# Secret Image Sharing based on Vector Quantization

Lee Shu-Teng Chen, Wei-Kai Su, and Ja-Chen Lin

***Abstract*—**This paper proposes an ($r$, $n$) threshold secret image sharing scheme based on Vector Quantization (VQ). By using the host images as the VQ codebooks, the VQ indices of the secret image is computed and then shared among the $n$ shadows. The created $n$ shadows and the mixed information of the VQ codebooks are hidden in the original host images to form the $n$ stego images. During the recovery phase, the secret image with VQ quality can be reconstructed by any $r$ of the $n$ stego images. The proposed method is therefore missing-allowable since $n$-$r$ stego images can be lost in the recovery phase. Experiments show that the qualities of our stego images and recovered images are all acceptable. Moreover, the proposed method is secure because it is unlikely to reveal the secret image if less than $r$ stego images are intercepted.

***Keywords*—**Cryptography, data hiding, missing-allowable, secret sharing, vector quantization.

## I. Introduction

COMPUTER network is very popular nowadays. They are useful in both communication and entertainment. People can transmit information through computer network easily. However, because of the open environment of network, attackers may steal or destruct the information transmitted in the network. Losing some data such as family photos is usually of no big deal, but some other information such as company financial budget or military map is so important that losing them will cost much money or even lives. Due to the risk of being hacked, people develop the cryptography methods to encrypt the important data [1]-[9]. For example, Data Encryption Standard (DES) [1], RSA [2], and Advanced Encryption Standard (AES) [3] are all famous cryptography methods still being used nowadays. The cryptography methods mentioned above are based on the so-called key(s). In other words, only the person who has the key(s) can extract the secret data.

L. S. T. Chen is with the Department of Computer Science and Information Engineering, National Chiao Tung University, Hsinchu, Taiwan, R.O.C. (corresponding author to provide phone: +886-3-5712121; e-mail: stlee@cs.nctu.edu.tw).

W. K. Su was with the Department of Computer Science and Information Engineering, National Chiao Tung University, Hsinchu, Taiwan, R.O.C. He is with the Department of R&D, Huper Laboratories Company, Limited, Taipei, Taiwan, R.O.C. (e-mail: gis92548@cis.nctu.edu.tw).

J. C. Lin is with the Department of Computer Science and Information Engineering, National Chiao Tung University, Hsinchu, Taiwan, R.O.C. (e-mail: jclin@cis.nctu.edu.tw).

Besides using the key(s), the other way to protect data is using the secret sharing technology [10]-[20]. Blakley [10] and Shamir [11] firstly proposed the ($r$, $n$) threshold secret sharing schemes. The user can use their polynomial schemes to share the secret data among the $n$ shadows. The $n$ shadows may then be distributed to $n$ different persons. If the user needs the secret data, he or she must collect at least $r$ shadows ($r \le n$) to recover the secret. The ($r$, $n$) threshold scheme assures that collecting at least $r$ shadows can reconstruct the secret data; however, if obtaining less than $r$ shadows, these shadows reveal nothing about the secret data. The method proposed by Shamir [11] can also be used for secret image sharing. The values of the pixels in a secret image are treated as the secret data. Using Shamir's method can share the secret image among the $n$ shadows, and collecting any $r$ of the $n$ shadows can recover the secret image. However, the $n$ shadows use a lot of storage space because each one is of the same size as the original secret image. Therefore, Thien and Lin [12] extended the idea of Shamir's scheme [11] to share the secret image. The size of each shadow in [12] is $1/r$ of that of the original secret image. This benefit lowers the storage space or transmission time. To reduce the size of each shadow further, Lin and Tsai [13] applied Discrete Cosine Transform (DCT) to transform the secret image from the spatial domain to the frequency domain, and then shared the first DCT coefficient of each transformed block; Wang and Su [16] used Huffman coding to encode the difference image of the input secret image, and the generated Huffman bitstream was then shared.

Because each shadow in almost all sharing methods looks like noisy rather than natural images, some data hiding schemes [21]-[31] may be applied to generate the stego images by hiding the noise-like shadows in some host images. Among the data hiding schemes, the simplest one is the Least Significant Bit (LSB) substitution scheme. It replaces the least $t$ bits of the host images by the secret data (the value of $t$ depends on the size of the host image and secret data, usually $1 \le t \le 4$). Later, Wang *et al*. [21] designed a moderately-significant-bit hiding method by the use of optimal substitution process and local pixel adjustment. Wang *et al*. [22] also presented a hiding scheme by using Genetic Algorithm. Thien and Lin [24] proposed another hiding method based on modulus operation by modifying LSB method. Both the theoretic results and the vision quality in [24] are better than those of simple LSB substitution method and GA-improved method. Wu and Tsai [23] introduced an image hiding method by using a difference value of two consecutive pixels in the host image. Chang *et al*. [30] proposed an image

hiding method based on search order coding [32] and modulus function.

However, each stego image in [21]-[30] is often two or four times larger than each shadow. Therefore, Wu *et al.* [31] used the sharing method in [12] and S-E table to reduce further the size of stego images. Notably, Vector Quantization (VQ) [33] is a simple image compression method to reduce the redundancy of a digital image by encoding a block of pixels with an index pointing to a similar block stored in a VQ codebook (the VQ codebook can be created by using algorithms such as the LBG algorithm [34], and some researchers [35]-[37] have developed the methods to speed up the generation of the VQ codebooks). By using VQ, although the image sacrifices its quality, the size of the shadows can be reduced to the smaller ones. Therefore, before sharing, the user may apply the VQ technique to compress the secret image, and the generated VQ indices are shared instead of the pixel values of the secret image. This will cause the sharing worthier because the data amount is reduced.

There are two major ways to share the secret image based on VQ. The first one [38] is that the user provides some host images, and the VQ codebooks are constructed using the first (8-$t$) bit-planes of the host images (assume that the gray levels of the pixels of the host images are in the range 0 to 255, i.e., there are 8 bit-planes in each host image). Then the user compresses the secret image by VQ with the constructed codebooks to generate the VQ indices. The obtained VQ indices are hidden in the last $t$ bit-planes of these host images to form the stego images. In the recovery phase, the user must collect all of the stego images. Then, the VQ codebooks and VQ indices can be, respectively, extracted from the first (8-$t$) and last $t$ bit-planes of the stego images to recover the secret image. Because the size of the VQ indices is much smaller than that of the secret image, the VQ indices can be hidden more easily. Besides, the quality of the recovered secret image is also not bad. However, there is a drawback in [38], namely, if one of the stego images is damaged or lost, the user cannot reconstruct the VQ codebook, and hence, recovering the secret image becomes impossible.

The other one [39] is that the user shares the VQ codebook among the $n$ shadows by Shamir's ($r$, $n$) threshold scheme, and the VQ indices of secret image are kept in a local storage unit. Thus if the user collects any $r$ of the $n$ shadows, the VQ codebook can be reconstructed. Then, by the recovered codebook and the VQ indices saved in the local storage unit, the user can reveal the secret image. Unlike Chen and Chang's method [38], Chang and Hwang's method [39] is missing-allowable. The VQ codebook in [39] can always be recovered as long as the number of the broken shadows is at most $n$–$r$. However, the quality of the recovered secret image in [39] is not as good as that in [38].

In order to archive the missing-allowable ability while maintaining the quality of the recovered secret image, an ($r$, $n$) threshold secret image sharing scheme based on VQ is proposed in this paper. The rest of this paper is organized as follows. Sec. Ⅱ reviews the related works. Sec. Ⅲ presents the proposed method. Sec. Ⅳ provides the experimental results. Finally, Sec. Ⅴ draws a conclusion.

### NOMENCLATURE

| | |
|---|---|
| $n$ | the number of created shadows |
| $r$ | the predefined threshold value where $2 \le r \le n$ |
| $t$ | the number of bit-planes in the host image where $1 \le t \le 4$ |
| $A$ | the VQ codebook generated by the first (8-$t$) bit-planes of the first host image |
| $B$ | the VQ codebook generated by the first (8-$t$) bit-planes of the second host image |
| $C$ | the VQ codebook generated by the first (8-$t$) bit-planes of the third host image |
| $X_1$ | the mixed information of the codebooks $A$ and $B$ |
| $X_2$ | the mixed information of the codebooks $B$ and $C$ |
| $Y_1$ | the mixed information of the codebooks $A$, $B$, and $C$ |

## II. RELATED WORKS

In this section, VQ technique [33] and Thein and Lin's secret image sharing scheme [12] are briefly reviewed in Sec. Ⅱ-*A* and Sec. Ⅱ-*B*, respectively, to provide some necessary background knowledge.

### *A. VQ*

VQ is a lossy image compression technique. It has a simple structure, especially in the decoding phase. Fig. 1 shows an encoding example of VQ. First, an input image is divided into several non-overlapping blocks of four by four pixels each. Then, each block is mapped to the most similar codeword of the codebook, and the VQ index of the mapped codeword is recorded. After processing all blocks, the input image is represented by the VQ indices. In the decoding phase of VQ, as shown in Fig. 2, the VQ compressed image is reconstructed by mapping each VQ index to the codeword of the codebook.

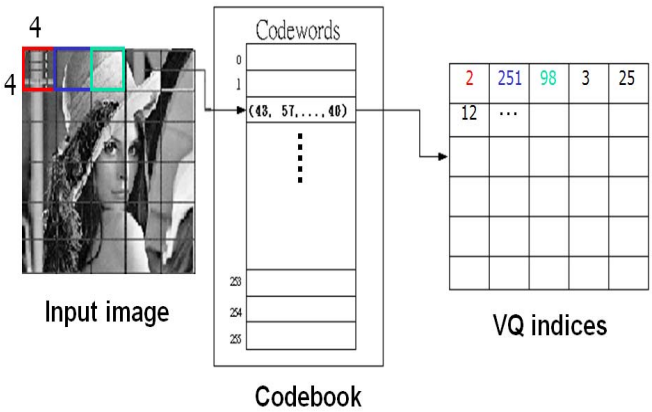


Fig. 1 an encoding example of VQ

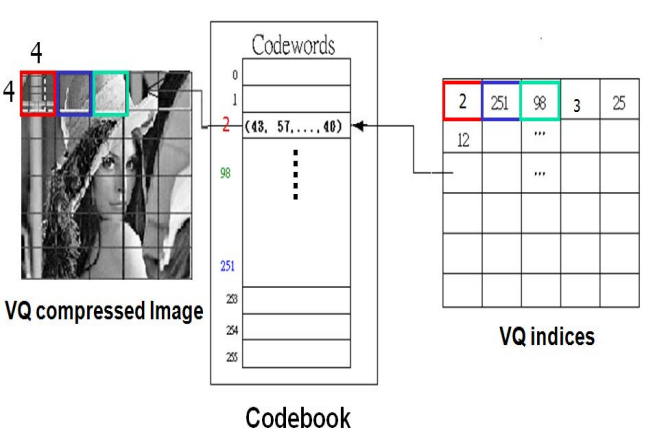


Fig. 2 a decoding example of VQ

### B. *Thien and Lin's Secret Image Sharing Scheme*

In Thien and Lin's ($r$, $n$) threshold scheme, an input gray-level secret image is partitioned into several non-overlapping sectors, and each of which has $r$ pixels. For each sector, the sharing polynomial is defined as

$$p(x) = (a_0 + a_1 x + a_2 x^2 + \ldots + a_{r-1} x^{r-1}) \bmod 251. \quad (1)$$

Here, $a_0, a_1, \ldots$, and $a_{r-1}$ are the gray values of the $r$ pixels of each sector. The $n$ values $p(1), p(2), \ldots$, and $p(n)$ are calculated and then sequentially attached to the $n$ shadows. After processing all sectors, the $n$ shadows for the secret image are created. Since each $r$ pixels contributes only one pixel to each shadow, the size of which is only $1/r$ of the original secret image. In the recovery phase, when collecting any $r$ of the $n$ shadows, sequentially take one not-yet-processed pixel from each of the $r$ shadows. Then, use these $r$ pixels to solve for the $r$ coefficients $a_0, a_1, \ldots$, and $a_{r-1}$ in Eq. (1) by Lagrange interpolation (see [12]). After processing all pixels of the $r$ shadows, the secret image can be obtained.

## III. The Proposed Method

The flowchart of the proposed encoding process is as illustrated in Fig. 3. First, the proposed encoding method uses any $r$ out of the $n$ input host images to construct the $r$ codebooks for VQ. Next, the VQ indices of the secret image are computed by VQ with these $r$ codebooks. Then, the generated VQ indices are shared among the $n$ shadows by Thien and Lin's ($r$, $n$) threshold scheme [12]. Finally, the created $n$ shadows and the mixed information of the $r$ codebooks are hidden in the $n$ input host images to form the $n$ stego images. Later, as shown in Fig. 4, when collecting any $r$ of the $n$ stego images, the VQ indices and codebooks can be extracted from the $r$ stego images to recover the secret image. The details of the proposed encoding and decoding processes are described in Sec. Ⅲ-*A* and Sec. Ⅲ-*B*, respectively.

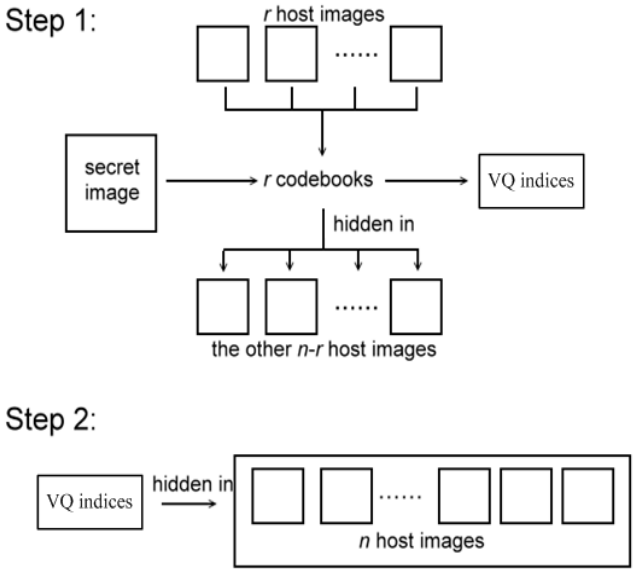


Fig. 3 the flowchart of our encoding method

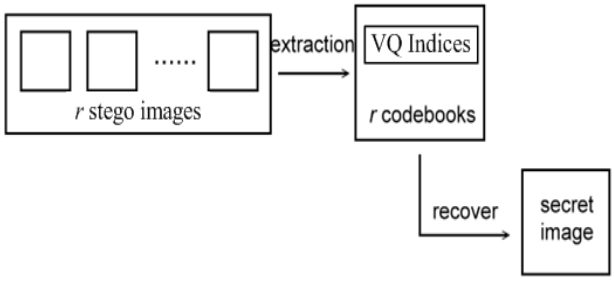


Fig. 4 the flowchart of our decoding method

### A. *Encoding*

Without loss of generality, suppose that the numbers of the host images and the VQ codebooks needed in our method are $n$=5 and $r$=3, respectively. In other words, collecting any $r$=3 stego images will be enough to reveal the secret image. The flow of the generation, sharing, and hiding of the VQ indices is as shown in Fig. 5. In the $n$=5 input host images, which all look like normal images, the first (8-$t$) bit-planes of the first, second, and third host images are, respectively, used to generate the $r$=3 VQ codebooks *A*, *B*, and *C*. Then, the VQ indices of the input secret image are computed by VQ [33] with the three created VQ codebooks. The generated VQ indices are shared by using Thien and Lin's ($r$=3, $n$=5) threshold scheme [12] among the $n$=5 shadows. After obtaining the $n$=5 shadows, they are, respectively, hidden in the last $t$ bit-planes of the $n$=5 input host images by using $t$-LSB substitution scheme.

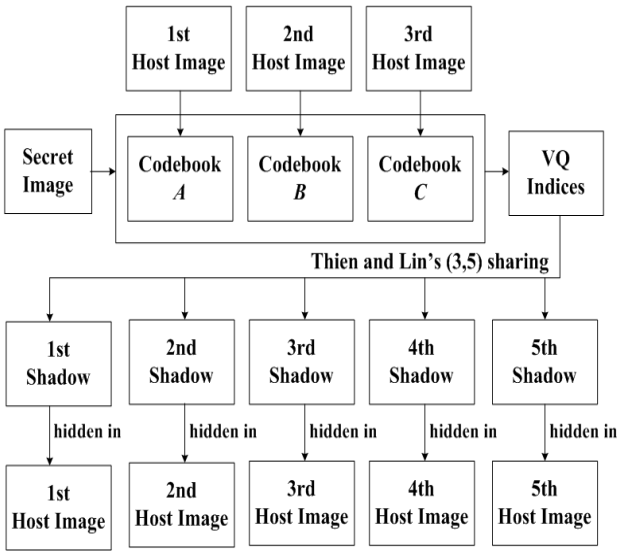


Fig. 5 the flow of the generation, sharing, and hiding of the VQ indices

As for the fourth and fifth host images, which are not utilized to generate the codebooks *A*, *B*, and *C*, they store not only the shadows of the VQ indices, but also the mixed information $X_1$, $X_2$, and $Y_1$ of the generated codebooks. Assume that each of the three codebooks *A*, *B*, and *C* is of the same size *N*. The mixed information $X_{1,j}$, $X_{2,j}$, and $Y_{1,j}$ for the codeword *j* ($0 \le j < N$) in the codebooks *A*, *B*, and *C* are calculated by the exclusive-OR operations as

$$X_{1,j} = A_j \oplus B_j. \tag{2}$$

$$X_{2,j} = B_j \oplus C_j. \tag{3}$$

$$Y_{1,j} = A_j \oplus B_j \oplus C_j. \tag{4}$$

Notably, the exclusive-OR operations can be set arbitrarily as long as they guarantee that the three VQ codebooks can be recovered when any *r*=3 stego images are received. For example, the mixed information $X_{1,j}$, $X_{2,j}$, and $Y_{1,j}$ generated by equations (5)-(8), instead of equations (2)-(4), can also be used as the hidden data in the fourth and fifth host images.

$$X_{1,j} = B_j \oplus C_j. \tag{5}$$

$$X_{2,j} = A_j \oplus B_j. \tag{6}$$

$$Y_{1,j} = A_j \oplus C_j. \tag{7}$$

$$Y_{2,j} = B_j \oplus C_j. \tag{8}$$

After processing all codewords in the codebooks *A*, *B*, and *C* by equations (2)-(4), as shown in Fig. 6, the generated mixed information $X_1$ and $X_2$ are hidden in the fourth host image, and $Y_1$ is hidden in the fifth host image. The fourth and fifth host images will look like the original host images if the size of the generated codebooks are not too huge. For example, in a 512×512 gray-level host image, it only needs about *t*=1 bit-plane to hide the mixed information $X_1$ and $X_2$ of the codebooks *A*, *B*, and *C* each which contains 256 16-dimension codewords.

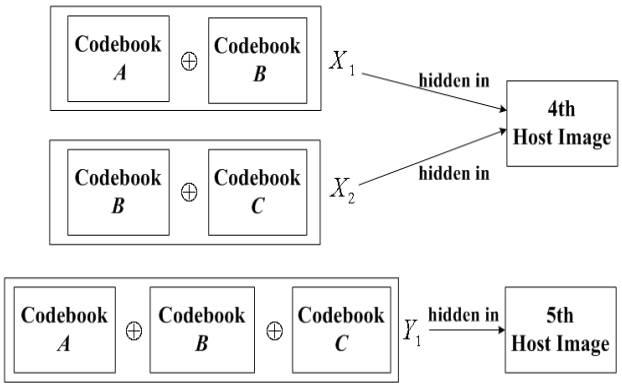


Fig. 6 the flow of the generation and hiding of the mixed information $X_1$, $X_2$, and $Y_1$ of the three VQ codebooks *A*, *B*, and *C*

### *B. Decoding*

When collecting any *r*=3 of the *n*=5 stego images, the secret image with VQ quality can be recovered. The decoding process consists of two phases: the reconstruction of the VQ indices and the reconstruction of the three VQ codebooks. For the reconstruction of the VQ indices, the three shadows can be, respectively, extracted from the last *t* bit-planes of any three of the five stego images. Then, the three obtained shadows are used to reveal the VQ indices by using the linear combination of Lagrange polynomials (see [12]).

As for the reconstruction of the three VQ codebooks *A*, *B*, and *C*, if the three stego images do not include the fourth and fifth ones (recalling that the fourth and fifth stego images contain the mixed information of the three codebooks, and the mixed information is calculated by the exclusive-OR operations), then the codebooks *A*, *B*, and *C* can be directly generated by the first (8-*t*) bit-planes of the three stego images. However, if one of the three stego images is the fourth or fifth one, only two VQ codebooks can be directly created, and the other one codebook is computed by applying the exclusive-OR operations. For example, as shown in Fig. 7, if the three stego images are, respectively, the first, second, and fourth ones, then the codebooks *A* and *B* can be directly created by using the first (8-*t*) bit-planes of the first and second stego images. As regards the codebook *C*, the mixed information $X_2$ is extracted from the last *t* bit-planes of the fourth stego images, and the codebook *C* is computed by

$$C = B \oplus X_2. \tag{9}$$

Similarly, as shown in Fig. 8, if the three stego images are the second, third, and fifth ones, then the codebooks *B* and *C* are directly obtained by using the first (8-*t*) bit-planes of the second and third stego images. The operations to obtain the codebook

$A$ become

$$A = B \oplus C \oplus Y_1. \tag{10}$$

Moreover, if two of the three stego images are the fourth and fifth ones, then only one codebook can be directly generated. The other two codebooks still can be computed by the exclusive-OR operations similarly. As a remark, if only one or two stego images are collected, it is unlikely to reveal the VQ indices even if the information of the VQ codebooks is sufficient.

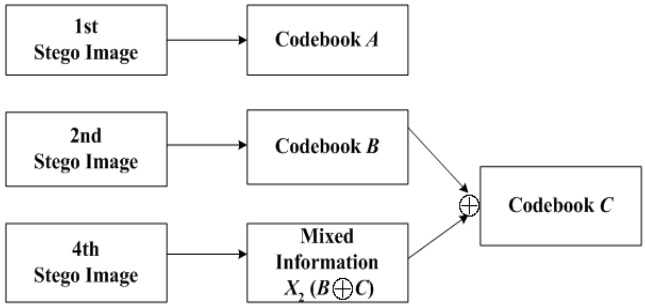


Fig. 7 the reconstruction of the three VQ codebooks when receiving the first, second, and fourth stego images

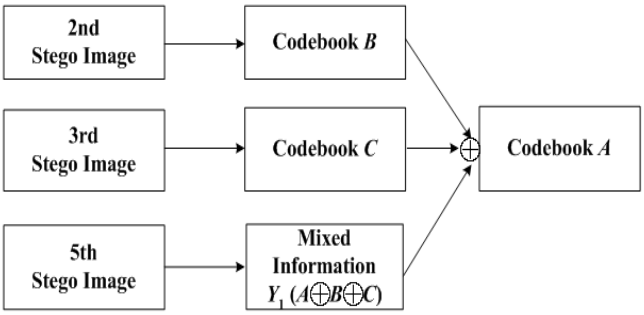


Fig. 8 the reconstruction of the three VQ codebooks when receiving the second, third, and fifth stego images

## IV. Experimental Results and Security Analysis

### A. Experimental Results

In the first experiment, the 1024×1024 gray-level secret image Lena and five 512×512 gray-level host images, Jet, Baboon, Peppers, Boat, and House are tested. The image quality is estimated by the peak signal-to-noise ratio (PSNR), which is defined as

$$\mathrm{PSNR} = 10\log_{10}\frac{255^2}{\mathrm{MSE}}. \tag{11}$$

Where the mean square error (MSE) for a gray-level image of $P\times Q$ pixels is defined by

$$\mathrm{MSE} = \left(\frac{1}{P\times Q}\right)\sum_{x=1}^{P}\sum_{y=1}^{Q}(z_{xy} - z'_{xy})^2. \tag{12}$$

Here, the pixel values of the original image and the stego image (or recovered image) are denoted as $\{z_{xy}\}$ and $\{z'_{xy}\}$, respectively.

Fig. 9 shows the original secret image Lena. Figs. 10(a)-10(e) display the five host images. The first seven bit-planes of the three host images Jet, Baboon, and Peppers are, respectively, used to generate the three codebooks for VQ. The VQ indices of the secret image Lena are computed by VQ and then shared among the five shadows by using Thien and Lin's ($r$=3, $n$=5) threshold scheme [12]. After obtaining the five shadows, they are, respectively, hidden in the last bit-plane of the five host images (Figs. 10(a)-10(e)). Besides, the mixed information of the three generated codebooks is also hidden in the last bit-plane of the two host images Boat and House. Figs. 11(a)-11(e) shows the five resulting stego images, and the PSNRs of them are 52.70, 52.71, 52.69, 48.87, and 50.34 dB, respectively. After collecting any $r$=3 of the $n$=5 stego images in Fig. 11, the recovered image Lena' (PSNR = 34.01 dB) is shown in Fig. 12. The qualities of our stego images and recovered image are all acceptable.

In the second experiment, the secret image is the 1024×1024 gray-level image Cameraman shown in Fig. 13, and the five host images are still the 512×512 gray-level host images in Fig. 10. After generating the VQ indices for Cameraman, they are shared among the five shadows. The obtained five shadows are then embedded together with the mixed information of the codebooks (created in the first experiment) into the five host images in Fig. 10. The five resulting stego images are shown in Figs. 14(a)-14(e), and the PSNRs of them are 52.84, 52.85, 52.84, 48.84, and 50.2 dB, correspondingly. Later, when obtaining any three of the five stego images in Fig. 14, the recovered image Cameraman' (PSNR = 30.11 dB) is displayed in Fig. 15.

Fig. 9 the original 1024×1024 secret image Lena

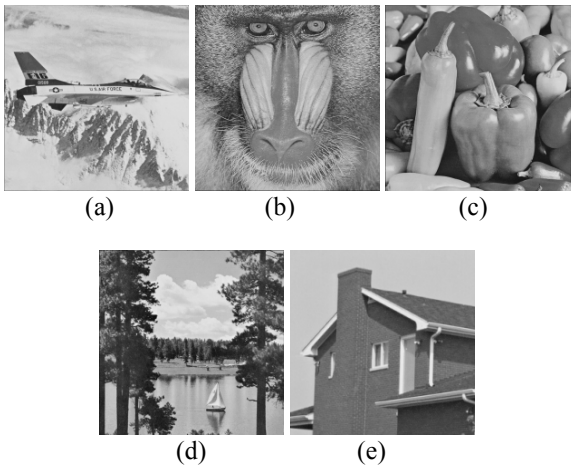


Fig. 10 the five 512×512 host images: (a) Jet; (b) Baboon; (c) Peppers; (d) Boat; and (e) House

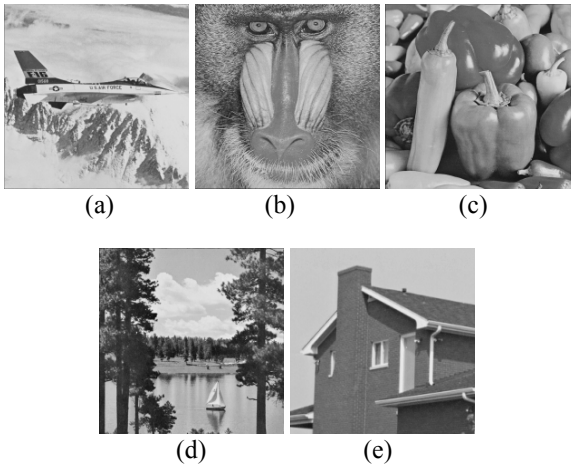


Fig. 11 the five 512×512 stego images, and the PSNRs of them are 52.70, 52.71, 52.69, 48.87, and 50.34 dB, respectively

Fig. 12 the recovered image Lena' (PSNR = 34.01 dB) by any $r$=3 of the $n$=5 stego images in Fig. 11

Fig. 13 the original 1024×1024 secret image Cameraman

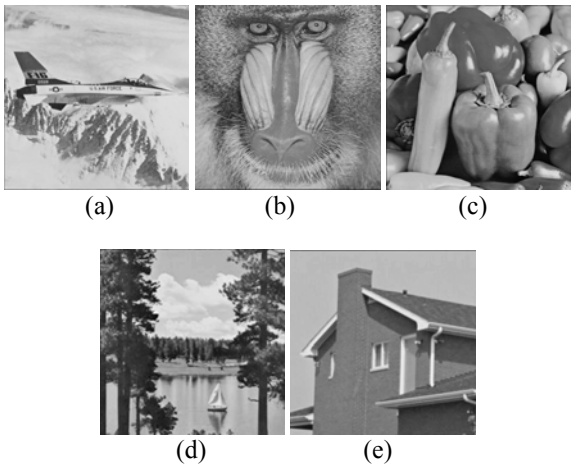


Fig. 14 the five 512×512 stego images, and the PSNRs of them are 52.84, 52.85, 52.84, 48.84, and 50.2 dB, correspondingly

Fig. 15 the recovered image Cameraman' (PSNR = 30.11 dB) by any three of the five stego images in Fig. 14

### *B. Security Analysis*

The security of the proposed method is discussed below. Without the loss of generality, let us inspect how the sharing polynomial $p(x)$ in Eq. (1) can be revealed. To solve or the coefficients $a_0 \sim a_{r-1}$ in Eq. (1), there are $r$ equations required. If

there are only $r-1$ equations, (without the loss of generality, suppose that $p(1)$, $p(2)$, …, and $p(r-1)$ are intercepted), then people can construct the following $r-1$ equations :

$$\begin{cases} p(1) = (a_0 + a_1 + \ldots + a_{r-1}) \bmod 251, \\ p(2) = (a_0 + 2a_1 + \ldots + 2^{r-1} a_{r-1}) \bmod 251, \\ \ldots \\ p(r-1) = (b_0 + (r-1)a_1 + \ldots + (r-1)^{r-1} a_{r-1}) \bmod 251. \end{cases} \quad (13)$$

To solve for $r_1$ unknown coefficients using above $r-1$ equations, there are 251 possible solutions, and the possibility of guessing the right solution is therefore 1/251. Assume the size of the VQ indices is $|V|$. Because there are $|V|/r$ sharing polynomials for the VQ indices, the possibility of obtaining the right VQ indices is $(1/251)^{|V|/r}$. For example, for the VQ indices with size $|V|$=16KB, there are about 8000 sharing polynomials if $r$=2. Therefore, the possibility of obtaining the right VQ indices is only $(1/251)^{8000}$.

## V. Conclusion

In this paper, we propose an ($r$, $n$) secret image sharing scheme based on VQ. The VQ indices of the secret image and mixed information of the VQ codebooks are hidden in the $n$ host images to form the $n$ stego images. During the recovery phase, by any $r$ out of the $n$ stego images, the VQ indices and the mixed information of codebooks can be obtained to recover the secret image with VQ quality. The proposed method improves the drawback of Chen and Chang's method [38] (no missing-allowable) at the cheap overhead of some simple logic operations. Thus, $n-r$ stego images can be lost since the secret image can still be recovered by the other $r$ survival stego images. Besides, it preserves another characteristic of the ($r$, $n$) threshold scheme that it is not easy to reveal the secret image if less than $r$ stego images are intercepted.

## References


[1] R. M. Davis, "The data encryption standard in perspective," *Computer Security and the Data Encryption Standard*, National Bureau of Standards Special Publication, Feb. 1978.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. Assoc. Comput. Mach.*, vol. 21, no. 2, pp. 120-126, Feb. 1978.

[3] NIST, "Announcing the advanced encryption standard (AES)," Federal Information Processing Standards Publication, Nov. 2001.

[4] V. Soulioti, Y. Bakopoulos, S. Kouremenos, Y. Vrettaros, S. Nikolopoulos, and A. Drigas, "Stream ciphers created by a discrete dynamic system for application in the Internet," *WSEAS Transactions on Communications*, vol. 3, no. 2, pp. 679-687, Apr. 2004.

[5] J. J. Climent, F. Ferrandez, J. F. Vicent, and A. Zamora "A nonlinear elliptic curve cryptosystem based on matrices," *Applied Mathematics and Computation*, vol. 174, no. 1, pp. 150-164, March 2006.

[6] T. Y. Lee and H. M. Lee, "Encryption and decryption algorithm of data transmission in network security," *WSEAS Transactions on Information Science and Applications*, vol. 3, no. 12, pp. 2557-2562, Dec. 2006.

[7] R. Alvarez, F. M. Martinez, J. F. Vicent, and A. Zamora, "A matricial public key cryptosystem with digital signature," *WSEAS Transactions on Mathematics*, vol. 7, no. 4, pp. 195-204, Apr. 2008.

[8] P. Margaronis and E. Antonidakis, "Design and Implementation of a Cipher System (LAM)," *WSEAS Transactions on Computers*, vol. 7, no. 7, pp. 972-976, July 2008.

[9] C. Racuciu, N. Jula, C. Balan, and C. Adomnicai, "Embedded real-time video encryption module on UAV surveillance systems," *WSEAS Transactions on Circuits and Systems*, vol. 7, no. 5, pp. 368-381, May 2008.

[10] G. R. Blakley, "Safeguarding cryptography keys," *Proceedings of AFIPS National Computing Conference*, vol. 48, pp. 313-317, June 1979.

[11] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[12] C. C. Thien and J. C. Lin, "Secret image sharing", *Computers and Graphics*, vol. 26, no. 5, pp. 765-770, Oct. 2002.

[13] C. C. Lin and W. H. Tsai, "Secret image sharing with capability of share data reduction," *Optical Engineering*, vol. 42, no. 8, pp. 2340-2345, Aug. 2003.

[14] K. E. Negm, "Secure mobile code computing in distributed environment," *WSEAS Transactions on Communications*, vol. 2, no. 4, pp. 506-512, Oct. 2003.

[15] R. Lukac and K. N. Plataniotis, "Bit-Level based secret sharing for image encryption," *Pattern Recognition*, vol. 38, no. 5, pp. 767-772, May 2005.

[16] R. Z. Wang and C. H. Su, "Secret image sharing with smaller shadow images," *Pattern Recognition Letter*, vol. 27, no. 6, pp. 551-555, Apr. 2006.

[17] K. Y. Chao and J. C. Lin, "Fault-tolerant and non-expanded visual cryptography for color images," *WSEAS Transactions on Information Science and Applications*, vol. 3, no. 11, pp. 2184-2191, Nov. 2006.

[18] D. Wang, L. Zhang, N. Ma, X. Li, "Two secret sharing schemes based on Boolean operations," *Pattern Recognition*, vol. 40, no. 10, pp. 2776-2785, Oct. 2007.

[19] H. K. Tso, "Sharing secret images using Blakley's concept," *Optical Engineering*, vol. 47, no. 7, p. 077001, July 2008.

[20] K. Y. Chao and J. C. Lin, "Secret image sharing: a boolean-operations-based approach combining benefits of polynomial-based and fast approaches," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 23, no. 2, pp. 263-285, March 2009.

[21] R. Z. Wang, C. F. Lin, and J. C. Lin, "Hiding data in images by optimal moderately-significant-bit replacement," *IEE Electronics Letters*, vol. 36, no. 25, pp. 2069-2070, Dec. 2000.

[22] R. Z. Wang, C. F. Lin, and J. C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," *Pattern Recognition*, vol. 34, no. 3, pp. 671-683, March 2001.

[23] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letter*, vol. 24, no. 9-10, pp. 1613-1626, June 2003.

[24] C. C. Thien and J. C. Lin, "A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function," *Pattern Recognition*, vol. 36, no. 12, pp. 2875-2881, Dec. 2003.

[25] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognition*, vol. 37, no. 3, pp. 469-474, Mar. 2004.

[26] S. J. Wang, "Steganography of capacity required using modulo operator for embedding secret image," *Applied Mathematics and Computation*, vol. 164, no. 1, pp. 99-116, May 2005.

[27] P. Singh, S. Batra, and H. R. Sharma, "Evaluating the performance of message hidden in 1st and 2nd bit plane," *WSEAS Transactions on Information Science and Applications*, vol. 2, no. 8, pp. 1220-1227, Aug. 2005.

[28] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods", *IEE Proceedings–Vision, Image and Signal Processing*, vol. 152, no. 5, pp. 611-615, Oct. 2005.

[29] S. K. Chen, "Embedding image on vector-quantized index file," *WSEAS Transactions on Information Science and Applications*, vol. 3, no. 11, pp. 2300-2305, Nov. 2006.

[30] Y. J. Chang, R. Z. Wang and J. C. Lin, "Hiding images using modified search-order coding and modulus function," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 22, no. 6, pp. 1215-1240, Sep. 2008.

[31] Y. S. Wu, C. C. Thien, and J. C. Lin, "Sharing and hiding secret images with size constraint," *Pattern Recognition*, vol. 37, no. 7, pp. 1377-1385, July 2004.

[32] C. H. Hsieh and J. C. Tsai, "Lossless compression of VQ index with search-order coding," *IEEE Transaction on Image Processing*, vol. 5, no. 1, pp. 1579-1582, Nov. 1996.
[33] R. M. Gray, "Vector quantization," *IEEE ASSP Magazine*, vol. 1, no. 2, pp. 4-29, Apr. 1984.
[34] Y. Linde, A. Buzo, and R. M Gray, "An algorithm for vector quantizer design," *IEEE Trans. Commun.*, vol. 28, no. 1, pp. 84-95, Jan. 1980.
[35] Y. C. Lin and S. C. Tai, "A fast Linde-Buzo-Gray algorithm in image vector quantization," *IEEE Transactions on Circuits and Systems-II: Analog and Digital Signal Processing*, vol. 45, no. 3, pp. 432-435, March 1998.
[36] C. C. Chang and Y. C. Hu, "A fast LBG codebook training algorithm for vector quantization," *IEEE Transactions on Consumer Electronics*, vol. 44, no. 4, pp.1201-1208, Nov. 1998.
[37] G. Patane and M. Russo, "The enhanced LBG algorithm," *Neural Networks*, vol. 14, no. 9, pp. 1219-1237, Nov. 2001.
[38] T. S. Chen and C. C. Chang, "New method of secret image sharing based upon vector quantization," *Journal of Electronic Imaging*, vol. 10, no. 4, pp. 988-997, Oct. 2001.
[39] C. C. Chang and R. J. Hwang, "Sharing secret images using shadow codebooks," *Information Science*, vol. 111, no. 1–4, pp. 335-345, Nov. 1998.

**Lee Shu-Teng Chen** received his B.S. degree in Computer Science from National Chiao Tung University (NCTU), Taiwan, in 1999, and M.S. degree in Computer Science and Information Engineering from National Taiwan University, Taiwan, in 2001. He is in the Ph.D. program since 2004 and currently a Ph.D. candidate in the Department of Computer Science and Information Engineering at NCTU. His current research interests include image sharing and data hiding.

**Wei-Kai Su** was born in 1981 in Taiwan, Republic of China. He received his M.S. degree in Computer and Information Science from National Chiao Tung University in 2005. His recent research interests include image sharing and image processing.

**Ja-Chen Lin** received his B.S. degree in computer science in 1977 and M.S. degree in Applied Mathematics in 1979, both from National Chiao Tung University (NCTU), Taiwan. In 1988, he received his Ph.D. degree in mathematics from Purdue University, USA. During 1981−1982, he was an instructor at NCTU. From 1984 to 1988 he was a graduate instructor at Purdue University. He joined the Department of Computer and Information Science at NCTU in August 1988, and became a professor there. His research interests include pattern recognition and image processing. Dr. Lin is a member of the Phi-Tau-Phi Scholastic Honor Society.