Color Image Encryption Algorithm Combining Compressive Sensing with Arnold Transform

Aidi Zhang[1], Nanrun Zhou[1,2 *]
1. Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China
2. National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876,China
adiun@163.com, znr21@163.com

Lihua Gong
Jiangxi Province Key Laboratory of Image Processing and Pattern Recognition, Nanchang Hangkong University, 330063 Nanchang, China
lhgong@ncu.edu.cn

***Abstract*—A new color image encryption algorithm combining compressive sensing with Arnold transform is proposed, which can encrypt the color image into a gray image. Considering the dimensional reduction and random projection of compressive sensing, we utilize compressive sensing to encrypt and compress the three color components of color image simultaneously. The three encrypted and compressed color components' dimensions are smaller than the original image, thus they can be grouped into a gray image, and then the gray image is scrambled by Arnold transform to enhance the security. The proposed algorithm can also be applied in the multiple-image encryption. The experimental results show the validity and the reliability of the proposed algorithm.**

***Index Terms*—compressive sensing, color image encryption, Arnold transform**

I. INTRODUCTION

With the development of multimedia technology, more and more information comes from images. The security of images becomes a serious issue. F Huang and X Qu proposed an image encryption algorithm based on compound two-dimensional maps [1]. A robust watermarking against shearing based on improved S-Radom transformation was proposed [2]. A new public-key cryptosystem based on two-dimensional discrete logarithm problem (DLP) was proposed to shorten the key length and improve the encryption efficiency [3].

Compressive sensing (CS) [4, 5] is a new powerful signal sampling technology, which has gained lots of interest due to its special ability to reconstruct the sparse signal from a relatively smaller sampling set. Since its characteristics of dimensional reduction and random projection, some image encryption-compression algorithms based on compressive sensing have been proposed recently. X Zhang and Y Ren proposed a scheme to compress and decompress encrypted image based on CS where the whole orthogonal transform was a secret [6]. The security of resisting against the brute force and structured attacks was researched [7]. AV Sreedhanya and KP Soman proposed a scheme where both compressive sensing and Arnold scrambling are employed to encrypt color image [8]. An image encryption method based on compressive sensing and double random-phase encoding was proposed [9], which can lower the data volume for encryption due to the dimensional decrease properties of CS. R Huang, KH Rhee and S Uchida proposed a parallel image encryption method based on CS where block cipher structure consisting of scrambling, mixing, S-box and chaotic lattice XOR is designed to further encrypt the quantized measurement data [10]. The anti-packet loss ability of the CS-based encryption method was quantified to overcome the inevitable problem of packet loss during wireless transmission [11]. A Orsdemir and HO Altun investigated the security and the robustness of encryption via compressive sensing and their results indicate that the CS based encryption is computationally secure [12]. Y Rachlin and D Baron researched the security when eavesdroppers have no idea of the measurement matrix and demonstrated a computational notion of secrecy [13].

Color images are more beautiful in vision and carry more information than gray images, thus color image encryption has become an important subject for information security. We explore a color image encryption algorithm combining CS with Arnold transform, where the three color components are encrypted and compressed to be a gray image, which can confuse the attacker. And then the gray image is scrambled by Arnold transform to enhance the security. The proposed algorithm can also be used in the multiple-image encryption case.

The rest of this paper is organized as follows: some fundamental knowledge is related in Section 2, the proposed color image encryption algorithm is introduced in Section 3, experimental results and analysis are given

* Corresponding author: Nanrun Zhou.

doi:10.4304/jcp.8.11.2857-2863

in Section 4, and we conclude the paper in the final section.

II. Fundamental Knowledge

A. Compressive Sensing

CS is a novel sample theory, which can reconstruct original signal by directly sampling a sparse or compressible signal at a rate much lower than the Nyquist rate. For a 1-D signal x with length N, its transform coefficient α is

$$\alpha = \Psi^{\mathrm{T}} x, \tag{1}$$

where Ψ is an $N \times N$ orthogonal transform matrix. In a general case, most of the coefficients in α are close to zero and only few large coefficients capture the principal information of the signal. Suppose that M measurements of x are taken through the following linear measurement

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

where Φ is an $M \times N$ matrix and y is an $M \times 1$ vector which maintains the space structure of the signal x, M is the number of measurements. If the measurement matrix Φ satisfies RIP [4], x can be approximately recovered from the M measurements.

To recover the signal x, it is required to estimate the sparest solution to $y = \Phi x = \Phi\Psi\alpha$. The problem of estimating the sparse solution can be expressed as

$$\min \|x\|_0 \text{ subject to } y = \Phi\Psi\alpha. \tag{3}$$

The above problem may be solved by exhaustive combinatorial search. Unfortunately, it will become an NP-hard problem for large N. To overcome this problem, some reconstruction algorithms, such as matching pursuit algorithm (MP) [14], orthogonal matching pursuit algorithm (OMP) [15] and smooth l^0 algorithm (SL_0) [16] and so on, have been developed. SL_0 will be adopted in our proposed algorithm.

B. Arnold Transform

Arnold transform is commonly used to scramble pixels' locations. The transform is a process of clipping and splicing that realigns the pixel matrix of digital image. Arnold transform is defined as the point (x, y) in the square matrix transforms into the other point (x', y'):

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\mathrm{mod}\ N), \tag{4}$$

where N is the order of the square matrix, x, $y \in \{1, 2, \ldots, N-1\}$. For a digital image of size $N \times N$, the original image can be recovered after undergoing period s numbers of iteration.

III. Color Image Encryption Algorithm Combining CS with Arnold Transform

The process of the proposed algorithm is shown in Fig. 1. Suppose the size of original color image is $N \times N$, the color image is encrypted as follows:

Step 1: Generate three measurement matrices, $\Phi_{M_1 \times N}$, $\Phi_{M_2 \times N}$, $\Phi_{M_3 \times N}$, by using keys specified by the sender, where $M_1 + M_2 + M_3 = N$. Measure the red, green and blue components, I_R, I_G and I_B, with matrices $\Phi_{M_1 \times N}$, $\Phi_{M_2 \times N}$ and $\Phi_{M_3 \times N}$, respectively. C_R, C_G and C_B are the measurements corresponding to the red, green and blue components. M_1, M_2, M_3 can be treated as sub-keys;

Step 2: Since $M_1 + M_2 + M_3 = N$, the measurements C_R, C_G and C_B can be grouped into a gray image C_N,

$$\begin{cases} C_N(1: M_1, :) = C_R \\ C_N(M_1 + 1: M_1 + M_2, :) = C_G \\ C_N(M_1 + M_2 + 1: N, :) = C_B \end{cases}, \tag{5}$$

where $C_N(i: j, :)$ means the partial matrix grouped by the vectors from *i*-th row to *j*-th row vectors of C_N;

Step 3: Perform T times Arnold transform on C_N to obtain the encrypted image C, T is the key.

In the decryption process, firstly perform $s - T$ times Arnold transform on the encrypted image to recover C_N,

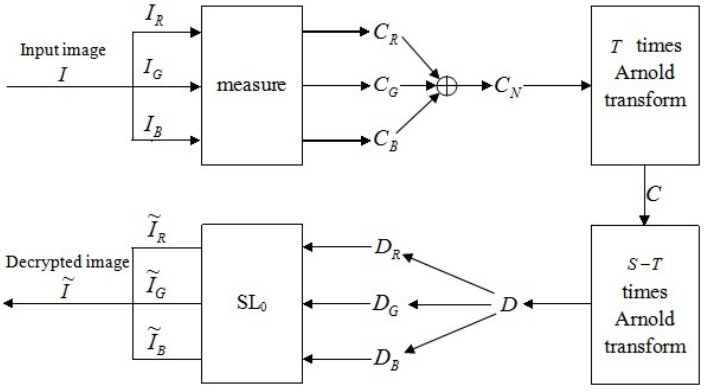


Figure 1. The process of the proposed encryption algorithm

note the recovered matrix as D, and then D_R, D_G and D_B can be obtained as:

$$\begin{cases} D_R = D(1:M_1,:) \\ D_G = D(M_1+1:M_1+M_2,:) \\ D_B = D(M_1+M_2+1:N,:) \end{cases} \cdot \quad (6)$$

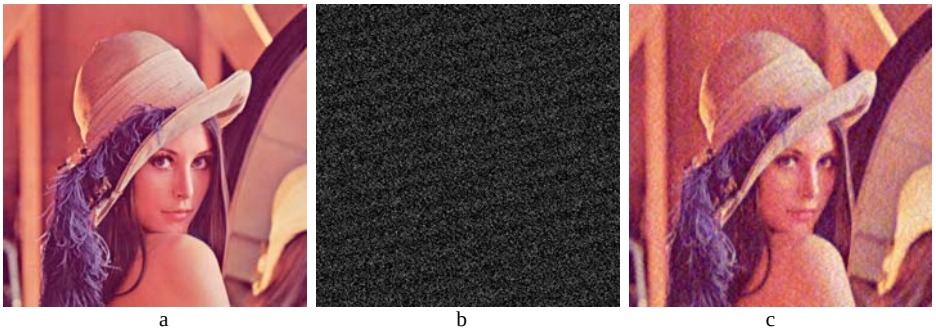
The decrypted color image $\tilde{I}$ can be obtained with three color components $\tilde{I}_R$, $\tilde{I}_G$, and $\tilde{I}_B$, which are obtained by performing the SL_0 reconstruction algorithm on D_R, D_G, and D_B, respectively.

IV. Experimental Results and Analysis

The color image 'Lena' with resolution 512×512 is served as the test image, which is shown in Fig. 2(a). Thus the period of Arnold can be computed as $s = 384$. Without loss of generality, Ψ is set as 2D-DCT. The parameters in the experiment are $M_1 = 200$, $M_2 = 200$, $M_3 = 112$ and $T = 30$. And the measurement matrices are generated by the random number generation function in matlab.R2011a (version 7.12.0.635). Fig. 2(b) is the encrypted image and Fig. 2(c) is the correct decrypted Lena. The encrypted image shows not any information of the original image visually.

A. Statistical Analysis Attack

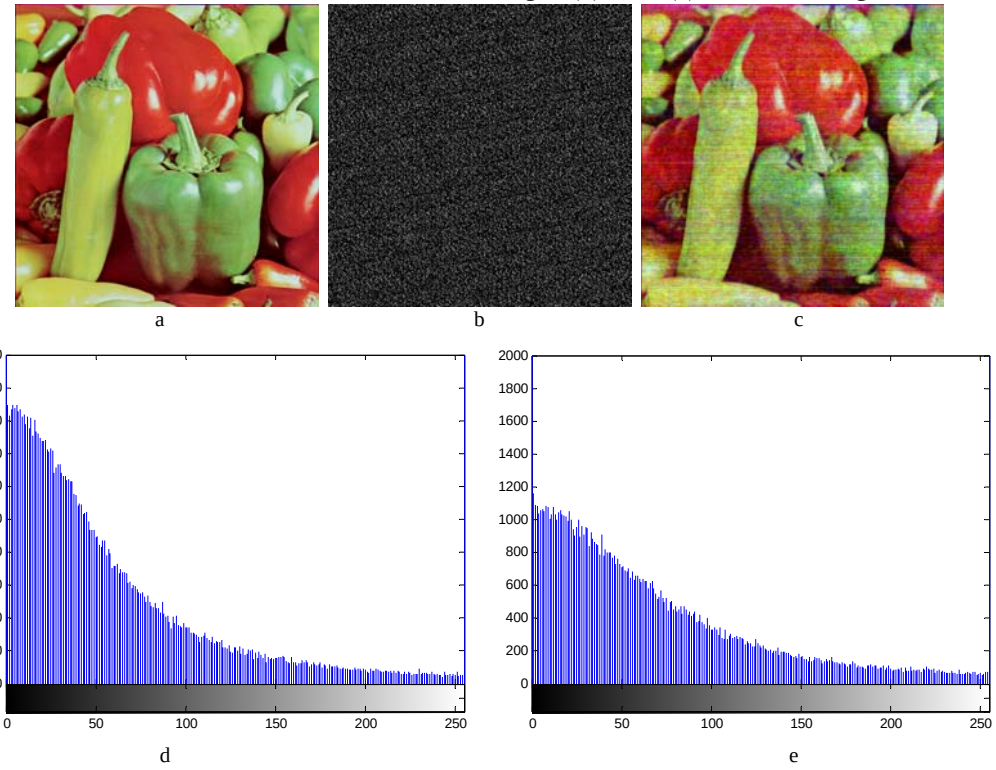
Statistical analysis of the proposed image encryption algorithm is tested from two aspects. One is to test the histograms of the encrypted images of different color images and the other is to test the correlations of adjacent pixels of the plain image and its corresponding encrypted image.



a b c

Figure 2. (a) Lena; (b) encrypted Lena; (c) decrypted Lena with correct keys

Fig. 3(a)-(c) display the color image 'Peppers', encrypted 'Peppers' and its decrypted image, respectively. Fig. 3(d) and (e) are the histograms of the encrypted



a b c

d e

Figure 3. (a) Peppers; (b) encrypted Peppers; (c) correct decrypted Peppers; (d) histogram of encrypted Lena; (e) histogram of encrypted Peppers.

'Lena' and encrypted 'Peppers', respectively. The two color images are different from each other obviously, while the histograms of their encrypted images are very similar. After a large number of parallel experiments, we conclude that the histograms of the ciphertexts of different original images are similar to Fig. 3(d) and (e). That is to say, the attackers cannot obtain any valid information by analyzing the histograms of the encrypted images.

The correlation coefficient r_{xy} of any two adjacent pixels is calculated as follows:

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{7}$$

$$\mathrm{cov}(x, y) = \frac{1}{K}\sum_{i=1}^{K}\left[\left(x_i - E(x)\right)\left(y_i - E(y)\right)\right], \tag{8}$$

where x and y are the gray levels in two adjacent pixels of the image, k is the number of pixels, $E(a) = \frac{1}{K}\sum_{i=1}^{K} a_i$, and $D(a) = \frac{1}{K}\sum_{i=1}^{K}\left[a_i - E\left(a\right)\right]^2$.

The locations of the pixels are scrambled and the tight relationship between the adjacent pixels is removed since the introduction of Arnold scrambling. To test the correlations between two adjacent vertical, horizontal and diagonal pixels in the original and encrypted images, 18000 pairs of adjacent pixels are chosen randomly. Table 1 shows the results of correlation coefficients of the original image and the encrypted one. The correlation of the plaintext is close to 1 in each direction of each component, while the correlation of the encrypted image is close to 0 in each direction. That is to say, the proposed algorithm removes the tight relationship between adjacent pixels of the original image successfully. The results indicate that the proposed algorithm has the ability to resist statistical analysis.

TABLE I.

COORRELATIONS OF TWO ADJACENT PIXELS

Correlation coefficient	Original image			Encrypted image
	R	G	B	
Horizontal	0.9893	0.9824	0.9583	−0.0618
Vertical	0.9796	0.9690	0.9360	0.0347
Diagonal	0.9680	0.9560	0.9206	−0.0364

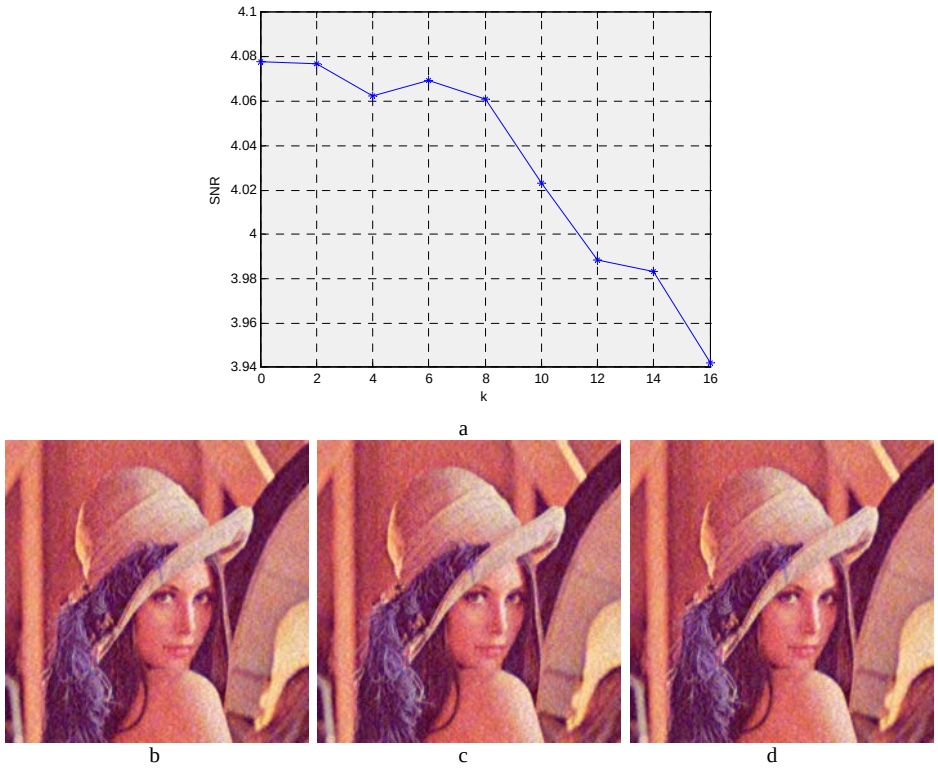
B. *Noise Attack*

It is inevitable that the encrypted image would be contaminated by noise at the stage of image processing and image transmission. Suppose the encrypted image is contaminated by noise as:

$$C' = C + kG, \tag{9}$$

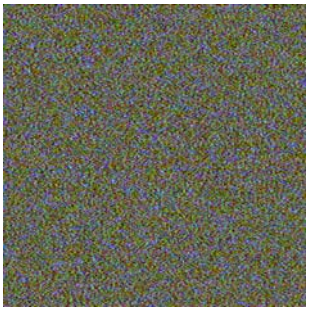
where C' and C are the noisy encrypted image and the original encrypted one, respectively. k indicates the noise strength, and G is the Gaussian white noise with zero-mean and identity standard deviation.

Signal-to-Noise Ration (SNR) is used to judge the quality of the decrypted digital image.

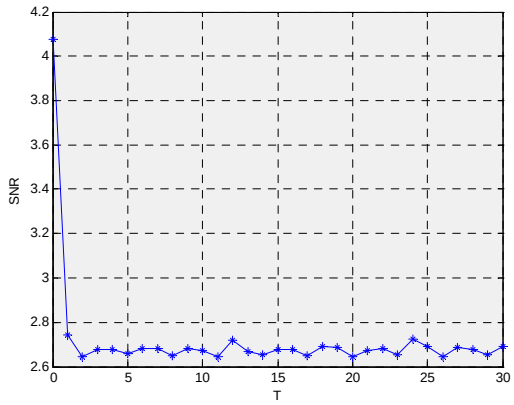


a b c d

Figure 4. Results of noise attack: (a) PSNR curve, (b) $k=1$, (c) $k=4$, (d) $k=8$



a



b

Figure 5. (a) Decrypted Lena with wrong iteration number $T = 31$; (b) SNR curve for iteration number T

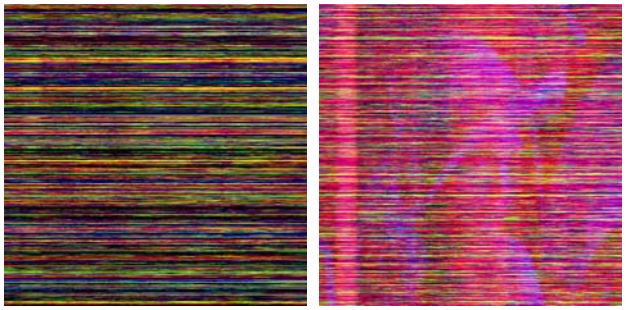
$$\mathrm{SNR} = \frac{\sum_{x=1}^{N}\sum_{y=1}^{N}\left|I(x,y)\right|^2 / 3}{\sum_{x=1}^{N}\sum_{y=1}^{N}\left|I(x,y)-\tilde{I}(x,y)\right|^2 / 3}, \qquad (10)$$

where $I(x,y)$ and $\tilde{I}(x,y)$ denote the values of the original image and the decrypted one for the pixel (x,y).

To test the ability of the proposed method to resist the noise attack, the Gaussian noises with different noise strengths are added to the encrypted image. The SNR versus noise strength is shown in Fig. 4(a). Fig. 4(b)-(d) show the decrypted images with $k = 1$, 4, and 8. It is easy to see that the decrypted images can still be recognized with some level of noise. That is to say, the proposed color image encryption algorithm has the ability to resist the noise attack.

C. Test with Wrong Iteration Number of Arnold Transform

Arnold transform is used to scramble the gray image grouped by the measurements. The attacker cannot obtain the correct measurements when he decrypts the image with the wrong iteration number of Arnold transform, thus the attacker cannot decrypt the image correctly. In the experiment, the iteration number in the encryption process is $T = 30$, thus the iteration number in the decryption process should be $s - T = 354$. Fig. 5(a) shows the decrypted image with wrong iteration number of Arnold transform. The wrong decrypted image cannot show any information of original image. Fig. 5(b) shows the SNR curve for the iteration number. The SNR is big only when the iteration number is correct, or else it is very small, which means that the quality of the decrypted image is too bad to recognize if the iteration number is wrong.



a b

Figure 6. Decrypted Lena with (a) wrong keys of measurement matrices; (b) wrong $M_1 = 199$ and $M_2 = 201$

D. Test with Wrong Measurement Matrices of CS

There are two cases that make the measurement matrices wrong, one is the wrong keys to generate the measurement matrices, and the other is the wrong size of matrices with correct keys, i.e., at least two parameters among M_1, M_2 and M_3 are wrong. The parameter in the control function of random number generation is 100. Fig. 6(a) shows the decrypted image when the parameter in the control function is 101, it is clear that no any useful information of the original image was shown in the wrong decrypted image. And Fig. 6(b) shows the decrypted image with wrong sizes of matrices ($M_1 = 199$ and $M_2 = 201$), the decrypted image is so fuzzy that the attacker can obtain a little information of the original image. That is to say, the proposed algorithm is sensitive to the keys to some degree. And if the measurement matrices are designed well, the proposed algorithm may become more sensitive.

E. Multiple-image Encryption

The proposed color image encryption algorithm can also be applied into multiple-image encryption. Fig. 7(a) and 7(b) show the gray image 'Lena' and gray image 'Baboon', respectively. Both of them are with resolution 512×512. With the proposed algorithm, they can be encrypted to be a gray image. The parameters in experiment are $M_1 = 212$, $M_2 = 300$ and $T = 30$. 7(c) is the encrypted image, 7(d) and 7(e) are the decrypted Lena and Baboon, respectively. The encrypted image looks like a random gray image and shows not any meaningful information about both images. The correct decrypted images show the main information of the original images. That is to say the proposed algorithm can be used to encrypt multiple-image, while it's not a good idea to encrypt too many images as the quality of the decrypted image corresponding to the small M_i may be too bad to recognize.

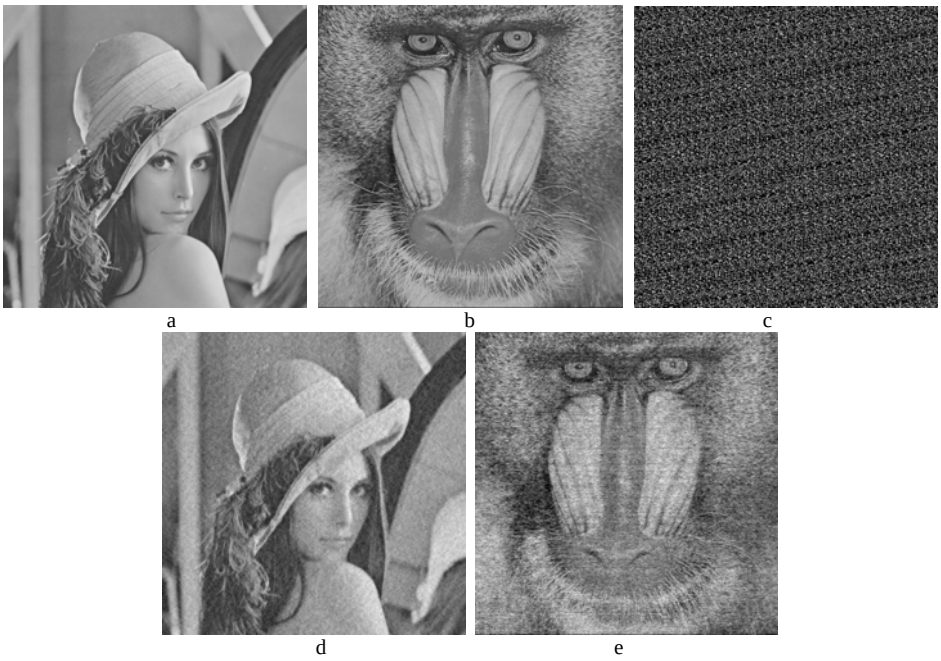


Figure 7. (a) Lena; (b) Baboon; (c) encrypted image; (d) decrypted Lena; (e) decrypted Baboon

V. CONCLUSION

A new color image encryption algorithm based on compressive sensing and Arnold transform is proposed. The three color components are encrypted and compressed simultaneously. They are grouped into a new gray image, and then the gray image is scrambled by Arnold transform to enhance the security. It is shown that the proposed algorithm is resistant to statistical analysis and brute-force attack, robust against noise attack and can be extended to multiple-image encryption.

ACKNOWLEDGMENT

The work is supported by the National Natural Science Foundation of China (Grant Nos. 61262084 and 61141007), the Foundation for Young Scientists of Jiangxi Province (Jinggang Star) (Grant No. 20122BCB23002), the Natural Science Foundation of Jiangxi Province, China (Grant No. 20132BAB201019), and the Opening Project of Key Laboratory of Image Processing and Pattern Recognition (Nanchang Hangkong University), Jiangxi Province (Grant No. TX201204002).

REFERENCES

[1] F. Huang, X. Qu, "Design of image encryption algorithm based on compound two-dimensional maps," *Journal of Software*, vol. 6, pp. 1953-1960, 2011.

[2] M. Deng, Q. Zeng and X. Zhou, "A robust watermarking against shearing based on improved S-Radon transformation," *Journal of Computers*, vol. 7, pp. 2549-2556, 2012.

[3] X. Zhang, G. Zhu, W. Wang, M. Wang and S. Ma, "New public-key cryptosystem based on two-dimensional DLP," *Journal of Computers*, vol. 7, pp. 169-178, 2012.

[4] D. L. Donoho, "Compressed sensing," *IEEE Transactions on Information Theory*, vol. 52, pp. 1289-1306, 2006.

[5] E. J. Candè s, "Compressive sampling," *International Congress of Mathematicians*, pp. 1433-1452, 2006.

[6] X. Zhang, Y. Ren, G. Feng and Z. Qian, "Compressing encrypted image using compressive sensing," *2011 7th International Conference on Intelligent Information Hiding and Multimedias Signal Processing (IIH-MSP)*, pp. 222-225, 2011.

[7] A. M. Abdulghani, E. R. Villegas, "Compressive sensing: from "compressing while sampling" to "compressing and securing while sampling"," *32nd Annual International Conference on IEEE EMBS*, pp. 1127-1130, 2010.

[8] A. V. Sreedhanya and K. P. Soman, "Secrecy of cryptography with compressed sensing," *International Conference on Advances in Computing and Communications*, pp. 207-210, 2012.

[9] P. Lu, Z. Xu, X. Lu and X. Liu, "Digital image information encryption based on Compressive Sensing and double random-phase encoding technique," *Optik-International Journal for Light and Electron Optics*, vol. 124, pp. 2514-2518, 2013.

[10] R. Huang, K. H. Rhee and S. Uchida, "A parallel image encryption method based on compressive sensing," *Multimedia Tools and Applications*, pp. 1-23, 2012.

[11] D. H. Liu, G. M. Shi, D. H. Liu and M. Gao, "A robust image encryption scheme over wireless channels," *International Conference on Wireless Communication & Signal Processing*, pp. 1-6, 2009.

[12] A. Orsdemir, H. O. Altun, G. Sharma, and M. F. Bocko, "On the security and robustness of encryption via compressed sensing," *IEEE Military Communications Conference*, pp. 1-7, 2008.

[13] Y. Rachlin, R. D. Baron, "The secrecy of compressed sensing measurements," *2008 46th Annual Allerton Conference Communication, Control, and Computing*, pp. 813-817, 2008.

[14] S. G. Mallat, Z. Zhang, "Matching pursuits with time-frequency dictionaries," *IEEE Transaction on Signal Processing*, vol. 41, pp. 3397-3415, 1993.

[15] E. Liu, V. N. Temlyakov, "The orthogonal super greedy algorithm and application in compressed sensing," *IEEE Transactions on Information Theory*, vol. 58, pp. 2040-2047, 2012.
[16] H. Mohimani, M. B. Zadeh and C. Jutten, "A fast approach for over-complete sparse decomposition based on smoothed l^0 norm," *IEEE Transactions on Signal Processing*, vol. 57, pp. 289-301, 2009.