band. HH_1 is high frequency band. HL_1 and LH_1 are middle frequency bands between LL_1 and HH_1.

3. The proposed method

The proposed method is divided into two processes: encryption process and decryption process. The two processes are introduced in detail in the following subsections.

3.1. Encryption process

The proposed encryption process includes two procedures: gray-level secret image compression procedure and data hiding procedure. Figure 1 shows the flow chart of the proposed encryption process.

3.1.1. Secret Image Compression Procedure.

The proposed method uses VQ to compress the secret image. In image hiding, if a codeword of the codebook is destroyed, all the referred blocks will be destroyed. Moreover, in order to reduce the quantity of data embedded in the cover image, the proposed method does not embed the codebook into the cover image. Therefore, the codebook training (as shown in Figure 2) of the proposed method picks up fixed images $I_1, I_2, ..., I_n$, which have different color distributions, to become an image pool. Before hiding the secret image, the *t* images $I_1, I_2, ..., I_t$ which have similar color histograms to the secret image will be selected from the image pool to train the codebook. Thus, the codebook trained by these *t* images has similar color distribution to the codebook trained by the original secret image.

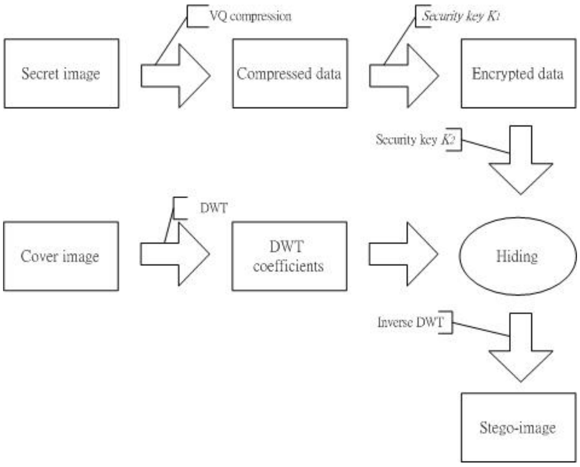


Figure 1: The flow chart of encryption process

Before training the codebook from the selected images $I_1, I_2, ..., \text{and } I_t$, employ LBG algorithm to train *k* blocks from the blocks of the secret image (for example, *k*=16). The blocks of the images $I_1, I_2, ..., I_t$ are divided into *k* groups by the *k* blocks trained from the secret image with *k*-mean. Each block of the image pool calculates the Euclidean distance with the initial *k* blocks. Then, assign each block to the group where the Euclidean distance is minimal.

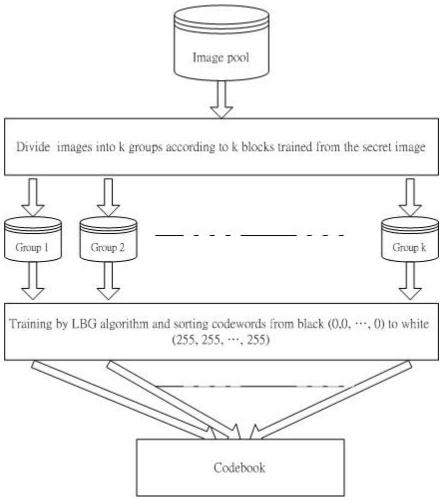


Image pool
Divide images into k groups according to k blocks trained from the secret image
Group 1
Group 2
Group k
Training by LBG algorithm and sorting codewords from black (0,0, ···, 0) to white (255, 255, ···, 255)
Codebook

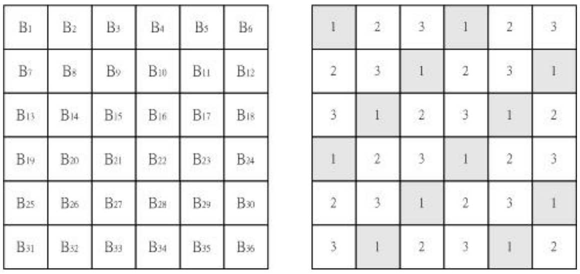
Figure 2: Codebook training with an image pool

Suppose that N_p is the total blocks of the secret image. Then $N_p = \sum_{i=1}^{k} N_i$, where N_i is block number of the *i*-th group when the *k* initial blocks are trained from the secret image. Let there be N_c codewords in the codebook, where N_c is predefined. For each group, there are $N_i / N_p \times N_c$ represented image blocks to be trained by LBG algorithm. Then sort these image blocks from (0, 0, …, 0) to (255, 255, …, 255) by calculating minimal Euclidean distance with (0, 0, …, 0). Finally, combine all represented blocks of each group together to become a codebook.

3.1.2. Data hiding processing.

For considering the security, before hiding the compressed data of the secret image, the proposed method generates a security key K_1. The size of security key K_1 is larger than 512 bits. K_1 is used to be a seed of the pseudo random number generator to generate a binary string S. Then use XOR (exclusive OR) operation on S and each index in the compressed data to generate the encrypted data. Then, the encrypted data can be hided into the cover image.

In order to enhance the robustness, this paper divides the blocks of the secret image into three levels (as shown in Figure 3). The blocks marked by 1 are the most important. The blocks marked by 2 or 3 are minor. When the secret image is hidden, the indices of the 1-marked image blocks should be hidden in the area where the data are not easy to be broken. The indices of the 2-marked or the 3-marked image blocks can be hidden in the place where the data are easier to be broken. Thus, when the indices of the 2-marked or the 3-marked image blocks are broken, they can be predicted by the 1-marked image blocks.



B1	B2	B3	B4	B5	B6
B7	B8	B9	B10	B11	B12
B13	B14	B15	B16	B17	B18
B19	B20	B21	B22	B23	B24
B25	B26	B27	B28	B29	B30
B31	B32	B33	B34	B35	B36

(a)

1	2	3	1	2	3
2	3	1	2	3	1
3	1	2	3	1	2
1	2	3	1	2	3
2	3	1	2	3	1
3	1	2	3	1	2

(b)

Figure 3: (a) Secret image and (b) three levels of image blocks of the secret image

In the proposed method, the cover image I_c is transformed by 1-level DWT. Thus, the transformed I_c is divided into 4 frequency bands: LL_1, HL_1, LH_1 and HH_1. The indices of the 1-marked image blocks of the secret image are hidden in the LL_1 and the indices of the image blocks belonged to be 2-marked and the 3-marked, respectively, are hidden in the HL_1 and LH_1. The proposed method also checks even parity for each hidden index and hides the checking bits into the coefficients of DWT. Figure 4 shows how the encrypted data and checking bits are embedded into the DWT coefficients. The encrypted data is embedded into the position '3' of the DWT coefficient and the checking bit is embedded into the position '2' of the DWT coefficient. For increasing the security of the hidden image, the robust image hiding method based on VQ also uses a security key K_2 to be a seed of the pseudo random number generator. Then use K_2 to decide the starting bit for the hidden indices in DWT coefficients.

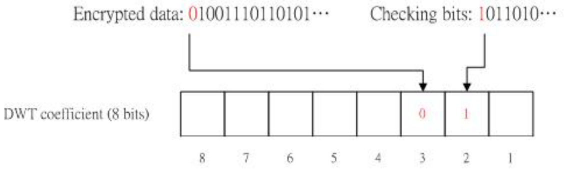


Figure 4: Embedding encrypted data and checking bits into DWT coefficients

Since each pixel is similar to its neighbors in an image, when the checking bits are used to check the embedded indices and some errors are found, the proposed method can predict the error blocks by using other correct blocks around each error one. The DWT coefficients of LL_1 sub-band are usually not easy to be broken by some common used image processing. But the coefficients of HL_1, LH_1 and HH_1 sub-bands do. Thus, when even parity checking bits find some errors of the indices, each mapped error block can be predicted by using the 1-marked blocks around it.

3.2. Decryption process

In the decryption process (as shown in Figure 5), the proposed method uses the same image pool as encryption process to train the codebook. The authorized participants use the keys K_1, K_2 and *k* initial codewords of the secret image to training the codebook. Thus, the codewords of each group are the same as the codewords in the encryption process.

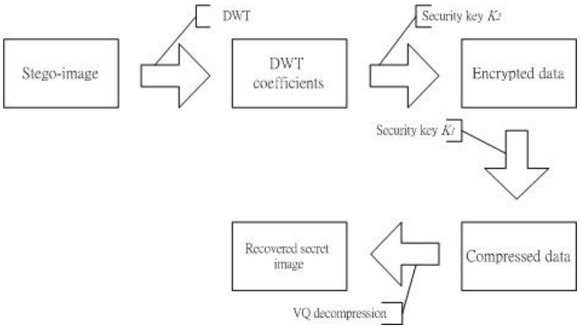


Figure 5: The flowchart of decryption process

In next step, transfer the stego-image I_s with 1-level DWT and decrypt the indices of the secret image from the coefficients of 1-level DWT stego-image I_s with security key K_2. Thus, the encrypted data of the secret image are decrypted from the stego-image. For each encrypted data, use security key K_1 to decrypt it. Thus, the index data is decrypted. For each index, calculate the even parity check-bits to verify if the index is correct.

For the correct indices, use mapped codewords to rebuild the secret image. For the error indices, predict them by the average of the 1-level image blocks around each of the error blocks. Thus, the decryption processing is done.

4. Experimental results

Table 3: The PSNR of the secret image when stego-images are compressed after JEPG lossy compression (unit: dB)

Compression rate*	1.30	1.53	1.91	2.37	2.88
Secret image (recovered)	19.65	17.52	15.71	14.06	12.94
Secret image (modified)	20.45	18.51	16.76	15.01	13.76

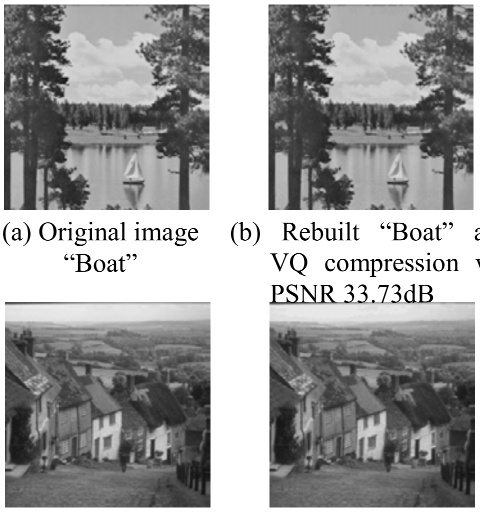
Table 1: The PSNR of the secret images after VQ compression (size: 256×256 pixels)

Images	PSNR
Boat	33.73 dB
Lena	34.49 dB
Gold	35.60 dB
Peppers	34.08 dB
Tiffany	35.89 dB

Table 2: The PSNR of stego-images in the experiment (unit: dB)

Secret image \ Stego-image	Boat	Lena	Gold	Peppers	Tiffany
Boat	34.11	33.99	36.17	33.90	33.90
F16	33.97	33.89	34.16	34.11	33.55
Splash	33.52	33.64	33.87	33.82	32.97
Baboon	34.49	34.40	34.57	34.38	34.33

In the experiment, the size of the cover image and the secret image are 512×512 and 256×256, respectively. The codebook size is 512. There are several images in the image pool, such as Baboon, Peppers, Tiffany, Boat, F16 and Splash, etc. For each secret image, there are 4 images picked from the image pool which color histograms are similar to the secret image and used to train the codebook. Table 1 shows the PSNR of the reconstructed secret images after VQ compression. When the stego-image is not destroyed, the PSNR of the decrypted secret images are equal to Table 1. The secret images before and after VQ compression with the proposed method are shown in Figure 6. The test images used in this paper are shown in Figure 7. The stego-image is shown in Figure 8. The PSNR of the cover image and the stego-image for hiding different secret images in are listed in Table 2. The secret image recovered from the stego-image after JEPG lossy compression can be modified. The PSNR of the secret images before and after modified are listed in Table 3. Figure 9 shows the secret images which is directly rebuilt from stego-images and the recovered secret images after being repaired by referring to the surrounding 1-marked blocks when the stego-images is compressed by JPEG lossy compression with compression rate 41.8%, respectively.



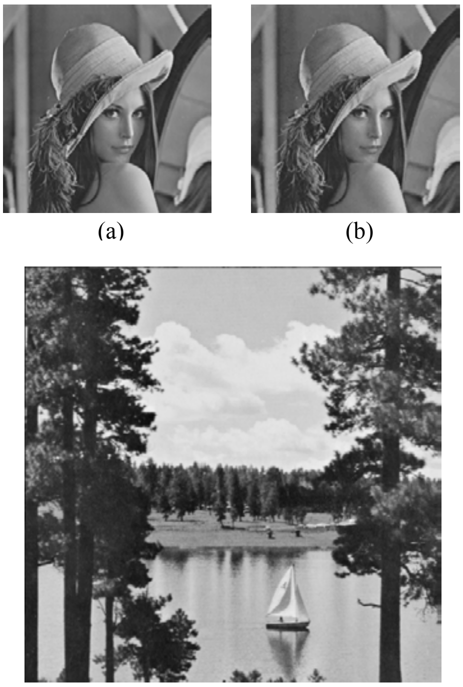
(a) Original image "Boat"

(b) Rebuilt "Boat" after VQ compression with PSNR 33.73dB

(c) Original image "Gold"

(d) Rebuilt "Gold" after VQ compression with PSNR 35.60 dB

Figure 6: VQ compression results



(a)

(b)

(c)

Figure 7: (a) Original secret image "Lena," (b) rebuilt secret image after VQ compression (PSNR=34.49 dB), and (c) cover image "Boat"

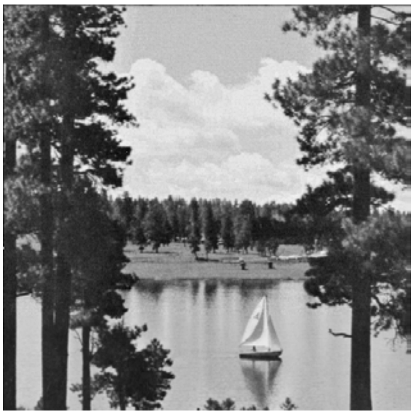
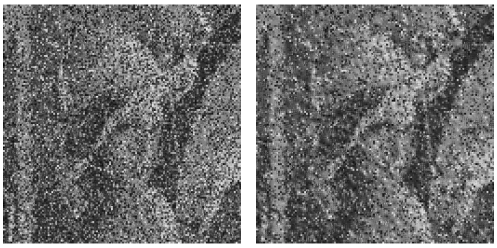


Figure 8: Stego-image "Boat"



(a) Rebuilt secret (b) Recovered secret

Figure 9: Rebuilt secret image from JPEG lossy compressed stego-image (compression rate of the stego-image is $107/256 \times 100\% \approx 41.80\%$)

In the experimental result, the quality of the recovered secret image is more than 33.7(as shown in Figure 11) if the stego-image is not destroyed. If the stego-image is destroyed by JEPG lossy compression, the PSNR of the modified secret images are higher than the recovered secret images. If the compression rate is below 34.50%, the secret image is hard to recovery from the stego-image. It is because the LL band of DWT coefficients is broken when the stego-image is compressed. Thus, the proposed method can improve the quality of the secret image which the stego-image is destroyed.

5. Conclusions

This paper proposes an image hiding method based on VQ compression and DWT. The proposed method improves the enshrouding, security and robustness of image hiding. For the enshrouding, the PSNR of the stego-images are higher than 33dB. For the security, the proposed method needs some information to recover the secret image. The information is transferred to the authorized participants with secure encryption methods, such as DES, in transmission. For the robustness, the secret image can be rebuilt from the JPEG lossy compressed stego-image. The recovered secret image is easier to be recognized than the directly rebuilt secret image. Finally, the proposed method also proposes a new method to train codebook without the original image. Only a few information of the original image is given, then the codebook can be trained with an image pool. Thus, this can be used in many applications based on VQ.

References

[1] C. C. Chang, D. C. Lin, and T. S. Chen, "An Improved VQ Codebook Search Algorithm Using Principal Component Analysis," *Journal of Visual Communication and Image Representation*, Vol. 8, No. 1, 1997, pp. 27-37.

[2] T. S. Chen, C. C. Chang, and M. S. Hwang, "A Virtual Image Cryptosystem Based upon Vector Quantization," *IEEE Transactions on Image Processing*, Vol. 7, No. 10, October 1998, pp. 905-910.

[3] K. L. Chung, C. H. Shen, and L. C. Chang., "A Novel SVD and VQ Based Image Hiding Scheme," *Pattern Recognition Letters*, Vol. 22, 2001, pp. 1051-1058.W. C. Du, and W. J. Hsu, "Adaptive Data Hiding Based on VQ Compressed Images," *IEE Proceedings-Vision, Image and Signal Processing*, Vol. 150, No. 4, 2003, pp. 233-238.

[4] Y. C. Hu, and C. C. Chang, "A Progressive Codebook Training Algorithm for Image Vector Quantization," *The Fifth Asia-Pacific Conference on Communications* (*APCC '99*), Vol. 2, pp. 936-939, 1999.

[5] H. Jiwu, and Y. Q. Shi, "Embedding Gray Level Images," *The 2001 IEEE International Symposium on Circuits and Systems* (*ISCAS 2001*), Vol. 5, 2001, pp. 239-242.

[6] R. Y. Li, J. Kim, and N. Al-Shamakhi, "Image Compression Using Transformed Vector Quantization," *Image and Vision Computing*, Vol. 20, No. 1, January 2002, pp. 37-45.

[7] Y. Linde, A. Buzo and R. M. Gray, "An Algorithm for Vector Quantization," *IEEE Transactions on Communications*, Vol. 28, Jan. 1980, pp. 84-95.

[8] J. S. Pan, F. H. Wang, L. Jain, and I. Nikhil, "A Multistage VQ Based Watermarking Technique with Fake Watermarks," *Lecture Notes in Computer Science*, Vol. 2613, January 2003, pp. 81-90.