Secret Image Recovery based on Search Order Coding

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

***Abstract*—**In this paper, we propose an image recovery method based on search order coding (SOC). By using SOC technique, we can generate a SOC image for an input secret image. If the secret image is damaged, by referring to its SOC image, the damaged image can be repaired to a better one. In addition to the proposed basic version of the SOC recovery technique, we also modify it to an advanced one. The advanced version provides a more flexible method that repairs the damaged image by two different ways according to the availability of the mapping table. The secret image can still be recovered even when it is seriously damaged. Besides, the proposed SOC recovery technique can be applied to not only the gray values of the secret image but also the VQ indices. Experiments show that the recovery ability of the VQ indices is better than that of pixel values. Moreover, the SOC image alone reveals nothing about the secret image. Therefore, the SOC image is safer than directly duplicating the secret image.

***Keywords*—**Image recovery, mapping table, search order coding (SOC), secret sharing.

I. Introduction

COMPUTER network nowadays is convenient so that images can be transmitted via network. However, since network is an open environment, a secret image may be intercepted or damaged during its transmission. Because the original image is secret, to back up using a duplicated secret image or double transmission is not smart (this increases the chance that the secret get pirated). Thus, before transmission, people may transform the secret image into several shadows by some secret sharing schemes [1]-[18]. There are many methods of secret sharing nowadays. Blakley [1] and Shamir [2] first independently introduced the concept of secret sharing. The user can use their polynomial-based (r, n) threshold scheme to share the secret among n shadows. When collecting at least r shadows, the secret image can be revealed by using Lagrange interpolation. Later, Thien and Lin [3] extended the idea in [2] to share the secret image among n shadows. Each of their shadow size is only $1/r$ of that of the original secret image. To reduce further the size of each shadow, some image sharing schemes based on vector quantization (VQ) have been proposed [6], [9]. VQ [19] is one of the well-known image compression schemes. By using VQ, the VQ indices of the secret image can be generated according to a VQ codebook. Therefore, Chen and Lin [6] used their bit-plane scanning method to transform the VQ indices of the secret image, and shared the bit-transformed VQ indices among n shadows. Su *et al.* [9] also shared the VQ indices, and hid the obtained n shadows with the mixed information of the VQ codebooks in the host images to from the n stego-images. Besides the sharing using polynomial, Tsai *et al.* [11] used the exclusive-OR operation to share the secret. Visual cryptography is also a convenient method to share the image [12]-[18]. By adjusting the luminance of the extended pixel in the shadow transparency, the secret data is shared among shadow transparencies, and nothing will be revealed from each transparent sheet alone. The user can stack two or more transparencies to see the secret data visually without the need of complicated computation.

Although the (r, n) threshold schemes [3], [5], [6], [8]-[10] have the fault-tolerant property that allows $n-r$ shadows to be lost in the recovery phase, the risk that the number of the modified (or damaged) shadows over $n-r$ still exists. Tompa and Woll [20] introduced how to cheat in the threshold scheme. Therefore, some researches provided the methods against the cheater. Wu and Wu [21] used one-way hash function to detect and identify the cheat. Chang and Hwang [22] proposed a method using quadratic residues instead of the hash functions. Lee and Won [23] used watermarking to correct the alterations. In this paper, an image recovery method based on SOC technique is proposed. The goal of this paper is that when reconstructing the secret image by any r out of the n shadows, and if the number of the damaged shadows exceeds $n-r$, a version of not-bad quality for the secret image may still be reconstructed with the help of the SOC image. Of course, before combining the SOC image with the secret image (damaged or not), it is required that no information about the secret image can be found by the SOC image alone. Notably, if

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).

L. S. T. Chen is with the Department of Computer Science and Information Engineering, National Chiao Tung University, Hsinchu, Taiwan, R.O.C. (e-mail: stlee@cs.nctu.edu.tw).

S. K. Chen is with the Department of Computer Science and Information Engineering, Yuanpei University, Hsinchu, Taiwan, R.O.C. (corresponding author to provide phone: +886-3-5381183; e-mail: cotachen@mail.ypu.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).

the recovered secret image is damaged too much, then the SOC image cannot repair the damaged image. Thus an advanced version of SOC recovery technique is proposed for the seriously damaged image. The anti-theft principle is not changed, namely, the information about the secret image cannot be retrieved from the SOC image alone.

The rest of this paper is organized as follows. Sec. Ⅱ presents the proposed method. Sec. Ⅲ introduces the SOC recovery application. Sec. Ⅳ shows the experiment results. Sec. Ⅴ provides a discussion. Finally, Sec. Ⅵ draws a conclusion.

II. The Proposed Method

By an additional image called SOC image, we can repair the damaged secret image to a better one. The details of the proposed basic and advanced versions of the SOC recovery technique are described in Sec. Ⅱ-A and Sec. Ⅱ-B, respectively.

A. Basic Version

The method to create the SOC image is somewhat like the one in [24]. However, the coding values used here are the gray value of pixels rather than the VQ indices. For every pixel in an input gray-level secret image, its searching range is limited to its previous points. The previous points of the pixel $p(x, y)$ in the secret image are the collection of all points whose rows are above Row x together with those points not only in Row x but also staying at the left of the point at (x, y). For example, in the 7×5 image shown in Fig. 1, the previous points of the pixel $p(4, 5)$ are those 3×7+4=25 points in the shaded region.

(1,1)	**(1,2)**	**(1,3)**	**(1,4)**	**(1,5)**	**(1,6)**	**(1,7)**
(2,1)	**(2,2)**	**(2,3)**	**(2,4)**	**(2,5)**	**(2,6)**	**(2,7)**
(3,1)	**(3,2)**	**(3,3)**	**(3,4)**	**(3,5)**	**(3,6)**	**(3,7)**
(4,1)	**(4,2)**	**(4,3)**	**(4,4)**	**(4,5)**		

Fig. 1 the previous points of the pixel at the position (4, 5) (the shaded region)

Before searching, the Starting Searching Point (SSP) must be specified. After the specification of the SSP, the search order is fixed. As shown in Fig. 2, if the left point of the pixel $p(x, y)$ is the SSP, then the search starts at SSP. At the end of each level, the search goes to next level and continues finding the pixel. In the beginning of the search, the "searching count" is initialized to 1. If the gray value of the SSP equals the gray value of $p(x, y)$, the initial value 1 is written to the corresponding position (x, y) in the SOC image. Otherwise, we find the next search point according to the order shown in Fig. 2, and add 1 to the searching count. Notably, since the gray values of neighborhood pixels are often similar, each gray value of the searching area may repeat frequently. Therefore, the searching count does not be added up if the gray value of the candidate point currently inspected appeared before. The search continues until a previous point whose gray value is the same as that of $p(x, y)$ is found, and the searching count at that moment becomes the content of the corresponding position (x, y) in the SOC image. However, when all previous points of $p(x, y)$ are searched, and if there is no previous point whose gray value is the same as that of $p(x, y)$, the value 0 is recorded to the position (x, y) in the SOC image. After sequentially processing all pixels of the input secret image by using above procedure, the SOC image of that secret image can be constructed.

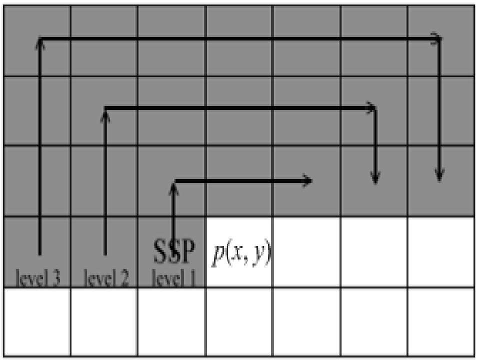


Fig. 2 the search order for the pixel $p(x, y)$

For example, in Fig. 3, if the gray value of $p(4, 4)$ is 10, the SSP of $p(4, 4)$ is $p(4, 3)$ whose gray value is 20. These two gray values are not equal, so the value 1 is added to the searching count. Then, the search continues according to the searching path. Because the gray value of the next point at (3, 3) is 45 which not equals 10, the value 1 is added to the current searching count and the search still continues. When the search comes to $p(3, 4)$ whose gray value is 20, due to the gray value 20 already appeared earlier during this search (in fact, it is the gray value of the point at (4, 3)), there is no need to increase the searching count. After finding the gray value 10 of the point at (3, 2), the search count 4 at that moment is recorded to the position (3, 2) in the SOC image.

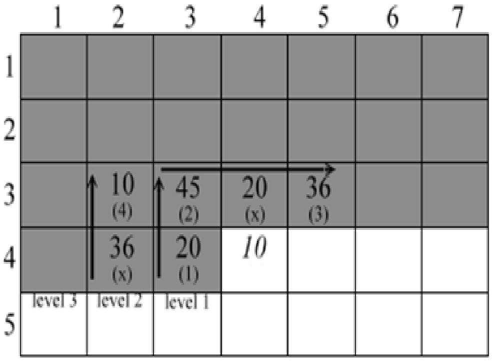


Fig. 3 an example of finding the searching count for the pixel $p(4, 4)$ whose gray value is 10

When receiving an image that may be damaged, we can recover the damaged image with the help of the SOC image. In the first stage, all pixels in the damaged image are divided into several groups according to the SOC image. The grouping starts from the first pixel of the SOC image, and the next grouped pixel is decided by a raster scan order (i.e. from left to right and then top to bottom). For each pixel $q(x, y)$ in the damaged image, if its search count is recorded as 0 in the SOC image, the gray value of the pixel $q(x, y)$ is allocated to a new group. Otherwise, the previous points of $q(x, y)$ are searched by the search order, and the search will find the only previous point for $q(x, y)$ by its search count as long as the SOC image is correct. The gray value of the pixel $q(x, y)$ is then merged to the group of the previous point being found.

After sequentially processing all pixels in the damaged image, there will be different gray values in one group, and the possible value for the group is decided by the gray value which appears most often. For example, in a group, if there are three different gray values 10, 73, and 240 with appearing frequencies 1547, 1036, and 4810, respectively, the most possible gray value of this group is set to 240 since this value appears most often. Therefore, the damaged image can be recovered to a better quality image by checking the most possible gray value in every pixel's group.

B. Advanced Version

Before generating the SOC image for a gray-level secret image, we divide the pixels of the secret image into 128 groups according to their pixel values. The pixel values 0 and 1 are merged to group 1, the pixel values 2 and 3 are merged to group 2, and so on. Then, a one-to-one and onto mapping table is used to map each of the 128 group numbers to a value ranged from 0 to 127. After that, for each pixel $p(x, y)$ in the secret image, the search will find a previous point whose group number (*not the gray pixel value*) is the same as that of $p(x, y)$, and a bit 0 followed by the 7-bit search count (there are 128 groups, so only 7 bits are needed to record the search count) is written to the corresponding position (x, y) in the SOC image. However, when all previous points of $p(x, y)$ are searched, and if there is no previous point whose group number is the same as that of $p(x, y)$, a bit 1 followed by the 7-bit mapped value of the group of $p(x, y)$ is recorded to the corresponding position (x, y) in the SOC image.

When the secret image is damaged, it still can be recovered by its (advanced) SOC image no matter the mapping table is available or not. For each pixel $q(x, y)$ in the damaged image, if the first bit of the pixel $s(x, y)$ in the SOC image is 1, the value of the last 7 bits of $s(x, y)$ is a mapped value. Therefore, if the mapping table is not available, the pixel $q(x, y)$ is used to allocate a new group; otherwise, the group number is computed by applying the inverse-mapping of the last 7 bits of t $s(x, y)$, and one of the two gray values in this group is used to allocate a new group (each of the 128 groups contains two different gray values). On the contrary, if the first bit of $s(x, y)$ in the SOC image is 0, the value of the last 7 bits of $s(x, y)$ is the search count. Therefore, the previous point is searched (and found) according to the search count. Then, the pixel $q(x, y)$ is merged to the group of the previous point being found. After the grouping and the determination of the most possible value of each group, the damaged image may become better.

III. The SOC Recovery Application

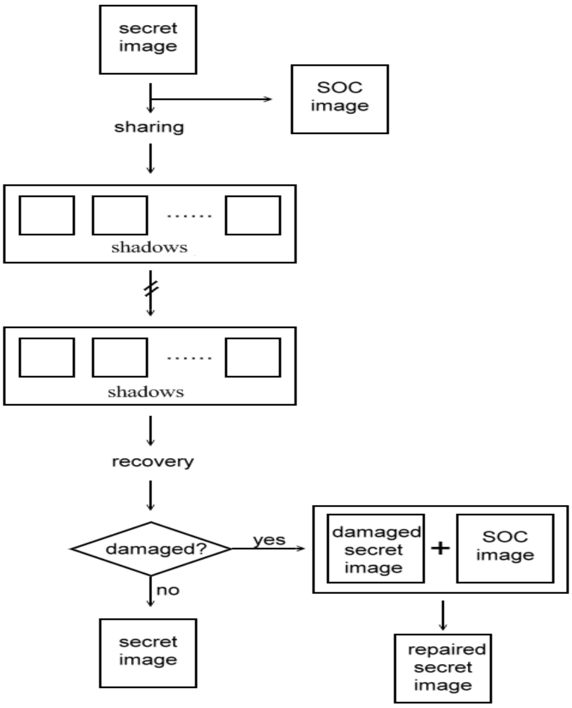


Fig. 4 the flow of the SOC recovery application

Fig. 4 shows the flow of the SOC recovery application. Before sharing, the secret image is processed by the SOC recovery technique proposed in Sec. Ⅱ-A to generate the SOC image. The secret image is then shared among shadows by any secret sharing technology. If one or more shadows are damaged so that the secret image cannot be recovered, by using the SOC image, the quality of the damaged secret image can be improved. The detail is described below.

To show that our SOC recovery technique can be also used to process the VQ indices, we apply Su *et al.*'s [9] secret image sharing scheme in the SOC recovery application. First, compute the VQ indices of the secret image according to the VQ codebooks constructed from the first seven bit-planes of the host images. Next, use the proposed SOC recovery technique to construct the SOC image for the generated VQ indices. Notably, the construction of the SOC image for the VQ indices is the same as that mentioned in Sec. Ⅱ-A, except that the data being processed here are the VQ indices instead of the pixel values. Finally, the VQ indices are shared, and the created n shadows are embedded together with the mixed information of the VQ codebooks into the host images to from the n stego-images.

When collecting any r of the n stego-images, the VQ indices of the secret image can be recovered by Lagrange interpolation. However, if the number of the damaged stego-images is over $n-r$, the VQ indices cannot be revealed. In this bad condition, the SOC recovery technique can be applied to the repairing of the VQ indices. After the repairing, the information of the VQ indices may become more precise. Note that the stego-images also contain the mixed information of the VQ codebooks. If the stego-image is damaged, not only the VQ indices, but also the VQ codebooks will be incorrect. Therefore, the SOC recovery technique will generate some strange blocks during the repairing. Even so, the SOC image is still useful if the damaged area of the stego-images is local (or the damage is widely distributed but the damaged level is slight).

IV. Experimental Results

First, the two 512×512 gray-level images Lena and Pepper are tested in the experiments. The peak-signal-to-noise ratio (PSNR) is used to measure the quality of the recovered image. In general, the PSNR value should be kept as high as possible. In the first experiment of the basic version, Fig. 5(a) shows the 512×512 secret image Lena, and Fig. 5(b) shows the SOC image of the secret image Lena in Fig. 5(a). Fig. 5(c) presents the damaged image Lena by adding noise to Fig. 5(a). After the repairing by using the SOC image in Fig. 5(b), an image of a quality better than that of Fig. 5(c) can be constructed. Fig. 5(d) displays the recovered image Lena' (PSNR=53.95 dB). In the second experiment, Figs. 6(a)-6(b) show, respectively, the original secret image Pepper and its SOC image. Figs. 6(c)-6(d) display, correspondingly, the cropped image Pepper and the recovered image Pepper'. The PSNR of Fig. 6(d) is 43.61 dB.

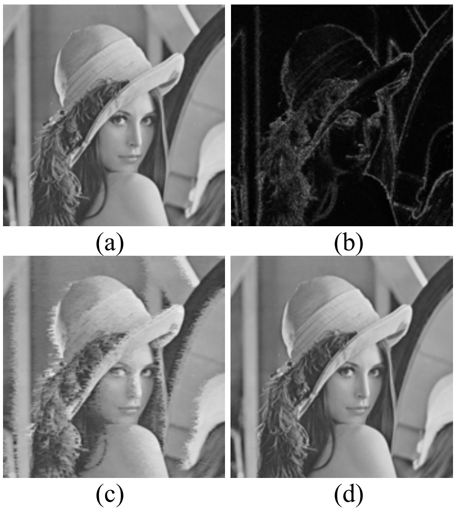


Fig. 5 the experiment result of the basic version when the image Lena is contaminated by some noise: (a) is the original secret image Lena; (b) is the SOC image of Fig. 5(a); (c) is the damaged image Lena; (d) is the recovered image Lena' (PSNR=53.95 dB) of Fig. 5(c) by Fig. 5(b)

In the experiment of the advanced version, the secret image is the image Pepper shown in Fig. 6(a). Fig. 7(a) is the (advanced) SOC image of the secret image Pepper (Fig. 6(a)). The damaged image Pepper in Fig. 7(b) is created by adding noise to Fig. 6(a). If the damaged image (Fig. 7(b)) is repaired by the SOC image (Fig. 7(a)) alone, the recovered image Pepper'' is shown in Fig. 7(c). Finally, by using the SOC image and the mapping table, a recovered image Pepper''' of much better quality can be reconstructed displayed in Fig. 7(d). The PSNRs of Figs. 7(c)-7(d) are 28.35 dB and 51.15 dB, correspondingly.

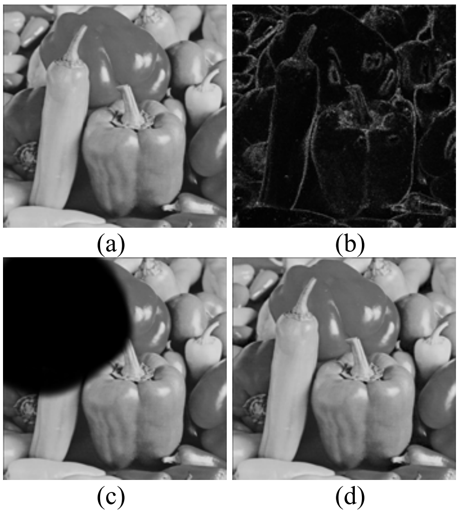


Fig. 6 the experiment result of the basic version when the image Pepper is cropped: (a) is the original secret image Pepper; (b) is the SOC image of Fig. 6(a); (c) is the cropped image Pepper; (d) is the repaired image Pepper' (PSNR=43.61 dB) of Fig. 6(c) by Fig. 6(b)

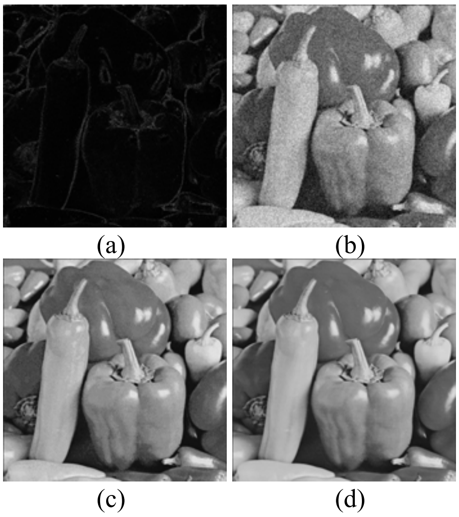
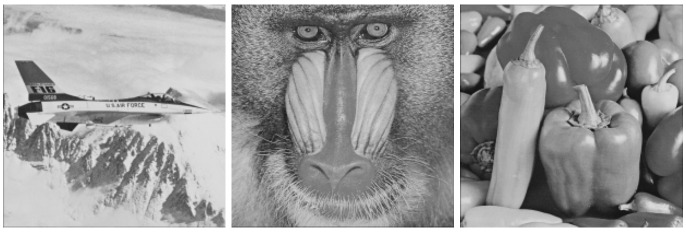


Fig. 7 the experiment result of the advanced version when noise is added to the image Pepper: (a) is the SOC image (advanced version) of Fig. 6(a); (b) is the damaged image Pepper; (c) is the repaired image Pepper'' (PSNR=28.35 dB) of Fig. 7(b) by Fig. 7(a); (d) is the repaired image Pepper''' (PSNR=51.15 dB) of Fig. 7(b) by Fig. 7(a) and the mapping table

Next, in the experiment of the SOC recovery application, according to [9], the two parameters r=3 and n=5, and the r=3 VQ codebooks which each contains 256 codewords of 16-dimension are tested. Fig. 8 shows the 1024×1024 gray-level secret image Lena, and Fig. 9 displays the five 512×512 gray-level host images. The secret image Lena is compressed by VQ to obtain the VQ indices. The SOC image of the created VQ indices is constructed shown in Fig. 10 (the size of the SOC image is 1024×1024/16=256×256). Then, the VQ indices are shared by Thien and Lin's (3, 5) scheme [3]. The five generated shadows and the mixed information of the three VQ codebooks are hidden in the five host images (Fig. 8) to form the five stego-images shown in Fig. 11. During the recovery phase, the VQ indices and codebooks can be extracted from any three stego-images in Fig. 11 to construct the secret image with VQ quality.

When at least three of the five stego-images in Fig. 11 are modified or damaged, the secret image cannot be recovered. Fig. 12 shows the three damaged stego-images by slightly modifying the stego-images Jet, Baboon, and Peppers in Figs. 11(a)-11(c). Fig. 13 shows the image reconstructed by the three stego-images in Fig. 12. We can see that Fig. 12 is seriously damaged and quite noisy. However, with the help of the SOC image in Fig. 10, the recovered image Lena'' (PSNR=27.93 dB) is shown in Fig. 14 (the PSNR of the recovered secret image Lena by using three non-damaged stego-images is 34.01dB). Fig. 15 shows the three seriously damaged stego-images by adding noise to the three stego-images in Figs. 11(a)-11(c), respectively. As displayed in Fig. 16, the image revealed by the three damaged stego-images in Fig. 15 almost reveals no information about the secret image Lena. However, after the repairing by the SOC image in Fig. 10, although the proposed method does not completely recover the damaged pixels, our recovered secret image Lena''' displayed in Fig. 17 becomes much better than Fig. 16. Even if the fifth stego-image in Fig. 9(e) (contain the mixed information of the VQ codebooks) is modified, the SOC image is also useful for repairing. Fig. 18 shows the three damaged stego-images by modifying the stego-image in Figs. 11(a), 11(b), and 11(e), respectively. Fig. 19 presents the image revealed by the three damaged stego-images in Fig. 18, and Fig. 20 shows the recovered image Lena'''' by the SOC image in Fig. 10.

Fig. 8 the original 1024×1024 secret image Lena



(a) (b) (c)

(d) (e)

Fig. 9 the five 512×512 host images: (a) Jet; (b) Baboon; (c) Peppers; (d) Boat; and (e) House

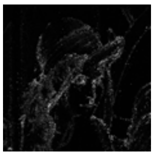
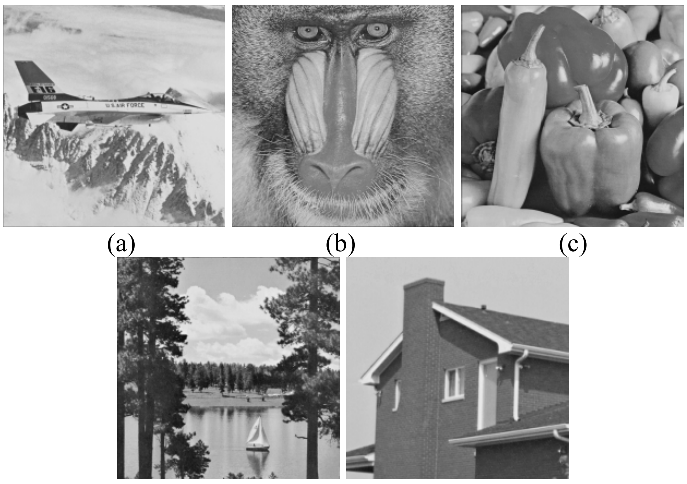


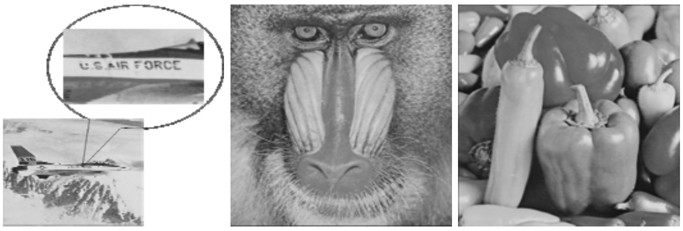
Fig. 10 the SOC image for the VQ indices of the image Lena (Fig. 8)



(a) (b) (c)

(d) (e)

Fig. 11 the five 512×512 stego-images



(a) (b) (c)

Fig. 12 the three damaged stego-images by slightly modifying the stego-image in Figs. 11(a)-11(c), respectively

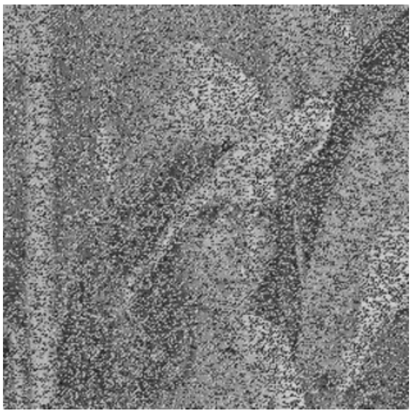


Fig. 13 the image revealed by all damaged stego-images in Fig. 12

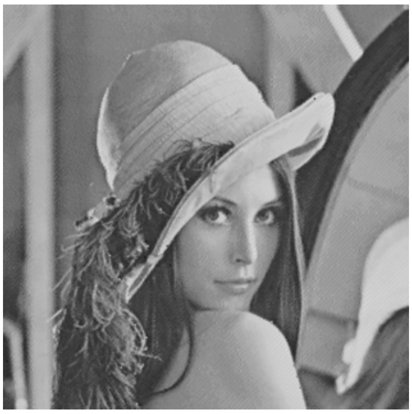
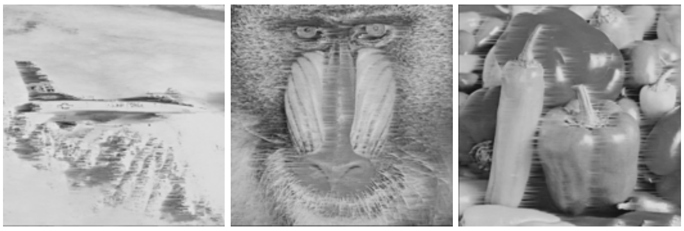


Fig. 14 the recovered image Lena'' by the SOC image in Fig. 10



(a) (b) (c)

Fig. 15 the three seriously damaged stego-images by adding noise to Figs. 11(a)-11(c), respectively

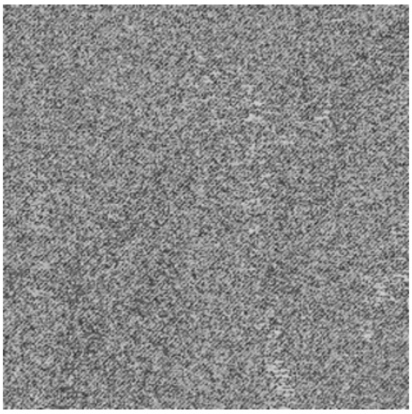


Fig. 16 the image revealed by all damaged stego-images in Fig. 15

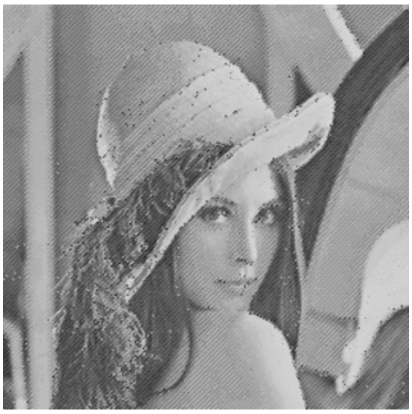
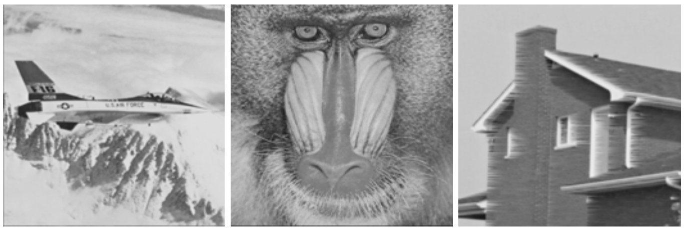


Fig. 17 the recovered image Lena''' by the SOC image in Fig. 10



(a) (b) (c)

Fig. 18 the three damaged stego-images by modifying the stego-images in Figs. 11(a), 11(b), and 11(e), correspondingly

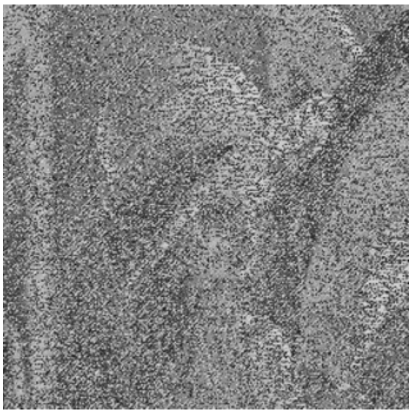


Fig. 19 the image revealed by all damaged stego-images in Fig. 18

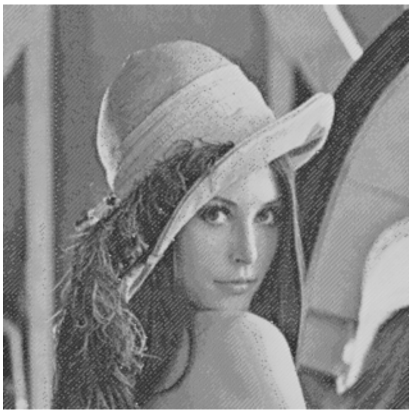


Fig. 20 the recovered image Lena'''' by the SOC image in Fig. 10

V. Discussion

A. SOC image Compression

There are usually many smooth areas in an image, and this will cause small search count. Because the SOC image only records the search count, the gray values in the SOC image are usually small. Table Ⅰ shows the occurrence frequencies of some pixel values of the SOC image for the image Pepper. For example, the gray values from 1 to 3 appear more than 100000 times in the SOC image of “Pepper”. On the other hand, the gray values greater than 200 seldom appear (each one appear in less than 100 times). Therefore, the SOC image can be efficiently compressed by the lossless compression method such as Huffman coding.

Table Ⅰ the occurrence frequencies of some pixel values of the SOC image for the image Pepper

Gray value	Occurrence frequencies	Gray value	Occurrence frequencies
1	19251	100	203
2	20551	101	193
3	19124	102	200
50	524	209	5
51	536	210	0
52	495	211	2

B. SOC image Security

The proposed method is secure because our SOC image does not directly record the information of the pixel values. In fact, the SOC image just records the search count of a pixel in the process of finding the previous point whose gray value is the same as that of the current pixel. Thus the secret image cannot be recovered by the SOC image alone. Although there are some contours can be seen on the SOC image, they can be scrambled by a random seed to prevent this condition. If the stealers want to guess the information of the original secret image according to the data recorded in the SOC image, they have to choose the most possible value among 256! different results to produce the secret image (since there are 256 values in the SOC image and). It is a very huge amount of work so that retrieving the secret image from the SOC image alone becomes extremely hard.

VI. Conclusion

This paper proposes an image recovery method based on SOC technique. With the auxiliary image generated by SOC, the damaged image can be repaired to a better one. Experiments show that the proposed method is not only useful with non-compressed image but also useful in VQ system. The occurrence frequencies of the pixel values in the SOC image show that the SOC image can be efficiently compressed by some lossless methods. Although the user can see some contours from the SOC image, it can be scrambled by a key. Therefore, the SOC image does not divulgate the information about the secret image.

There are three reasons why the technique of SOC image is better than duplicating the original secret image: 1) the scrambled SOC image reveals nothing about the secret image, and the SOC image is only useful when it is combined with the secret image (damaged or not); 2) if the secret image is destructed after sharing, there is no other way to obtain the secret image except retrieving it from the shadows, and when the number of the broken shadows exceeds $n-r$, the SOC image can be used to improve the quality of the damaged secret image; 3) if people want to duplicate the secret image to avoid the possible crash of the secret image, the risk that the secret image is stolen also increases.

References

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

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

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

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

[5] C. C. Thien, W. P. Fang, and J. C. Lin, “Sharing secret images by using base-transform and small-size host images,” *International Journal of Computer Science and Network Security*, vol. 6, no. 6, pp. 219-225, June 2006.

[6] S. K. Chen and J. C. Lin, “Fault-tolerant and progressive transmission of vector-quantized images,” *WSEAS Transactions on Signal Processing*, vol. 2, pp. 787-793, May, 2006.

[7] V. Srisarkun and C. Jittawiriyanukoon, “Image sharing over satellite communications using embedded secret code,” *WSEAS Transactions on Information Science and Applications*, vol. 3, no. 10, pp. 2047-2053, Oct. 2006.

[8] S. J. Lin and J. C. Lin, “VCPSS: A two-in-one two-decoding-options image sharing method combining visual cryptography (VC) and polynomial-style sharing (PSS) approaches,” *Pattern Recognition*, vol. 40, no. 12, pp. 3652-3666, Dec. 2007.

[9] W. K. Su, L. S. T. Chen, and J. C. Lin, “Fault-tolerant VQ-style secret image sharing,” *8th WSEAS International Conference on Applied Computer & Applied Computational Science*, pp. 40-43, May 2009.

[10] 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.

[11] C. S. Tsai, C. C. Chang, and T. S. Chen, “Sharing multiple secrets in digital images,” *The Journal of Systems and Software*, vol. 64, no. 2, pp. 163-170, 2002.

[12] M. Naor and A. Shamir, “Visual cryptography”, *Advances in Cryptology-EUROCRYPT’94*, Lecture Notes in Computer Science, vol. 950, pp. 1-12, 1995.

[13] C. C. Lin, and W. H. Tsai, “Visual cryptography for gray-level images by dithering techniques,” *Pattern Recognition Letters*, vol. 24, no. 1-3, pp. 349-358, Jan. 2003.

[14] Y. C. Hou, “Visual cryptography for color images,” *Pattern Recognition*, vol. 36, no. 7, pp. 1619-1629, July 2003.

[15] 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, Sep. 2004.

[16] 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.

[17] C. N. Yang and T. S. Chen, “Extended visual secret sharing schemes: improving the shadow image quality,” *International Journal of Pattern*

Recognition and Artificial Intelligence, vol. 21, no. 5, pp. 879-898, Aug. 2007.

[18] S. J. Shyu, S. Y. Huang, Y. K. Lee, R. Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography," *Pattern Recognition*, vol. 40, no. 12, pp. 3633−3651, Dec. 2007.

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

[20] M. Tompa and H. Woll, "How to share a secret with cheaters," *Journal of Cryptology*, vol. 1, no. 2, pp. 133-138, 1988.

[21] 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, Sep. 1995.

[22] 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.

[23] J. Lee and C. S. Won, "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.

[24] 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.

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.

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.

Shang-Kuan Chen received his B.S. degree in Applied Mathematics from Fu Jen Catholic University, Taiwan, in 1994, and M.S. degree in Applied Mathematics from National Chiao Tung University (NCTU), Taiwan, in 1998. In 2006, he received his Ph.D. degree in Computer Science from NCTU. His research interests include data hiding, visual cryptography, and image sharing. He joined the Department of Computer Science and Information Engineering at Yuanpei University in 2006 and is currently an assistant professor there.

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.