Chapter 5

Conclusions and Future Works

5.1 Conclusions

In this thesis, some methods of VQ-style secret image sharing and recovery have been proposed. Chapter 2 introduced two methods to share the secret image. The first one uses the mixed information of the codebooks generated from the host images to achieve the goal of fault-tolerance; and the second one is a progressive image sharing whose best recovery level can be lossless. The error correction method of secret image using SOC is proposed in Chapter 3. Then, Chapter 4 combines the techniques in Chapters 2 and 3, and presents some applications of the SOC-images.

Notably, in the first section of Chapter 2, to achieve the goal of fault-tolerance, the code indices of the secret image are shared using an (r, n) threshold scheme. The other component of the VQ system – the codebooks, which are calculated from the host images, are operated using some exclusive-OR operations to generate the mixed information. During the recovery phase, the user can recover the secret image using any r shadows. This method improved the drawback of the ordinary method (no fault-tolerance) at the cheap overhead of some simple logic operations. Thus, $n-r$ shadows can be lost since the secret image can still be recovered using the other r shadows. It is also preserves another characteristic of the (r, n) threshold scheme that insufficient number of the shadows reveals nothing about the secret image. Because of the use of VQ, the secret image is compressed to code 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. In the second part of Chapter 2, a lossless progressive

image sharing method is proposed. By calculating and sharing the code indices of the image and the difference, the user can recover image versions of different qualities according to the number of the received shadows. Due to the character of (r, n) sharing scheme, the user also need not to care about the receiving order of the shadows. Being progressive, there are some benefits of this method (as compared with the progressive sharing method proposed in [15]):

(1) Fast and easy decoding– Since the recovered data are code indices and the only thing must be done is look up the codewords in the codebooks and fill them to the image.

(2) The adjustment of the threshold is easy – the user only need to adjust the r in the (r, n) system to achieve the threshold scheme.

(3) Lossless – This method provides lossless recovery if the user collect enough number (not less than the last threshold of) shadows.

The secret image error correction using SOC is proposed in Chapter 3. The SOC-image is generated. Then, at the recovery of the shared secret image, if the recovered image is damaged, the user can improve its quality using the SOC-image. There are three reasons why the technique of SOC-image is much better than duplicating the original secret image:

(1) The SOC-image reveals nothing about the secret image. The SOC-image is only useful when it is combined with the recovered secret image (damaged or not).

(2) If the secret image is destructed after sharing, then there is no other way to get the secret except retrieving it from the shadows. If the shadows contain error, then SOC-images can be used to improve image quality.

(3) If people want to duplicate the secret image to avoid the possible crash of the secret image, then the risk that the secret image is stolen also increases.

The advanced version of the SOC-image provides two flexible ways to correct the damaged image. According to the availability of the hash table, the user can use two different ways to improve the quality of the damaged image. The experimental results showed that both two ways are useful in the correction.

In Chapter 4, the applications of the SOC-image are introduced. Firstly, we combine the SOC-image and the fault-tolerant sharing proposed in Chapter 2. The experiment shows that the SOC-image is not only useful with normal image, but also useful in VQ system. The character of the SOC-image (the distribution of the values in the SOC-image) provides an efficient way to decrease its size easily by a lossless compression method, too. The SOC-image technique can also improve the recovery quality of the progressive sharing introduced in Section 2.3.

5.2 Future Works

Some extensions of the proposed method are shown below:

1. In the fault-tolerant sharing system introduced in Section 2.2, the mixed information of the codebooks was calculated using the exclusive-OR operations. The operations are set arbitrarily as long as the mixed information can achieve the threshold scheme. Thus we can develop a system that other operation are applied in the new (r, n) threshold scheme. Then the user can just refer to this system and does not need to design the mixed information generated scheme before sharing.
2. About the progressive image sharing, we can apply weight sharing to it. That is, the recovered details are different using different shadows. Some shadows may recover a better quality of the secret image than

another other set of shadows do, even if the numbers of shadows are the same. Receiving the light-weight shadow can recover the secret image in a not-so-good quality, while receiving the heavy-weight shadows can recover a better quality of the secret image. It will provide an additional feature that the manager can get a good quality recovered image and the staffer only recovers a rough one.

3. We can develop another scheme to increase the recovery ability of the basic version of the SOC-image. Although the experiments showed that the SOC-image indeed improved the quality of the damaged image, there is still some room to repair the damaged image to a better one. Besides, if the image is damaged too much, the repairing ability of the basic SOC-image becomes not good. This is a drawback can be addressed. People may also increase the fault-tolerance level of the SOC-image so that even if the SOC-image is damaged, it still can correct the error.

References

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

[2] R. M. Gray, "Vector Quantization," *IEEE ASSP Magazine*, vol.1, no.2, pp.4-29, 1984.

[3] T. C. Wu and W. H. He, "A geometric approach for sharing secrets," *Computers & Security*, vol. 14, no. 2, pp.135-145, 1995.

[4] A. Beimel and B. Chor, "Secret Sharing with public reconstruction," *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 1887-1896, 1998.

[5] C. C. Thien and J.C. Lin, "An image-sharing method with user-friendly shadow images," *IEEE Transactions on Circuits and Systems for Video Technology*, no. 13, vol. 12, pp. 1161-1169, 2003.

[6] C. C. Chang, C. H. Lin, W. Lee, and P. C. Hwang, "Secret sharing with access structures in a hierarchy," *Proceedings of the 18th International Conference on Advanced Information Networking and Application*, pp. 31-34, 2004.

[7] C. C. Thien and J. C. Lin, "Secret image sharing," *Computers & Graphics*, vol. 26, pp. 765-770, 2002.

[8] Y. S. Wu, C. C. Thien, and J. C. Lin, "Sharing and hiding secret images with size constraint," *Pattern Recognition*, vol. 37, pp. 1377-1385, 2004.

[9] C. S. Tsai, C. C. Chang, and T. S. Chen, "Sharing multiple secrets in digital images," *The Journal of Systems and Software*, vol. 64, pp. 163-170, 2002.

[10] M. Naor and A. Shamir, "Visual cryptography", *Advances in Cryptology-EUROCRYPT '94*, Lecture Notes in Computer Science, Springer-Verlag, Perugia, Italy, vol. 950, pp. 1-12, 1994.

[11] C. C. Lin, and W. H. Tsai, "Visual cryptography for gray-level images by

dithering techniques," *Pattern Recognition Letters*, vol. 24, issue 1–3, pp. 349-358, 2003.

[12] Y. C. Hou, "Visual cryptography for color images," *Pattern Recognition*, vol. 36, pp. 1619-1629, 2003.

[13] H. C. Hsu, T. S. Chen, and Y. H. Lin, "The ringed shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing," *Proceedings of the 2004 IEEE International Conference on Networking, Sensing, and Control*, pp. 996-1001, 2004.

[14] M. Manohar and J. C. Tilton, "Progressive vector quantization on a massively parallel SIMD machine with application to multispectral image data", *IEEE Transaction on Image Processing*, vol. 5, no. 1, pp. 142-174, 1996.

[15] K.H. Hung, "Progressive image sharing," Master Thesis, Department of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 2003.

[16] 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, 1998.

[17] 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, 1998.

[18] G. Patane and M. Russo, "The enhanced LBG algorithm," *Neural Networks*, vol. 14, pp. 1219-1237, 2001.

[19] C. C. Chang and I. C. Lin, "Novel full-search schemes for speeding up image coding using vector quantization," *Real-Time Imaging*, vol. 10, pp.95-102, 2004.

[20] C.C. Chang and R.J. Hwang, "Sharing secret images using shadow codebooks," *Information Sciences*, vol. 111, pp. 335-345, 1998.

[21] 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, 2001.

[22] R. Z. Wang, C. F. Lin, and Z. C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," *Pattern Recognition*, vol. 34, no. 3, pp. 101-113, 2001.

[23] 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, 2003.

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

[25] M. Tompa and H. Woll, "How to share a secret with cheaters," Journal of Cryptology, vol. 1, no, 2, pp. 133-138, 1998.

[26] T. C. Wu and T. S. Wu, "Cheating detection and cheater identification in secret sharing schemes," *IEE Proceedings, Computer and Digital Techniques*, vol. 142, no. 5, pp. 367-369, 1995.

[27] S. J. Hwang, C. C. Chang, and W. P. Yang, "New cheater identification in threshold schemes," *Technical report of the Institute of Computer and Information Science*, National Chiao Tung University, Taiwan, R.O.C., 1995

[28] C. C. Chang and R. J. Hwang, "Efficient cheater identification method for threshold schemes," *IEE Proceedings, Computer and Digital Techniques*, vol. 144, no. 1, pp. 23-27, 1997.

[29] J. Lee and C. S. Wan, "A watermarking sequence using parities of error control coding for image authentication and correction," *IEEE Transaction on Consumer Electronics*, vol.46, no.2, pp.313-317, 2000.

[30] C. H. Heh and J. C. Tsai, "Lossless compression of VQ index with search-order

coding," *IEEE Transaction on Image Processing*, vol. 5, no. 11, pp. 1579-1582. 1996.