LETTER

Secret Image Transmission Scheme Using Secret Codebook

Shih-Chieh SHIE[†a)], **Ji-Han JIANG**[†], **Long-Tai CHEN**[††], *Nonmembers*, *and* **Zeng-Hui HUANG**[†], *Student Member*

SUMMARY A secret image transmission scheme based on vector quantization (VQ) and a secret codebook is proposed in this article. The goal of this scheme is to transmit a set of good-quality images secretly via another high-quality cover image with the same image size. In order to reduce the data size of secret images, the images are encoded by an adaptive codebook. To guarantee the visual quality of secret images, the adaptive codebook applied at the transmitter is transmitted to the receiver secretly as well. Moreover, to enhance the security of the proposed scheme and to compact the data size of the codebook, the adaptive codebook is encoded based on VQ using another codebook generated from the cover image. Experiments show impressive results.

key words: *secret image transmission, vector quantization, adaptive codebook*

1. Introduction

Image hiding techniques have been widely studied in the last decade [1]–[3]. The research of transmitting a set of images secretly via another cover medium has attracted much attention in recent years [4], [5]. A secret image transmission scheme involves embedding multiple secret images into another cover medium at the transmitter. Then, the cover medium convoying the information of secret images is transmitted to the receiver through the communication channel. Finally, the receiver reconstructs the secret images from the received cover medium based on the designed extraction procedure. The visual quality of secret images reconstructed at the receiver should be a main consideration in the secret image transmission scheme. Moreover, the cover medium should be in a meaningful form. That is it should be perceptually imperceptible to human beings.

In prior research [4], [5], vector quantisation (VQ) technique [6] performs well in the applications of simultaneously transmitting a set of secret images. Hu proposed a VQ-based secret image transmission scheme in which several secret images can be simultaneously hidden into another cover image [4]. Hu's scheme provides an impressive improvement on the number of secret images that can be hidden in one cover image. However, the quality of secret images extracted at the receiver is not good enough. To overcome this problem, Lin et al. proposed a novel idea to transmit more secret images via an adaptive codebook [5]. Although the visual quality of the received secret images improves greatly, the cover medium applied in Lin et al.'s scheme is meaningless for human eyes. This drawback may make it less suitable for secret image transmission.

In this article, a new VQ-based secret image transmission scheme which employs an adaptive secret codebook is proposed. The proposed scheme puts emphasis not only on the hiding capacity of cover image but also on the visual quality of secret images and the cover image. Moreover, the secret images are self-extractable at the receiver. That is, the receiver is capable of reconstructing the secret image set independently by using only the received cover image.

2. The Proposed Scheme

The goal of the proposed scheme is to transmit a set of good-quality images secretly and simultaneously through another significant cover image of the same image size. The cover image convoys the whole information that is essential for reconstructing secret images at the receiver. Accordingly, the secret images are self-extractable in the proposed scheme, without using any separately transmitted side information.

In order to simultaneously transmit multiple secret images through another cover image, the data size of the secret image set has to be reduced before it is embedded into the cover image. For this purpose, the traditional VQ technique is applied in the proposed scheme. Assume that the number of secret images to be transmitted is t, the cover image is $\boldsymbol{H}$, and each of these images is composed of $w \times h$ pixels with g levels of color. To reduce the data size of secret images, a codebook $\boldsymbol{C}$ is generated from the secret images and the images are compressed into index set $\boldsymbol{I}_S$ based on the VQ encoding system. Let the size of codebook $\boldsymbol{C}$ be N_C and the codeword of it be composed of $m \times n$ elements. The data size k (in the unit of bit) of codebook $\boldsymbol{C}$ and the data size l (in the unit of bit) of the compressed secret images can be defined by the equations:

$$k = N_C \times m \times n \times \log_2 g \tag{1}$$

$$l = t \times \lceil w/m \rceil \times \lceil h/n \rceil \times \log_2 N_C \tag{2}$$

To enable the receiver to reconstruct secret images independently, the codebook $\boldsymbol{C}$ has to be completely embedded into the cover image. However, considering the embedding capacity of cover image, the data size of codebook $\boldsymbol{C}$ could be too large. Moreover, when good visual quality is

Manuscript received May 7, 2009.
Manuscript revised October 1, 2009.

[†]The authors are with National Formosa University, Yunlin County 632, Taiwan.
[††]The author is with Industrial Technology Research Institute, Hsinchu 31040, Taiwan.
a) E-mail: scshie@nfu.edu.tw

DOI: 10.1587/transinf.E93.D.399

required for the reconstructed secret images at the receiver, the size of codebook $\boldsymbol{C}$ must be enlarged. This will make it impossible to embed the whole codebook, together with the compressed information of multiple secret images, into the cover image while maintain good visual quality for the cover image. To further reduce the data size of codebook $\boldsymbol{C}$, a novel idea of encoding codebook $\boldsymbol{C}$ based on VQ utilizing a codebook $\boldsymbol{B}$ generated from the cover image is proposed. In the proposed scheme, the encoded codebook $\boldsymbol{I}_C$ is called the secret codebook. Instead of codebook $\boldsymbol{C}$, the secret codebook $\boldsymbol{I}_C$ is embedded into the cover image and transmitted to the receiver. Let the size of codebook $\boldsymbol{B}$ be N_B and the codeword size of it be $i \times j$, the data size (in the unit of bit) p of the secret codebook $\boldsymbol{I}_C$ can be defined by the following equation:

$$p = N_C \times \lceil m/i \rceil \times \lceil n/j \rceil \times \log_2 N_B \tag{3}$$

The steps for generating secret codebook $\boldsymbol{I}_C$ is summarized as the followings.

Step 1: Generate codebook $\boldsymbol{C}$ based on the Linde-Buzo-Gray (LBG) algorithm [6] using the secret images as training set.

Step 2: Generate a modified cover image $\boldsymbol{H}^*$ by replacing the least significant bit (LSB) planes of cover image $\boldsymbol{H}$ with a pseudo random bit stream generated by the key s.

Step 3: Generate codebook $\boldsymbol{B}$ using the slightly modified cover image $\boldsymbol{H}^*$ as training set.

Step 4: Encode the codewords of codebook $\boldsymbol{C}$ into secret codebook $\boldsymbol{I}_C$ based on VQ using the codewords of codebook $\boldsymbol{B}$.

Note that the codeword dimension of codebook $\boldsymbol{C}$ is designed to be larger or equal to that of codebook $\boldsymbol{B}$ in the proposed scheme. To secretly transmit a set of good-quality images via a meaningful cover image, the compressed data of secret images $\boldsymbol{I}_S$ and the secret codebook $\boldsymbol{I}_C$, together with the parameters utilized at the transmitter, have to be embedded into the cover image. These parameters include the number of secret images t, the size of image w and h, the color depth of image g, the size of codebook $\boldsymbol{C}N_C$, the codeword dimension m and n of codebook $\boldsymbol{C}$, the size of codebook $\boldsymbol{B}N_B$, the codeword dimension i and j of codebook $\boldsymbol{B}$, and the key s for generating random bit stream. For more security, all of the information is first merged and than encrypted by the advanced encryption standard (AES) encryption system [7] with the cryptographic key x before it is embedded into the cover image. Since AES is a symmetric-key algorithm, the cryptographic key x used in the transmitter is shared with the receiver. Finally, a significant and high-quality stego-image $\boldsymbol{H}^{**}$ which convoys a set of good-quality images secretly is generated. The flow chart of the proposed secret image transmitting scheme at the transmitter is illustrated in Fig. 1.

To reconstruct the secret images at the receiver, the encrypted information is first extracted from the received stego-image $\boldsymbol{H}^{**}$ and then decrypted by the AES decryption system with the cryptographic key x. After the decryption process, all the parameters including t, w, h, g, N_C, m, n, N_B, i, j, and s can be easily obtained. According to the extracted parameters, the slightly modified cover image $\boldsymbol{H}^*$ can be obtained based on the stego-image $\boldsymbol{H}^{**}$ and the key of the random bit stream s. Consequently, the codebook $\boldsymbol{B}$ can be generated based on $\boldsymbol{H}^*$, N_B, i, and j. In addition, the secret codebook $\boldsymbol{I}_C$ can be decoded using the codebook $\boldsymbol{B}$, N_C, m, and n. Finally, the secret images can be reconstructed by using the decoded secret codebook $\boldsymbol{C}^*$ and the image parameters t, w, h, and g. Therefore, the secret images are self-extractable at the receiver. The flow chart of the proposed secret image transmitting scheme at the receiver is illustrated in Fig. 2.

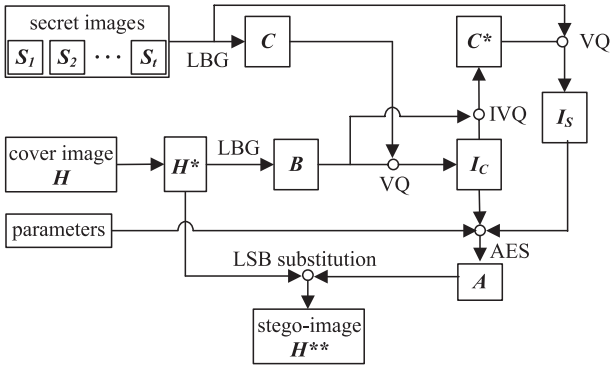

Fig. 1 Flow chart of the proposed secret image transmission scheme at the transmitter.

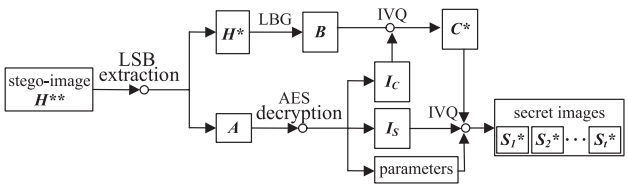

Fig. 2 Flow chart of the proposed secret image transmission scheme at the receiver.

3. Simulation Results

The proposed secret image transmission scheme has been conducted on a set of standard images to verify its performance. In the experiment, the images are with size 512×512 pixels and 256 levels per pixel. To guarantee the visual quality of secret images, the size of codebook $\boldsymbol{C}$ is set to be 512 and the codeword dimension is 4×4. Moreover, to reduce the data size of secret codebook $\boldsymbol{I}_C$ while retain the codebook quality, the size of codebook $\boldsymbol{B}$ ranges from 1024 to 16384 and the codeword dimension is 2×2. Consequently, the overall data size of secret codebook $\boldsymbol{I}_C$ ranges from 31.25% to 43.75% of the original data size of adaptive codebook $\boldsymbol{C}$.

To demonstrate the performance of the proposed secret image transmission scheme, some of our simulation results are provided here. Table 1 lists the comparison between our scheme and Hu's scheme [4] in terms of the peak signal-to-noise ratio (PSNR) values of the reconstructed se-

Table 1 Performance comparison (in PSNR) between the proposed scheme and Hu's scheme [4].

Test images	Cover image	Secret images			
	Airplane	Lena	Pepper	Toys	Average
[4]	45.324	31.072	30.948	30.567	30.862
Proposed	45.275	32.672	32.792	32.796	32.753

cret images and the cover image. Note that both of the two schemes accomplish the same goal in this performance comparison. That is to transmit the three secret images (Lena, Pepper and Toys) simultaneously through the cover image (Airplane) under the restriction of modifying at most two LSBs of cover image pixels. In this experiment, the sizes of codebooks $\boldsymbol{C}$ and $\boldsymbol{B}$ are 512 and 16384, respectively. In addition, the number of bits for representing all the parameters, including t, w, h, g, N_C, m, n, N_B, i, j, and s, is 154 bits for the proposed scheme. Therefore, the embedded bits of our scheme is about 460 kilo-bits while that of Hu's scheme is about 480 kilo-bits. That is the embedded bits of the proposed scheme and Hu's scheme are almost the same.

As shown in Table 1, the proposed scheme provides a significant improvement on the visual quality of the extracted secret images at the receiver and the averaged improvement over [4] is 1.89 dB. In addition, the visual quality of stego-image of the proposed scheme is similar to that of Hu's scheme. For evaluation by human eyes, the stego-image, together with the secret images, obtained at the receiver is illustrated in Fig. 3. Note that the covering capacity (the maximum number of secret images that can be covered by one image) of the proposed scheme is nearly the same as that of Hu's scheme. Therefore, the proposed scheme outperforms Hu's scheme in the aspect of secret image quality.

For more performance comparison, the comparison between the proposed scheme and Lin et al.'s scheme [5] in terms of the appearance of stego-medium received by the receiver is given Fig. 4. Note that both of the two schemes achieve the identical goal of transmitting five secret images (Lena, Pepper, Boats, Goldhill and Toys) simultaneously via another cover medium with data size equals 256 kilo-bytes (KB) in this experiment. The averaged PSNR value of the five secret images achieved by our scheme is 32.91 dB while the one achieved by Lin et al.'s scheme is 32.38 dB. That is the visual quality of secret images obtained by the two schemes is almost the same when the same number of secret images is transmitted. To compare the proposed scheme with Lin et al.'s scheme, three LSBs of each cover image pixels have to be modified for convoying the information of the five secret images and the secret codebook. However, the stego-medium of our scheme is a meaningful image with high visual quality (PSNR = 35.73 dB) while that of Lin et al.'s scheme is a meaningless data stream. Therefore, the proposed scheme outperforms Lin et al.'s scheme in the aspect of visual quality of stego-medium.

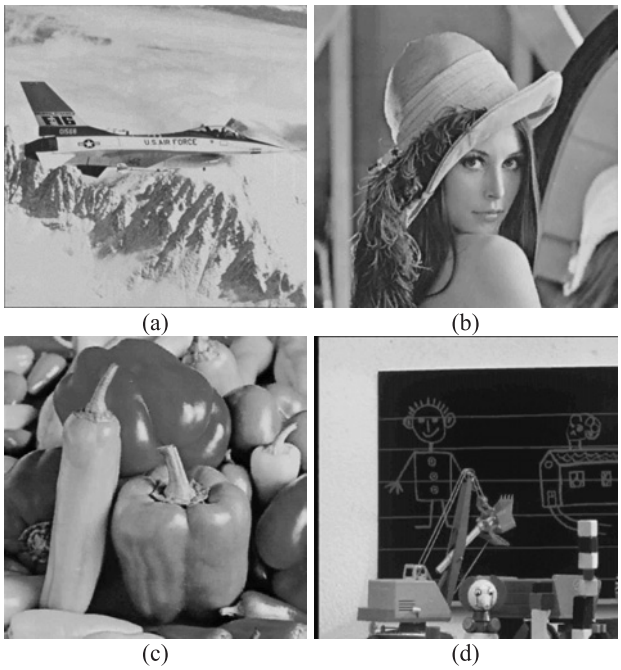

Fig. 3 (a) Stego-Airplane, PSNR = 45.275 dB, (b) the extracted secret image "Lena", PSNR = 32.672 dB, (c) the extracted secret image "Pepper", PSNR = 32.792 dB, and (d) the extracted secret image "Toys", PSNR = 32.796 dB.

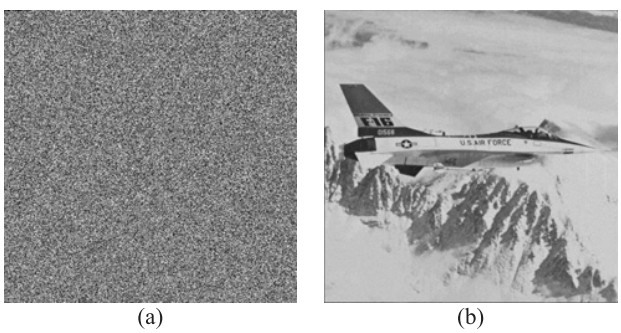

Fig. 4 Performance comparison on the visual quality of stego-media. (a) Lin et al.'s scheme [5], and (b) the proposed scheme.

To show the robustness of proposed scheme against steganalysis, we apply the Chi-square steganography test program [8] provided by Guillermito[2] on our stego-images. Figure 5 illustrates an example of the test results. Fig. 5 (a) shows the Chi-square result of the original cover image while Fig. 5 (b) shows the Chi-square result of the stego-image. Note that the Chi-square steganography test is a kind of statistical attack. In the steganalysis result, the red curve is the result of the Chi-square test while the green curve is the average value of the LSBs. As shown in Fig. 5, the red curve for the stego-image is similar with that for the original image. In addition, the green curve for the stego-image is more variable than that for the original image. Therefore, the proposed scheme withstands the Chi-square steganography test.

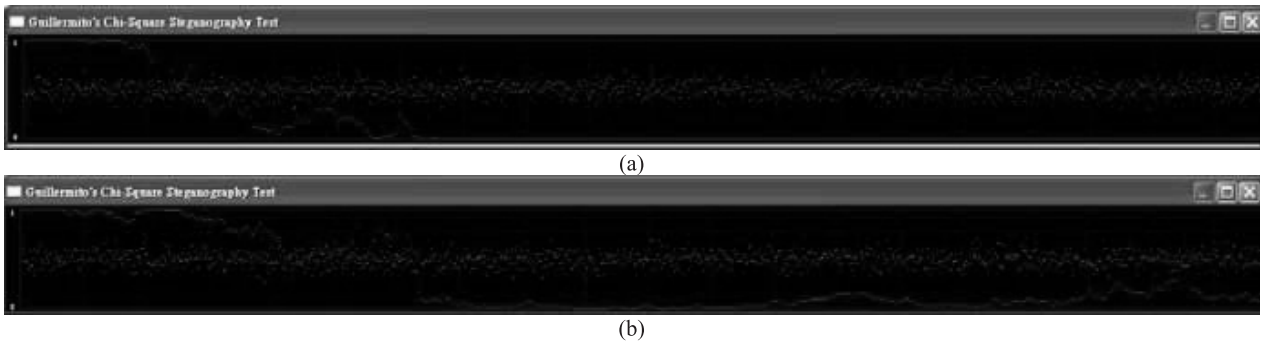

Fig. 5 Experimental results of statistical attack on the proposed scheme using Chi-square steganography test. (a) Chi-square result of the original cover image, and (b) Chi-square result of the stego-image.

4. Conclusions

A novel secret image transmission scheme based on VQ and secret codebook has been introduced in this Letter. The proposed scheme provides significant improvement not only on the visual quality of extracted secret images but also on the appearance of stego-medium. In addition, the covering capacity of the proposed scheme is comparable with that of earlier works. Moreover, the secret images are all self-extractable at the receiver. In summary, the proposed scheme outperforms Hu's scheme and Lin et al.'s scheme because of the following reasons. (1) The adaptive codebook of secret images is applied in the image encoding procedure. (2) The performance of the adaptive codebook is well-preserved by using another codebook generated from the cover image. (3) The data size of secret images and secret codebook is greatly reduced by the VQ technique. (4) The security of secret images is enhanced by applying a secret codebook and incorporating the AES encryption technique in the proposed scheme. And (5) the encrypted information of secret images and secret codebook is embedded in the cover image based on the LSBs substitution technique. According to the provided simulation results, we conclude that the proposed scheme is feasible for secret image transmission.

References

[1] T.S. Chen, C.C. Chang, and M.S. Hwang, "A virtual image cryptosystem based upon vector quantization," IEEE Trans. Image Process., vol.7, no.10, pp.1485–1488, 1998.
[2] Y.K. Chiang and P. Tsai, "Steganography using overlapping codebook partition," Signal Process., vol.88, no.5, pp.1203–1215, 2008.
[3] S.C. Shie, S.D. Lin, and C.M. Fang, "Adaptive data hiding based on SMVQ prediction," IEICE Trans. Inf. & Syst., vol.E89-D, no.1, pp.358–362, Jan. 2006.
[4] Y.C. Hu, "Gray-level image hiding scheme based on vector quantisation," Electron. Lett., vol.39, no.2, pp.202–203, 2003.
[5] S.D. Lin and S.C. Shie, "Secret image communication scheme based on vector quantisation," Electron., Lett., vol.40, no.14, pp.859–861, 2004.
[6] Y. Linde, A. Buzo, and R.M. Gray, "An algorithm for vector quantizer design," IEEE Trans. Commun., vol.28, pp.84–95, 1980.
[7] National Technical Information Service, "Specification for the advanced encryption standard (AES)," Federal Information Processing Standards Publication, no.197, Springfield, U.S.A., 2001.
[8] Guillermito, "Chi-square Steganography Test Program," http://www.guillermito2.net/stegano/tools/index.html