Journal of Information Hiding and Multimedia Signal Processing ©2015 ISSN 2073-4212
Ubiquitous International Volume **6**, Number **2**, March **2015**

A Lossy Secret Color Image Sharing Scheme with Small Shadows and Error-resilient Capability

Li Liu[1], An-Hong Wang[1,†], Chin-Chen Chang[2,3,*], Zhi-Hong Li[1], and Jin-bo Liu[1]

[1]College of Electronic Information and Engineering
Taiyuan University of Science and Technology, Taiyuan 030024, China.
skies5315@sina.com.cn; wah_ty@163.com; zy_lzh@sohu.com; 775134782@qq.com
†Correspondence Autor: wah_ty@163.com

[2,*]Department of Information Engineering and Computer Science,
Feng Chia University, Taichung 40724, Taiwan.
∗Correspondence Autor: alan3c@gmail.com

[3]Department of Computer Science and Information Engineering,
Asia University, Taichung 41354, Taiwan.

Received August, 2014; revised September, 2014

Abstract. *A novel secret sharing scheme for color images with small shadows and error-resilient capability was proposed that combines compressive sensing and Shamir's (k, n)-threshold scheme. Since the human eye is more sensitive to the luminance of an image than its chromaticity, first, this scheme converts RGB images into YUV format and compresses the components of luminance and chrominance using a different measurement rate. Then, the measurement values are quantified and encoded as polynomial coefficients in Shamir sharing to get n shadow images. At the receiver side, the secret image can be reconstructed if any k of n shadows are offered, while less than k shadows reveal no information. The simulation results showed that the scheme had a small shadow size and also achieved good error-resilient capability. Even though the shadow images may be affected by noise or a hostile attack in the transmission process resulting in some distortion, the managers still are able to reconstruct the original secret image. Therefore, this scheme provides advantages over others in the actual transmission environment.*

Keywords: Compressive sensing, Secret sharing, (k, n)-threshold scheme, Shadow image, Error-resilient capability

1. **Introduction.** With the rapid development of network technology, information hiding technology [1, 2, 3] has gained extensive attention. Secret sharing technology, one of the important ways of hiding information, has gradually become an issue of great interest in the field of information security. In 1979, Shamir [4] and Blakley [5] independently proposed the concept of (k, n)-threshold secret sharing. This concept is performed by dividing secret data into n shadows and distributing them to n different participants, each of whom holds one shadow. The secret data can be reconstructed if there is at least complete knowledge of $k(k \leq n)$ shadows, while $k-1$ shadows reveal no information. In 1995, Naor and Shamir [6] successfully extended this concept into the image domain and proposed a new secret image sharing scheme. This scheme divided the secret image into n noise-like shadow images, and then these shadows were transmitted over the open network instead of the secret image. Although the scheme had all of the merits of (k, n)-threshold

secret sharing, the problem of pixel expansion resulted in high transmission and storage costs.

Later, many secret image sharing schemes [7, 8, 9, 10, 11] were proposed that aimed to curtail the size of the shadow. Even so, only the scheme proposed by Chang et al. [9] is directly suitable for color images, because the amount of color-image data is triple the amount of gray-image data. This scheme combined the gradual search algorithm for one single bitmap block truncation coding (GSBTC) with the (k, n)-threshold scheme, thereby producing better results for the size of the shadows and the quality of the reconstructed image.

Another topic [12, 13, 14] related to error-resilient capability also has been discussed extensively by scholars, because noise and hostile attacks always exist in the actual transmission channel. Based on the theory of the (k, n)-threshold scheme, at most $(n - k)$ shadows are allowed for complete loss during the process of transmission. The remaining k shadows determine whether the original image can be reconstructed. If the scheme does not have a certain error-resilient capability, it can lead to the complete loss of the original image when the remaining k shadows have been damaged a little in the process of transmission.

In this paper, we proposed a lossy secret color-image sharing scheme with small shadows and error-resilient capability. First, this scheme employs compressed sensing (CS) to produce a few measurement values in order to compress the image and reduce the shadow size. Next, the (k, n)-threshold scheme was used to divide the data into n shadows in order to ensure the security of the secret image. So, the characteristics of our scheme are as follows: (1) It has a small shadow size and more easily adapts to different network environments; (2) It has a better error-resilient capability. It will get a better result for reconstructing the secret color image even if the shadows are distorted a little in the transmission process. Our experimental results proved the expected characteristics of the proposed scheme.

2. **Related Works.**

2.1. **Compressed Sensing (CS).**

According to theory of CS, if the signal can be represented by a small number of non-zero coefficients, it can be converted into a limited number of incoherent random measurements by constructing a suitable measurement matrix. These random measurements maintain the information of the reconstructed signal, so the original signal can be accurately reconstructed from a small number of measurements by solving the sparse optimization problem.

Assume that a real-valued signal, $x \in R^N$, is a k-sparse vector on an orthonormal basis $\Psi \in R^{N \times N}$, i.e., only $k(k \ll N)$ out of the N elements of x have non-zero values. Then

$$x = \Psi\theta, \tag{1}$$

where the coefficient θ can be well approximated by k non-zero values. So, a small number of linear random measurements $y \in R^m$, $k < m \ll N$ obtained as

$$y = \Phi x, \tag{2}$$

where $\Phi \in R^{m \times N}$ is a measurement matrix that is incoherent with Ψ and satisfies the restricted isometric property (RIP) [15].

Then, according to the given y, we can reconstruct signal x by solving the following optimization problem [16]:

$$\min_{\theta} \| \theta \|_1 \quad s.t. \quad y = \Phi\Psi\theta = \Phi x. \tag{3}$$

2.2. **Shamir's (k, n)-threshold scheme.** In general, assume that the secret S is a number. We can construct a $(k-1)$-degree polynomial function, $f(x)$, to divide S into n pieces $(S_1, S_2, ..., S_n)$. This function is defined as shown in Eq. (4).

$$f(x) = (a_0 + a_1 x + ... + a_{k-1} x^{k-1}) \pmod{g}, \tag{4}$$

where $a_0 = S$, $a_0 < g$, g is a random prime number, and $\{a_1, a_2, ...a_{k-1}\}$ are n random numbers within the range of $[0,\ g-1]$. Each S_i, which is calculated by Eq. (5), is considered to be a piece, and each S_i is given to the i^{th} participant.

$$S_i = (i, f(i)),\ 1 \le i \le n, \tag{5}$$

The secret S can be reconstructed from at least k pieces chosen randomly from n pieces. That is to say, when we collected any k pieces of n pieces, these coefficients $a_1, a_2, ...a_{k-1}$ of $f(x)$ can be calculated by the Lagrange interpolation formula as defined in Eq. (6), and then, the secret data $S = a_0$ can be extracted.

$$f(x) = \sum_{m=1}^{k} f(i_m) \prod_{r=1, r\neq m}^{k} \frac{x - i_r}{i_m - i_r} \pmod{g}. \tag{6}$$

3. **Proposed Scheme.** Figure 1 shows that the operating steps consist of a sending and a receiving phase. The human eye is more sensitive to luminance of an image than its chrominance, so it is unable to perceive even significant reductions in chromaticity component. So we used the YUV format in our scheme to process color images. The detailed steps of sending phase are described below.

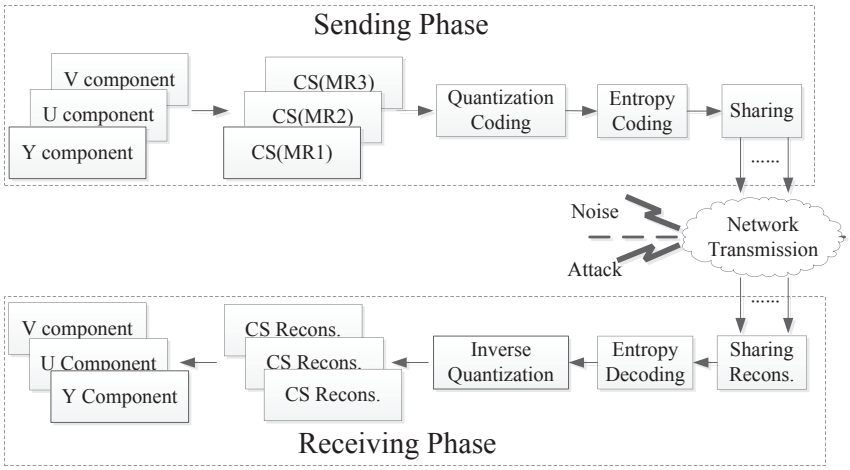


FIGURE 1. Diagram of the proposed system

Sending Phase.

Input. an RGB color image.

Output. n shadow images.

Steps.

Step 1. Extracting the luminance component Y and chromaticity components U and V from the color image.

Step 2. Measure every component by CS using different measurement rates (MRs) to generate a few random measurements y, where MR is the ratio of the number of measurements to the length of the signal). Because Y is more important than U and V,

we set measurement rate MR1 in Y to be greater than measurement rates MR2 and MR3 in U and V, respectively, where $MRi \in [0, 1]$.

Step3. Random measurements y are quantized using non-uniform 8-bit quantization to satisfy the request of sharing coefficients for the image sharing, and every 8 bits from the quantization coding are processed sequentially into a decimal number.

Step4. Using entropy coding to further compress these decimal number, there is no distortion in this step.

Step5. The processed numbers in the above step become the coefficients of the sharing function $f(x)$, and then, n shadows are generated according to the theory of Subsection 2.2.

Then, the n shadows were transmitted in actual channel.

The process of the receiving phase is the inverse of the process of the sending phase. To extract a compressed secret color image, at least any k of n shadows must be collected in advance. Then, the k collected shadows are used to reconstruct the sharing coefficients. Entropy decoding and inverse quantization were implemented to determine measurements and then the original secret color image was reconstructed according to the theory of Subsection 2.1.

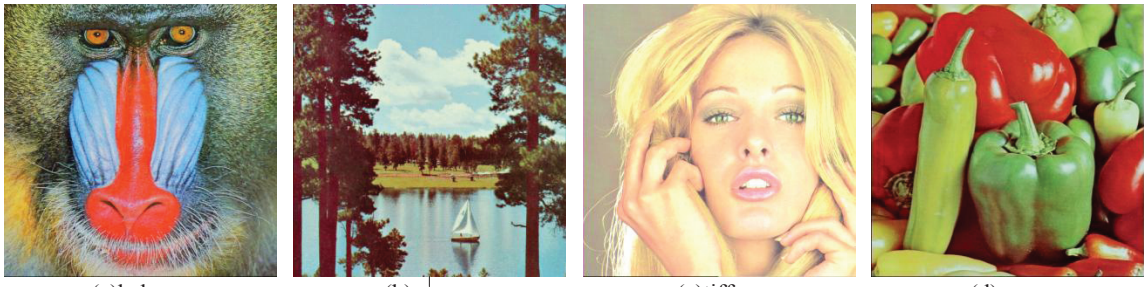
4. **Experimental Results.** The experimental results presented in this section demonstrate the performance of our proposed scheme. Figure 2 shows the four 512×512 color images (baboon, scenes, tiffany, peppers) that were used to conduct the experiments. The peak signal-to-noise ratio ($PSNR$) was used to evaluate the image quality of the reconstructed secret color image. $PSNR$ is defined as

$$PSNR = 10log_{10}(\frac{255^2}{MSE}), \tag{7}$$

where MSE is the mean square error between the original color image and the reconstructed color image.

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{(R_{ij} - R'_{ij})^2 + (G_{ij} - G'_{ij})^2 + (B_{ij} - B'_{ij})^2}{3}. \tag{8}$$

where $m \times n$ is the size of the original color image, and R_{ij}, G_{ij}, B_{ij} are the pixel values of the three primary colors, i.e., R, G, and B in the original color image, and $R'_{ij}, G'_{ij}, B'_{ij}$ are the pixel values of the three primary colors, i.e., R, G, and B in the reconstructed color image.



(a)baboon (b)scenes (c)tiffany (d)peppers

FIGURE 2. Four test color images: (a)baboon; (b)scenes; (c)tiffany; (d)peppers

To demonstrate the performance of our proposed scheme, a $(2, 4)$-threshold secret sharing was used, and the size of the generated shadows changed with the different MR values. Usually, the MR of the Y component has a decisive role in the quality of the reconstructed

color image. So we set the MRs of the U and V components to 0.1, and the quality of the reconstructed color image can be improved by increasing the MR of Y.

Figure 3 compares the four shadows for our proposed scheme with those of Chang et al.'s scheme [9]. Figure 3(a) is the original secret color image "peppers." Figure 3(b) is the reconstructed color image using our proposed scheme, and its PSNR was 34.75 dB when the MR of Y was 0.5. Figure 3(d) shows the four shadows with sizes of 284×201 pixels in our proposed scheme. Another four shadows with sizes of 256×256 pixels in Ref. [9] are shown in Figure 3(e), and its reconstructed color image, with a PSNR of 29.15 dB, is shown in Figure 3(c). From Figures 3(d) and 3(e), it is apparent that these shadows are all noise-like grayscale images, and we cannot determine any information about the original image from them.

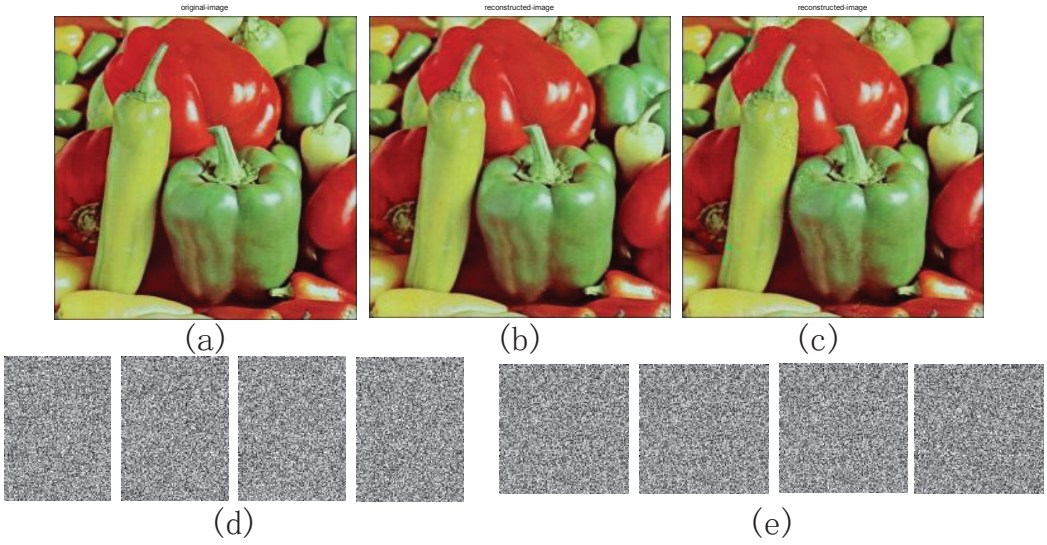


FIGURE 3. (a) original secret color image "peppers"; (b) reconstructed color image with PSNR=34.75 dB in our proposed scheme; (c) reconstructed color image with PSNR=29.15 dB in Ref. [9]; (d) four shadow images with 284×201 in our proposed scheme; (e) four shadow images with 256×256 in Ref. [9]

Table 1 summarizes the sizes in bytes of the shadow images generated using our proposed scheme for different values of MR and $PSNR$ of the reconstructed image; the table also compares the performance of our proposed scheme with the performance of Chang et al.'s scheme [9]. As can be seen from this table, our proposed scheme can obtain different sizes (in bytes) of the shadows by adjusting the MR of Y, and our proposed scheme has smaller shadows when the $PSNR$ values of the reconstructed color image are very close.

Another important performance of our scheme was its error-resilient capability. Assume that the two shadows used for reconstruction were transmitted in an identical channel environment with binary pulse amplitude modulation (BPAM) baseband signals and controllable additive white Gaussian noise (AWGN) [17]. Figure 4 shows the transmission characteristic of this system [17]. We used the received shadows to reconstruct the original secret color image and compute the $PSNRs$ that corresponded to each the bit-error rates (BERs), and the results are shown in Figure 5.

Figure 5 shows that our proposed scheme has a certain error-resilient capability. Even if the channel was disturbed by a certain noise ($BER < 10^{-3}$) that lead to a small distortion of the shadows, the original color image also can be reconstructed, and the quality of the

TABLE 1. Comparison of the data provided for the test color images by the proposed scheme with the data provided by Chang et al.'s scheme [9]

Image	Our proposed scheme			The scheme in Ref.[9]	
	MR of Y	Size of Shadows(Bytes)	$PSNR(dB)$ of Reconstruction	Size of Shadows(Bytes)	$PSNR(dB)$ of Reconstruction
baboon	0.4	49337	22.47	65536	23.70
	0.5	58668	23.24		
	0.6	64238	23.63		
scenes	0.4	49286	28.28	65536	28.28
	0.5	56979	29.08		
	0.6	65724	30.13		
tiffany	0.4	32699	29.63	65536	29.85
	0.5	40279	29.86		
	0.6	49574	31.57		
peppers	0.4	44248	33.95	65536	29.15
	0.5	56997	34.75		
	0.6	61117	35.51		

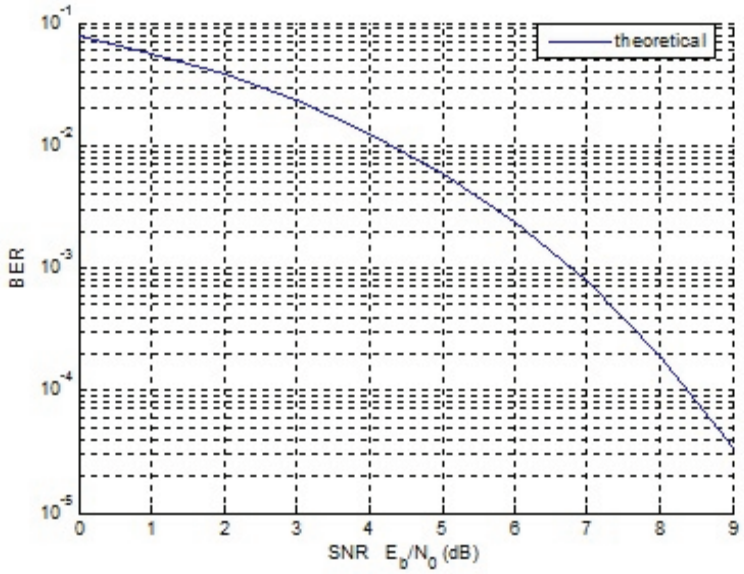


FIGURE 4. Graph of the transmission characteristic in selected communication system

reconstruction was acceptable to the human eye. But in the Chang et al.'s scheme [9], a one-pixel difference caused a significant difference in each shadow. That means any change in each shadow could lead to failing to recover the original secret image. So their scheme has no error-resilient capability.

5. **Conclusions.** In this paper, a lossy secret color image sharing scheme with small shadows and error-resilient capability was proposed. Because we used compressed sensing (CS) and the (k, n)-threshold secret sharing scheme, our proposed scheme has the following two advantages over the scheme in Ref. [9]: (1) Its shadows are small in size facilitating its operability with different network environment and (2) it has better error-resilient capability, both of which make our scheme more practical for the intended use. However,

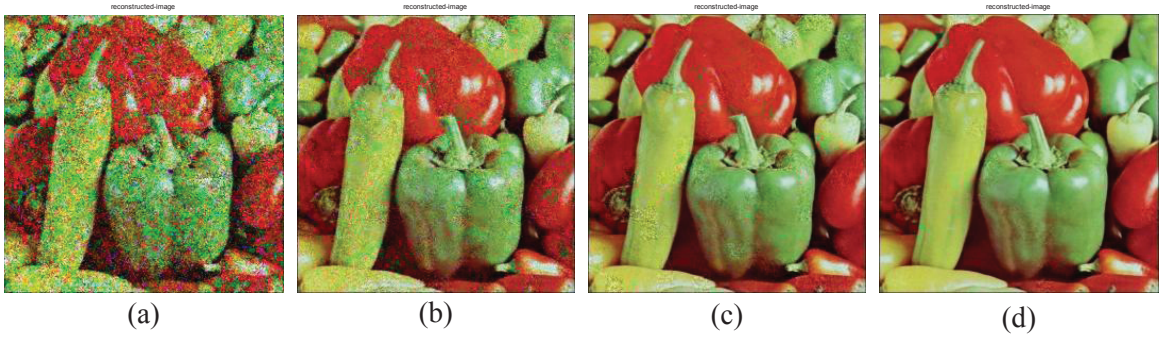


FIGURE 5. Reconstructed image of our scheme with the indicated BER and the resulting $PSNR$: (a)$BER = 2 \times 10^{-2}, PSNR = 14.68dB$; (b)$BER = 3 \times 10^{-3}, PSNR = 21.41dB$; (c)$BER = 8 \times 10^{-4}, PSNR = 26.51dB$; (d)$BER = 2 \times 10^{-4}, PSNR = 32.60dB$

because the compressed sensing of our scheme uses lossy compression, the proposed scheme cannot be used in the medical and military field, which required better image quality.

Acknowledgment. We would like acknowledge the supports from the National Natural Science Foundation of China (No.61272262), The Shanxi Provincial Foundation for Leaders of Disciplines in Science (20111022), Shanxi province Talent Introduction and Development Fund (2011), Shanxi Provincial Natural Science Foundation?012011014-3? YSTRF of TYUST (No.20123004), UIT of TYUST (No.xj2013007).

REFERENCES

[1] J.S. Pan, H.C. Huang and L.C. Jain, *Intelligent Watermarking Techniques*, World Scientific Publishing Company, Singapore, 2004.
[2] J.S. Pan, H.C. Huang, L.C. Jain, and W.C. Fang, *Intelligent Multimedia Data Hiding: New Directions*, Springer, Berlin-Heidelberg, Germany, 2007.
[3] J.S. Pan, W. Li, C.S. Yang, and L.J. Yan, Image steganography based on subsampling and compressive sensing, *Multimedia Tools and Applications*, pp. 1-15, 2014.
[4] A. Shamir, How to Share a Secret, *Communication of ACM*, vol. 24, no. 11, pp. 612-613, 1979.
[5] G.R. Blakley, Safeguarding cryptographic keys, *Proc. of the National Computer Conference* , New York, USA, pp. 313-317, 1979.
[6] M. Naor, A. Shamir, Visual Cryptography, *Proc. of Advances in Ctyptology-EUROCRYPT'94*, Berlin, Gemany , pp.1-12, 1995.
[7] C. Thien, J. Lin, Secret Image Sharing, *Computer Graphics*, vol. 26, no. 1, pp. 765-770, 2002.
[8] R.Z. Wang, C.H. Su, Secret Image sharing with smaller shadow images, *Pattern Recognition Letters*, vol. 27, no. 6, pp. 551-555, 2006.
[9] C.C. Chang, C.C. Lin, C.H. Lin and Y.H.Chen, A novel secret image sharing scheme in color images using small shadow images, *Information Sciences*, vol. 178, no. 11, pp. 2433-2447, 2008.
[10] C.C. Chang, W.L. Tai, and C.C. Lin, Hiding a secret colour image in two colour images, *Imaging Science Journal*, vol. 53, no. 4, pp. 229-240, 2005.
[11] Y.X. Liu, C.N. Yang, and P.H. Yeh, Reducing shadow size in smooth scalable secret image sharing, *Security and Communication Networks*, 2014.
[12] C.P. Huang, Secure, error-resilient, and real-time progressive image transmission, *Optical Engineering*, vol. 48, no. 12, pp. 127001, 2009.
[13] S.K. Chen, J.C. Lin, Secure, Fault-tolerant and progressive transmission of images, *Pattern Recognition*, vol. 38, no. 12, pp. 2466-2471, 2005.
[14] L. Liu, A.H. Wang, C.C. Chang, A novel real-time and progressive secret image sharing with flexible shadows based on compressive sensing, *Signal Processing: Image Communication*, vol. 29, no. 1, pp. 128-134, 2014.

[15] E. Candes, Compressive Sampling, *Proc. of International Congress of Mathematicians*, Madrid, Spain, pp. 1-20, 2006.
[16] D.L. Donoho, Compressed Sensing, *IEEE Trans. on Information Theory*, vol.52, no. 4, pp. 1289-1306, 2006.
[17] J.G. Proakis, M. Salehi, *Communication Systems Engineering: 2nd ed*, Prentice Hall, Englewood Cliffs, 2002.