Fault-tolerant VQ-style Secret Image Sharing

Wei-Kai Su, Lee Shu-Teng Chen, and Ja-Chen Lin
Department of Computer Science and Information Engineering
National Chiao Tung University
Hsinchu, 300
Taiwan
stlee@cs.nctu.edu.tw

Abstract: - In this paper, we propose a fault-tolerant secret image sharing scheme based on vector quantization (VQ). The proposed method uses some of the \( n \) host images to generate the codebooks for VQ, and compresses the secret image by VQ with the generated codebooks. The VQ indices are thus created and then shared among \( n \) shadows. After obtaining the \( n \) shadows, they are embedded together with the mixed information of the generated codebooks into the \( n \) host images to form the \( n \) stego-images. When collecting any \( r \) (\( r \leq n \)) of the \( n \) stego-images, the VQ indices and codebooks can be retrieved to recover the secret image. However, no information about the secret image can be revealed if obtaining less than \( r \) stego-images. Because of using VQ, the secret image is compressed to the VQ indices, and thus easier to be hidden than the non-compressed one. The quality of the recovered image is the same as the one of the ordinary VQ.

Key-words: fault-tolerant, secret sharing, vector quantization, data hiding.

1 Introduction
Secret sharing is a technique for protecting secret data. There are many secret sharing schemes nowadays [1-8]. Blakley [1] and Shamir [2] firstly propose the \( (r, n) \) threshold secret sharing scheme. The user can use their polynomial method to share the secret data among \( n \) shadows. If some of the users need the secret, he or she has to collect at least \( r \) \((r\leq n)\) shadows to recover the secret. However, the \( n \) shadows use a lot of storage space because the size of each one is the same as that of the original secret image. Therefore, Thien and Lin [3] extend the idea of Shamir’s scheme [2] to share the secret image, and the size of each shadow in [3] is only \( 1/r \) of that of the original secret image.

Vector quantization (VQ) is a simple image compression scheme [9]. By using VQ, although the image sacrifices its quality, the size of shadows can be reduced to smaller ones. Therefore, before sharing, the user may apply VQ to compress the secret image, and the generated VQ indices are shared instead of the gray values of the secret image. This will cause the sharing worthier because the data amount is reduced. There are two major ways about the VQ-style image sharing. The first one [10] is that the first \( m \) \((4\leq m\leq 7)\) bit-planes of the host images are used to construct the VQ codebooks. Then, the secret image is compressed by VQ with these codebooks to create the VQ indices. Finally, the obtained VQ indices are hidden in the last \((8-m)\) bit-planes of the host images to form the stego-images. Because the to-be-hidden VQ indices are of small amount, the impact to the host images is small. The quality of the reconstructed secret image in [10] is also not bad. However, there is a drawback in [10], namely, if any one of the stego-images is damaged, then the user cannot extract the full VQ indices from the other undamaged stego-images, and thus the secret image cannot be completely recovered.

The other VQ-style sharing method [11] is that the VQ codebooks are shared among \( n \) shadows by Shamir’s \((r, n)\) threshold scheme [2], and the VQ indices of the secret image are kept in a local storage unit. When the user collects any \( r \) of the \( n \) shadows, the VQ codebooks can be revealed, and then used together with the VQ indices (saved in the local storage unit) to recover the secret image. Unlike Chen and Chang’s method [10], Chang and Hwang’s method [11] is fault-tolerant. The VQ codebooks can always be reconstructed as long as the number of the damaged shadows is no more than \( n-r \). However, the recovered-image quality in [11] is not good as that in [10]. In order to keep the fault-tolerant property while maintaining the quality of the recovered image, we provide a fault-tolerant VQ-style image sharing method here.

The rest of this paper is organized as follows. Sec. 2 presents the proposed method. Sec. 3
provides the experimental results. Sec. 4 draws the conclusion.

2. The proposed method

The proposed method uses any $r$ out of the $n$ input host images to construct the $r$ codebooks for VQ. Then, the VQ indices of the secret image are computed by VQ with these $r$ codebooks. After generating the VQ indices, they are shared among $n$ shadows by Thien and Lin’s $(r, n)$ threshold scheme [3]. Finally, the created $n$ shadows and the mixed information of the $r$ codebooks are hidden in the $n$ input host images. The $n$ stego-images are thus generated. Later, if collecting any $r$ of the $n$ generated stego-images, then the VQ indices and codebooks can be obtained to recover the secret image.

2.1 The sharing-hiding phase

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. Fig. 1 shows the flowchart of our generation and hiding of the VQ indices. First, the first $m$ bit-planes of the first, second, and third host images are used to generate the $r=3$ VQ codebooks $A$, $B$, and $C$, respectively. Next, the VQ indices of the input secret image are computed by VQ with the generated codebooks. Now, the generated VQ indices are shared using Thien and Lin’s $(r=3, n=5)$ threshold scheme [3] to produce the $n=5$ shadows. Finally, the five created shadows are, respectively, hidden in the last $(8-m)$ bit-planes of the five input host images to from the five stego-images.

After processing all codewords in the codebooks $A$, $B$, and $C$ according to the equations (1)−(3), as shown in Fig. 2, the obtained information $X_1$ and $X_2$ are hidden in the fourth host image, and $Y_1$ is hidden in the fifth host image. Notably, the exclusive-OR operations can be set arbitrarily as long as they guarantee that the three VQ codebooks can be recovered when any three stego-images are received.

2.2 The recovery phase

In the recovery part, any $r=3$ of the $n=5$ stego-images are needed to recover the secret image. When collecting any three of the five stego-images, three shadows can be, respectively, extracted from the last $(8-m)$ bit-planes of the collected stego-images. Then, the extracted shadows are used to reveal the VQ indices by using the linear combination of Lagrange polynomials (see [3]). As for the reconstruction of the VQ codebooks, the first $m$ bit-planes of the collected stego-images which do not include the fourth and fifth ones can be directly used to generate the three codebooks for VQ.

However, if one of the collected stego-images is the fourth or fifth one, then two codebooks can be directly created by using the first $m$ bit-planes of the first two collected stego-images, and the third codebook is computed by applying the
exclusive-OR operations. For example, if three collected stego-images are, respectively, the first, second, and fourth ones, then the information of the two codebooks $A$ and $B$ are extracted from the last $(8-m)$ bit-planes of the first and second stego-images, respectively, and the mixed information $X_2$ is extracted from the last $(8-m)$ bit-planes of the fourth one. After that, the third codebook $C$ is computed by

$$C = B \oplus X_2.$$ \hspace{1cm} (4)

Moreover, if two of the three collected stego-images are the fourth and fifth ones, then only one codebook can be directly generated. The other two codebooks still can be created by the exclusive-OR operations similarly.

After obtaining the VQ indices and three VQ codebooks (either directly, or after some computation), the secret image can be reconstructed. As a remark, if only one or two stego-images are collected, then the VQ indices cannot be revealed by the Lagrange polynomials even if the information of the VQ codebooks is sufficient, so nothing about the secret image will be revealed.

### 3. Experimental results

The secret image Lena and five host images, Jet, Baboon, Peppers, Boat, and House are tested in the experiments. The quality of the image is estimated by the peak signal-to-noise ratio (PSNR), which is defined as

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\text{MSE}},$$ \hspace{1cm} (5)

where

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (x_{ij} - \hat{x}_{ij})^2.$$ \hspace{1cm} (6)

Note that $x_{ij}$ and $\hat{x}_{ij}$ are the original pixel value and the stego (or recovered) pixel value, in the $M \times N$ image, respectively.

Fig. 3 shows the original secret image Lena whose size is 1024×1024. Figs. 4(a)–4(e) are the five host images, and each of which is of size 512×512. The first $m=7$ bit-planes of the three host images Jet, Baboon, and Peppers are, respectively, used to generate the three VQ codebooks. The VQ indices of the secret image Lena are computed by VQ with the generated codebooks, and then shared using Thien and Lin’s ($r=3, n=5$) threshold scheme [3]. After generating the five shadows, they are, respectively, hidden in the last bit-plane of the five host images (Figs. 4(a)–4(e)). Besides, the mixed information of the generated codebooks is also hidden in the last bit-plane of the two host images Boat and House. Figs. 5(a)–5(e) are the five resulting stego-images, and the PSNRs of them are 52.70, 52.71, 52.69, 48.87, and 50.34 db, respectively. Fig. 6 shows the recovered image Lena (PSNR= 34.01 db) when using any $r=3$ of the $n=5$ stego-images in Fig. 5. The qualities of our stego-images and recovered image are all acceptable.

![Fig. 3. The original 1024×1024 secret image Lena.](image)

![Fig. 4. The five host images of size 512×512. (a) Jet; (b) Baboon; (c) Peppers; (d) Boat; and (e) House.](image)

![Fig. 5. The five 512×512 stego-images, which are the hiding results of Figs. 4(a)–4(e), respectively. The PSNRs of Figs. 5(a)–5(e) are 52.70, 52.71, 52.69, 48.87, and 50.34 db, correspondingly.](image)
4. Conclusion

In this paper, a fault-tolerant method of VQ-style secret image sharing is proposed. To achieve the goal of the fault-tolerance, the VQ indices of the secret image are generated by VQ with the VQ codebooks, and then shared among \( n \) shadows using Thien and Lin’s \((r, n)\) threshold scheme [3]. The created \( n \) shadows and the mixed information of the VQ codebooks are embedded into the \( n \) host images to form the \( n \) stego-images. During the recovery phase, the user can recover the secret image by using any \( r \) of the \( n \) stego-images. The proposed method improves the drawback of the Chen and Chang’s method [10] (no fault-tolerance) 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 using the other \( r \) survival stego-images. Besides, it preserves another characteristic of the \((r, n)\) threshold scheme that insufficient number (less than \( r \)) of the stego-images reveals nothing about the secret image. Furthermore, the quality of the recovered image is not bad, too (the same as that of the original VQ).

References: