Optics Communications 366 (2016) 22–32

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Simultaneous image compression, fusion and encryption algorithm based on compressive sensing and chaos

Xingbin Liu*, Wenbo Mei, Huiqian Du

School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China

ARTICLE INFO

Article history:
Received 9 November 2015
Received in revised form
10 December 2015
Accepted 12 December 2015
Available online 24 December 2015

Keywords:
Image fusion
Image encryption
Compressive sensing
Chaos
Fractional Fourier transform

ABSTRACT

In this paper, a novel approach based on compressive sensing and chaos is proposed for simultaneously compressing, fusing and encrypting multi-modal images. The sparsely represented source images are firstly measured with the key-controlled pseudo-random measurement matrix constructed using logistic map, which reduces the data to be processed and realizes the initial encryption. Then the obtained measurements are fused by the proposed adaptive weighted fusion rule. The fused measurement is further encrypted into the ciphertext through an iterative procedure including improved random pixel exchanging technique and fractional Fourier transform. The fused image can be reconstructed by decrypting the ciphertext and using a recovery algorithm. The proposed algorithm not only reduces data volume but also simplifies keys, which improves the efficiency of transmitting data and distributing keys. Numerical results demonstrate the feasibility and security of the proposed scheme.

© 2015 Elsevier B.V. All rights reserved.

1. Introduction

With the rapid development of communication and information processing technologies, image compression, fusion and encryption have been three hot topics in the image processing field. Image compression is used to eliminate redundancies of image data, which is essential in reducing the storage space and bandwidth requirements [1]. Image fusion can integrate multi-source images into a single visual perception enhanced image to better describe the scene [2]. Image encryption technique is used to secure the image from information leaking during the storage and transmission processes [3,4].

In general, these aforementioned image processing techniques are independently applied to accomplish a specific purpose. Recently, due to the intrinsic compression feature of compressive sensing (CS) theory [5–7], several image fusion methods [8–12] and image encryption methods [13–17] based on CS were proposed to realize compressive image fusion or compressive image encryption schemes. Wan et al. [18] presented a CS based image fusion framework and investigated the construction performance under different sampling patterns. Yang et al. [19] used adaptive local energy metrics to fuse measurements. In Liu's scheme [20], the sparse representation coefficients were firstly fused and then measured, which achieves a better fusion result. In the research of compressive image encryption, a number of CS based image encryption algorithms aiming at reducing data volume and improving security have been proposed. Zhou et al. [21] proposed an image encryption algorithm using logistic map to generate the measurement matrix, which is beneficial to keys distribution and storage. Lu et al. [22] proposed an image encryption method by CS and classical double random phase encoding algorithm, which can significantly reduce data volume. Subsequently, the Arnold transform is introduced into the proposed compressive encryption scheme to enhance the security [23]. To resist data expansion and security risks of linear transforms, an image encryption scheme by combining CS and nonlinear fractional Mellin transform [24] was proposed [25]. By utilizing CS and chaotic map, a joint image encryption and watermarking algorithm was proposed [26].

Although combining two image processing techniques at the same time has a wide application prospect, the three techniques need to be implemented in some certain circumstances. For example, in telemedicine, the multi-modal medical images not only need to be fused to integrate complementary information but also require to be encrypted to protect the privacy of patients. In military surveillance, infrared and visible images are need to be fused to enhance visual perception and then encrypted for secure transmission. In these mentioned applications, it is also necessary to reduce the amount of transferred data. Therefore, it is of great practical importance to accomplish image compression, fusion and encryption simultaneously.

In this paper, a simultaneous image compression, fusion and encryption approach based on CS and chaos is presented to ensure the efficiency and security of image transmission. Firstly, the multi-modal source images are sparsely represented with discrete

* Corresponding author.
E-mail address: xbliu6@163.com (X. Liu).

http://dx.doi.org/10.1016/j.optcom.2015.12.024
0030-4018/© 2015 Elsevier B.V. All rights reserved.

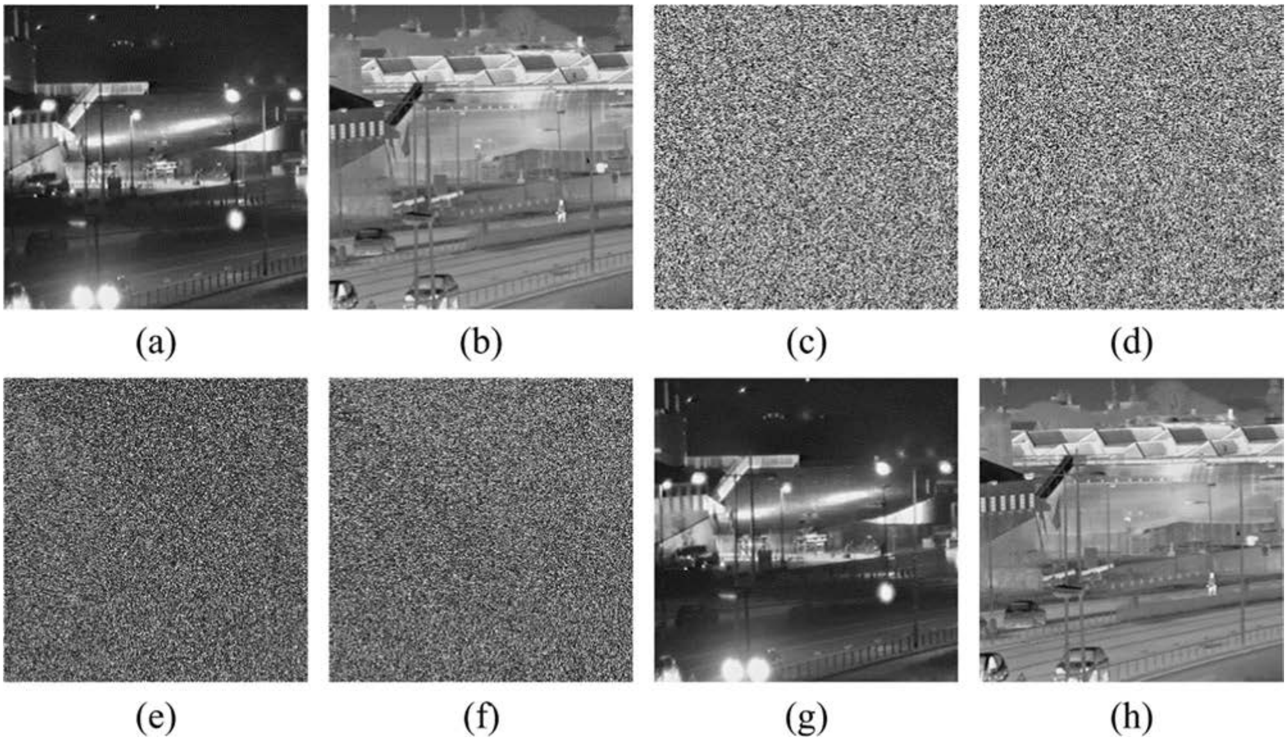


Fig. 1. The pixel scrambling results using the improved pixel exchanging technique.

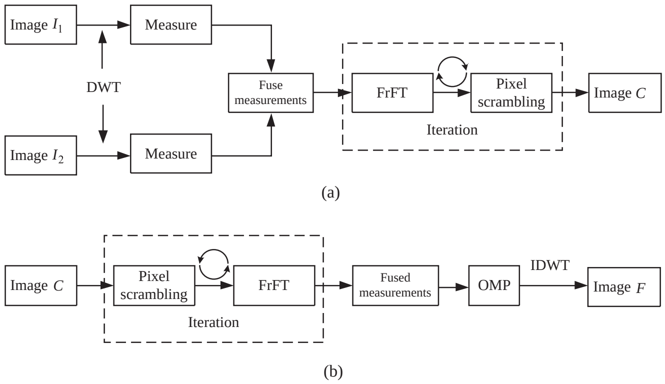


Fig. 2. The flowchart of the proposed scheme.

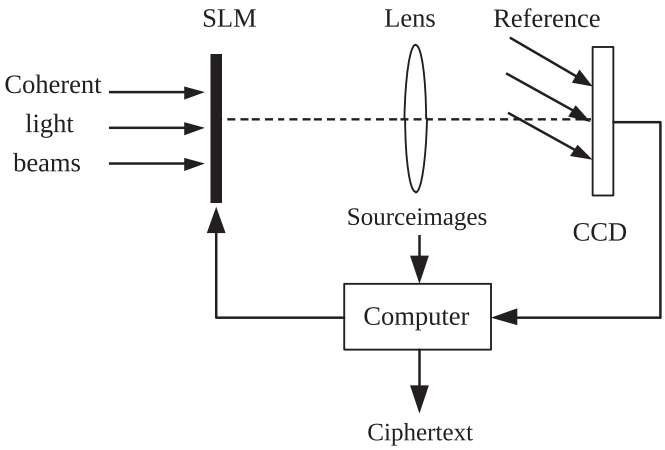


Fig. 3. The designed optoelectronic hybrid setup of the proposed scheme.

wavelet transform (DWT) and then the coefficients are measured with a key-controlled measurement matrix constructed by logistic map. The obtained measurements are fused by the proposed adaptive weighted fusion rule. The final ciphertext can be obtained by encoding the fused measurement with iterative pixel scrambling and fractional Fourier transform (FrFT) operations. At the received terminal, the fused image can be reconstructed by decrypting the ciphertext and using a recovery algorithm. The proposed algorithm has the merits of data volume reduction, keys simplification, high security and high transmission efficiency, which are verified by numerical simulation results.

2. Basic theory

In this section, some fundamental principles including CS theory, logistic map and FrFT are briefly introduced.

2.1. Compressive sensing

CS theory demonstrates that sparse signals can be perfectly reconstructed from random measurements, the samples of which are far fewer than the traditional Nyquist sampling theorem required. Therefore, the CS-based image processing techniques possess intrinsic compression feature, which is promising in significantly reducing computational costs.

For a one-dimensional compressible signal $x \in R^N$, it can be sparsely represented with an orthogonal transform matrix Ψ as

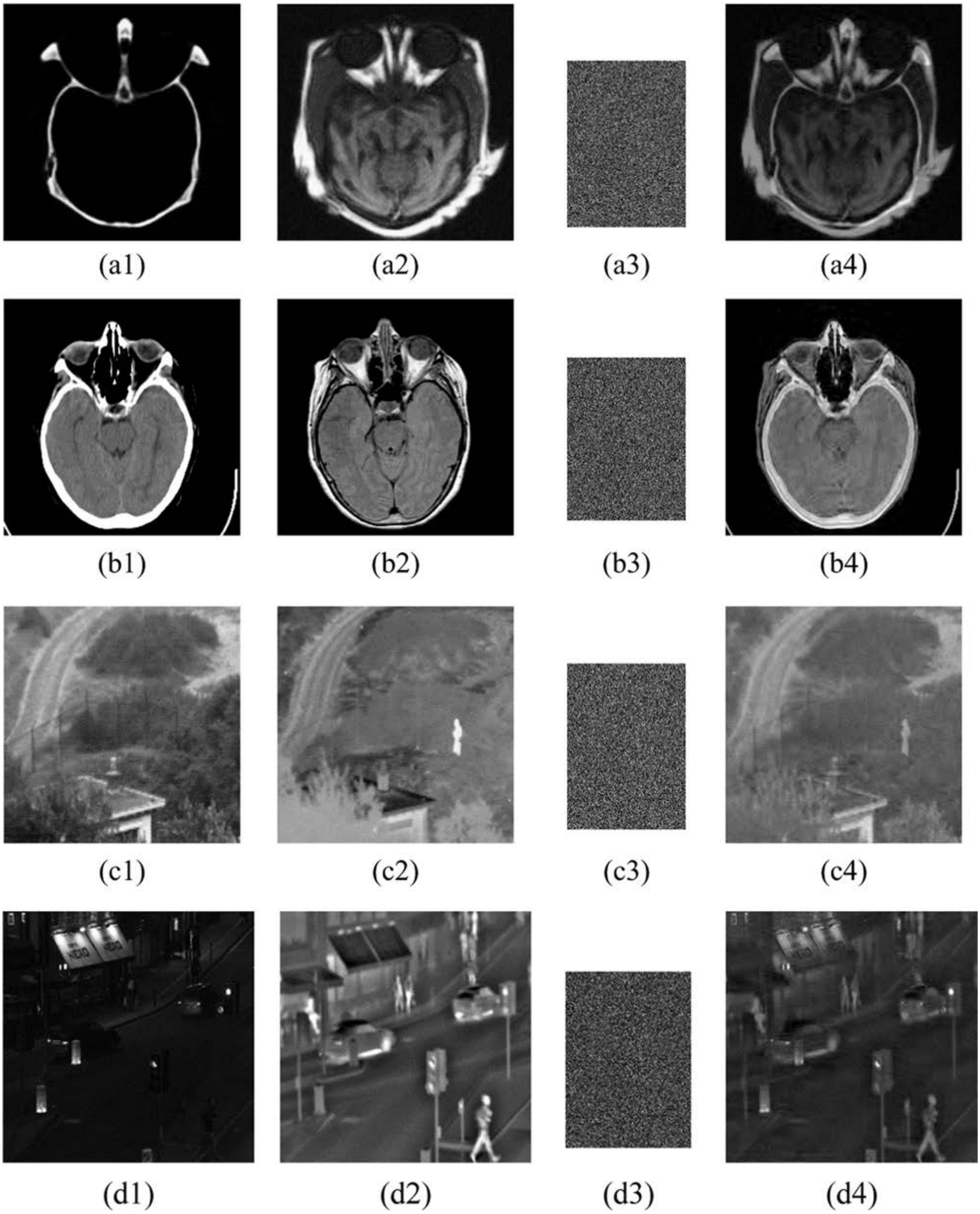
$$x = \Psi\xi, \tag{1}$$

where ξ denotes the transform coefficients. If there are only K non-zero components in ξ, then ξ is said to be $K-$sparse.

The process of sensing is to get the linear measurement y with an incoherent measurement matrix $\Phi \in R^{M\times N}(M < < N)$, i.e.

$$y = \Phi x = \Phi\Psi\xi. \tag{2}$$

Then the approximation of ξ can be retrieved by solving a non-convex optimization problem as follows:


(a1) (a2) (a3) (a4)

(b1) (b2) (b3) (b4)

(c1) (c2) (c3) (c4)

(d1) (d2) (d3) (d4)

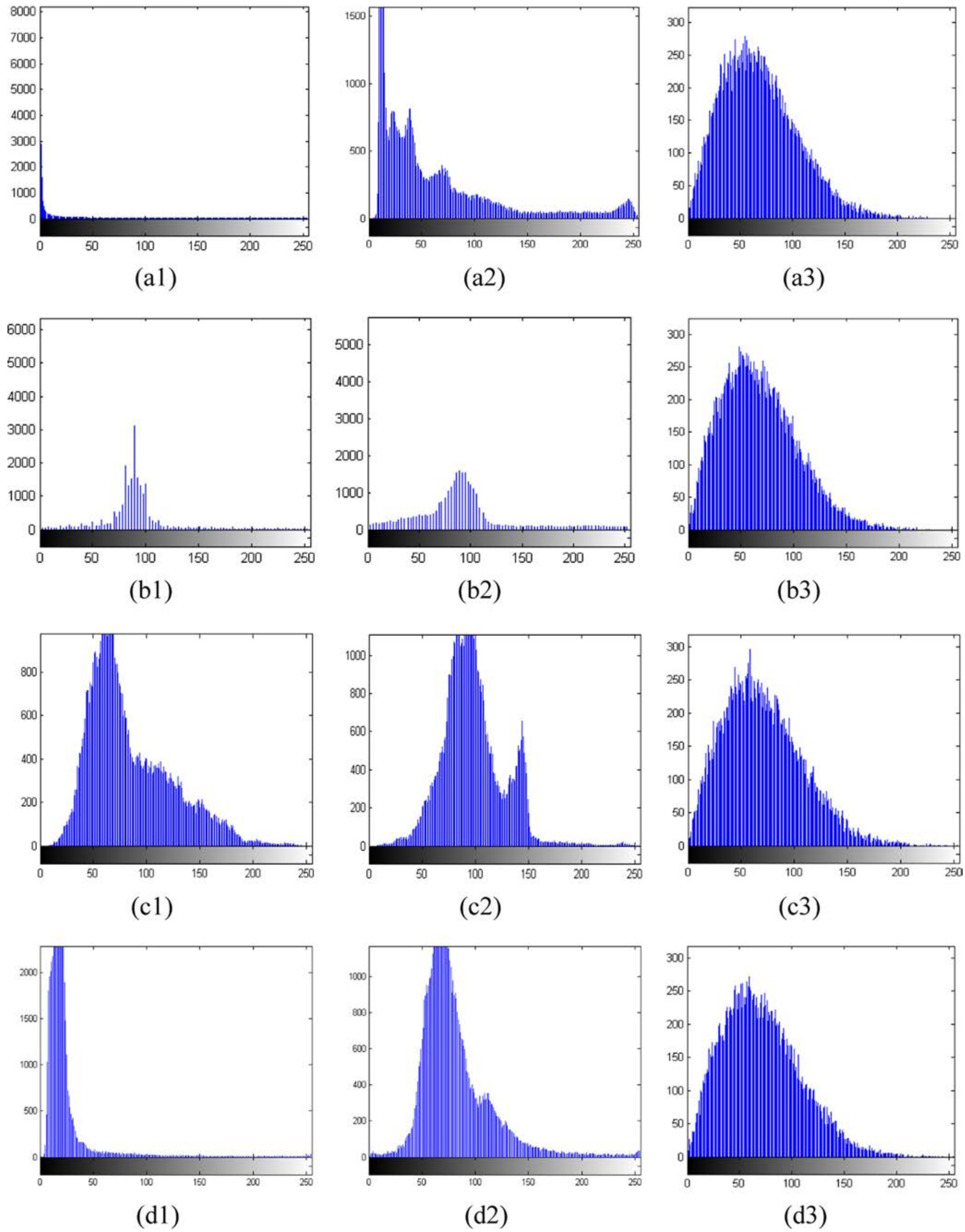
Fig. 4. The source images, encrypted images and reconstructed images with correct keys.

$$\min \|\xi\|_0,\ s.\ t.\ y = \Phi\Psi\xi. \tag{3}$$

As the above problem is NP-hard [5] when N is large, the recently developed Orthogonal Matching Pursuit (OMP) algorithm [27] is adopted in the proposed algorithm to solve this issue.

2.2. Logistic map

The logistic map is a simple nonlinear chaos system, which is usually used to generate pseudo-random sequences. The logistic map is defined in an iterative form as



(a1) (a2) (a3)

(b1) (b2) (b3)

(c1) (c2) (c3)

(d1) (d2) (d3)

Fig. 5. The histograms of source images and encrypted images.

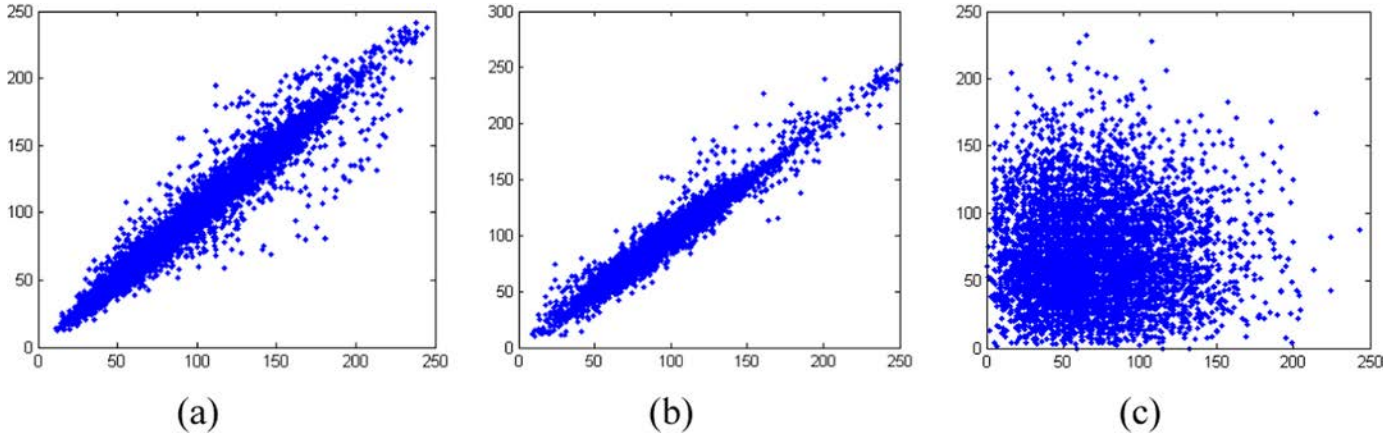


Fig. 6. Correlation distributions in vertical direction of (a) visible image, (b) infrared image, and (c) encrypted image.

Table 1
Correlation coefficients in three directions.

Correlation coefficient	Visible image	Infrared image	Ciphertext
Horizontal	0.9851	0.9819	0.0187
Vertical	0.9872	0.9809	0.0076
Diagonal	0.9672	0.9596	0.0203

$$x_{n+1} = \mu x_n (1 - x_n), \tag{4}$$

where μ is the control parameter, and the system will in chaotic state when $3.5699456 \le \mu \le 4$. This chaos system is sensitive to the seed value x_0 and the generated sequence x_n distributes in the range of $(0, 1)$.

2.3. Fractional Fourier transform

The FrFT is a powerful time–frequency analysis tool, which is the generalization of Fourier transform. The α order FrFT [28] of a one-dimensional signal $f(x)$ is defined as

$$F^{\alpha}\{f(x)\}(u) = \int_{-\infty}^{+\infty} K_{\alpha}(x, u) f(x) \mathrm{d}x. \tag{5}$$

The $K_{\alpha}(x, u)$ is the transform kernel and defined as

$$K_{\alpha}(x, u) = \begin{cases} A \exp\left[i\pi\left(\cot\varphi - 2xu\csc\varphi + u^2 \cot\varphi \right) \right] & \text{if} \quad \varphi \ne n\pi \\ \delta(x - u) & \text{if} \quad \varphi = 2n\pi \\ \delta(x + u) & \text{if} \quad \varphi = (2n + 1)\pi \end{cases} \tag{6}$$

where $A = \frac{\exp[-i(\pi\,\mathrm{sgn}(\varphi)/4 - \varphi/2)]}{\sqrt{|\sin\varphi|}}$ and $\varphi = \alpha\pi/2$. The FrFT is periodic and the period is 4.

3. Simultaneous image compression, fusion and encryption algorithm

In this section, the detailed procedures of the proposed simultaneous image compression, fusion and encryption algorithm are described. The proposed algorithm is realized by the following main steps: (1) sparse representation of the source images; (2) pseudo-random measure; (3) measurements fusion; (4) fused measurement encryption. Firstly the source images are sparsely represented in DWT domain. The wavelet coefficients of source images are measured with a measurement matrix constructed by logistic map. Then the obtained measurements are fused by the proposed adaptive weighted fusion rule. The final compression, fusion and encryption result is obtained by encrypting the measurement with an iterative procedure including pixel scrambling and FrFT operations.

3.1. Sparse representation

Suppose two registered real-valued source images with $N \times N$ pixels to be fused and encrypted are denote as I_1 and I_2, respectively. Firstly, they are transformed to the DWT domain:

$$\begin{aligned} Z_1 &= \mathrm{DWT}[I_1] \\ Z_2 &= \mathrm{DWT}[I_2]' \end{aligned} \tag{7}$$

where the coefficient matrices Z_1 and Z_2 are sparse as most entries of them are close to zero.

3.2. Pseudo-random measure

In the pseudo-random measure process, the measurement matrix $\Phi \in R^{M \times N} (M < N)$ is constructed using logistic map. A length of $M \times N + p_1$ pseudo-random sequence is generated according to Eq. (4) by giving control parameter c_1 and seed value s_1. The ahead p_1 elements are discarded and the remaining elements are used to construct a $M \times N$ measurement matrix Φ.

Each columns of coefficient matrices will be measured by the constructed measurement matrix Φ and thus two measurements B_1 and B_2 are obtained:

$$\begin{aligned} B_1 &= \Phi Z_1 \\ B_2 &= \Phi Z_2^{\cdot} \end{aligned} \tag{8}$$

The pseudo-random measure process accomplishes the measure operation. Meanwhile, it can be viewed as the first level encryption and the parameters of logistic map (c_1, s_1, p_1) are severed as keys.

3.3. Measurements fusion

After obtaining the measurements of the source images, the next step is to fuse the measurements reasonably. Here, an adaptive weighted fusion rule is proposed to fuse the measurements. As most detail information exists in the high-frequency components, in order to transfer more detail information to the fused image, the weights are computed using latter three quarters of the measurements. The weights ω_1 and ω_2 assigned to B_1 and B_2 respectively are computed as

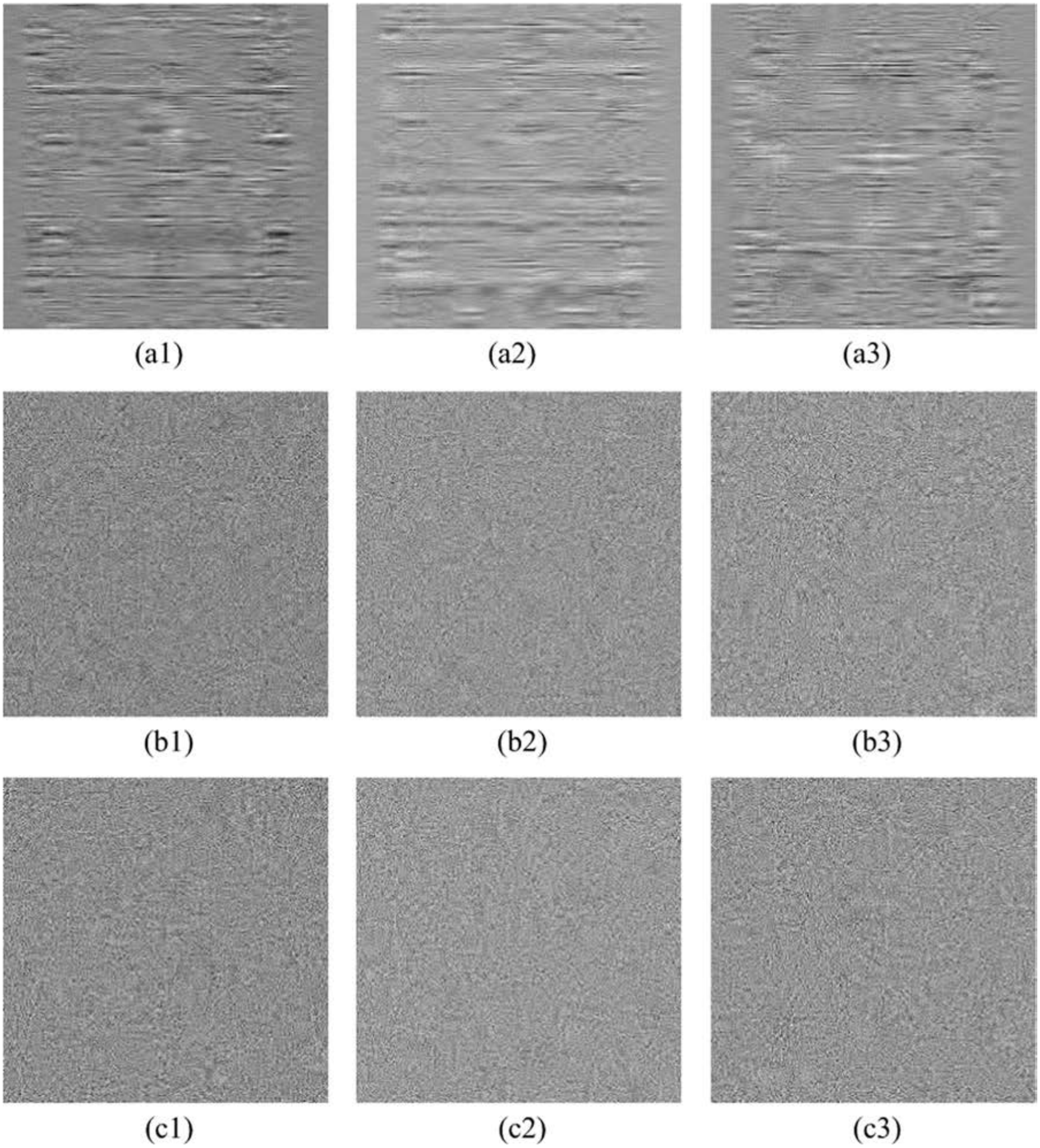


Fig. 7. Reconstructed images using incorrect logistic map parameters.

Table 2
Incorrect logistic map parameters for decryption and the PSNR of the decrypted image.

Incorrect parameter	PSNR
$c_1 = 3.997352 + 1.0 \times 10^{-15}$	10.4986
$s_1 = 0.6 + 1.0 \times 10^{-16}$	10.0927
$p_1 = 12000 + 1$	10.5742
$c_2 = 3.873536 + 1.0 \times 10^{-15}$	0.0476
$s_2 = 0.55 + 1.0 \times 10^{-14}$	0.0706
$p_2 = 16000 + 1$	0.0578
$c_3 = 3.973891 + 1.0 \times 10^{-15}$	0.0990
$s_3 = 0.72 + 1.0 \times 10^{-15}$	0.0568
$p_3 = 13800 + 1$	0.0115

$$\omega_1 = \frac{\sum_{i=\frac{N}{4}+1}^{N} \|B_1^i\|_1}{\sum_{i=\frac{N}{4}+1}^{N} \|B_1^i\|_1 + \sum_{i=\frac{N}{4}+1}^{N} \|B_2^i\|_1},$$
$$\omega_2 = \frac{\sum_{i=\frac{N}{4}+1}^{N} \|B_2^i\|_1}{\sum_{i=\frac{N}{4}+1}^{N} \|B_1^i\|_1 + \sum_{i=\frac{N}{4}+1}^{N} \|B_2^i\|_1}, \tag{9}$$

where B_1^i and B_2^i denote the i-th column of the B_1 and B_2, respectively. The operator $\|\cdot\|_1$ denotes L1-norm, which is used to compute the sum of absolute values from given variables.

The final fused measurement B_F can be obtained by computing the weighted sum of the measurements:

$$B_F = \omega_1 B_1 + \omega_2 B_2. \tag{10}$$

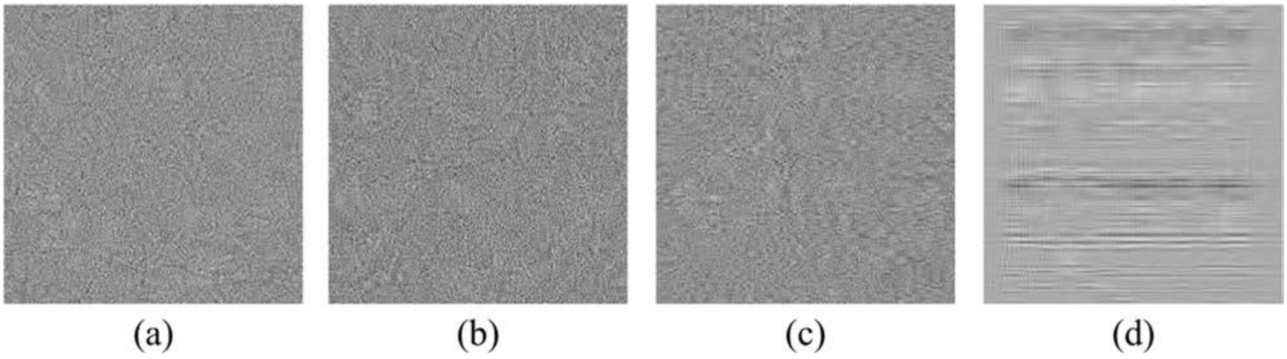


Fig. 8. The reconstructed images with incorrect fractional orders.

3.4. Fused measurement encryption

To further encrypt the fused measurement B_F, an iterative procedure including pixel scrambling and FrFT is applied to complete confusion and diffusion operations. The pixel scrambling is realized by improving the random pixel exchanging technique proposed in the literature [29]. In our proposed improved version of random pixel exchanging technique, two group of logistic parameters are used to generate random matrices, which enlarges key space and simplifies the keys distribution.

In order to efficiently compress and encrypt the measurement B_F, it is evenly divided into two parts in the center and the size of each part is $M \times N/2$. The left part and right part of the measurement B_F are denoted as B_F^{l} and B_F^{r}, respectively. The divided two parts are composed into a complex-valued measurement

$$B_F^{\mathrm{c}} = B_F^{\mathrm{l}} + iB_F^{\mathrm{r}}. \tag{11}$$

In the following iterative procedure, the complex-valued measurement B_F^{c} is transformed to FrFT domain

$$B_F^{\mathrm{c}'} = \mathrm{FrFT}\left[B_F^{\mathrm{c}}\right] \tag{12}$$

and the real part and imaginary part are extracted from $B_F^{\mathrm{c}'}$ as

$$\begin{cases} B_F^{\mathrm{l}'} = \mathrm{real}\left(B_F^{\mathrm{c}'}\right) \\ B_F^{\mathrm{r}'} = \mathrm{imag}\left(B_F^{\mathrm{c}'}\right) \end{cases}. \tag{13}$$

The random pixel exchanging technique aims at scrambling pixels between $B_F^{\mathrm{l}'}$ and $B_F^{\mathrm{r}'}$. Suppose the initial position of a pixel denote as (m, n), the new position (m', n') is computed through the following function

$$\begin{cases} m' = 1 + \mathrm{round}\left(R_1(m, n) \times (M - 1)\right) \\ n' = 1 + \mathrm{round}\left(R_2(m, n) \times (N/2 - 1)\right) \end{cases}, \tag{14}$$

where R_1 and R_2 are two random matrices generated using logistic map with parameters (c_2, s_2, p_2) and (c_3, s_3, p_3), respectively. The function 'round' is used to compute the nearest integer.

The pixel exchanging rules include inter-exchange and intra-exchange. The pixels are changed between the two images when $R_1(m, n) > R_2(m, n)$, otherwise the pixels are changed within the image. Assume that the pixel exchanging operation is denoted with the symbol '↔', then the improved random pixel exchanging technique can be expressed as follows

$$\begin{cases} \begin{cases} B_F^{\mathrm{l}'}(m, n) \leftrightarrow B_F^{\mathrm{r}'}(m', n') \\ B_F^{\mathrm{r}'}(m, n) \leftrightarrow B_F^{\mathrm{l}'}(m', n') \end{cases} & \text{if } R_1(m, n) > R_2(m, n) \\ \begin{cases} B_F^{\mathrm{l}'}(m, n) \leftrightarrow B_F^{\mathrm{l}'}(m', n') \\ B_F^{\mathrm{r}'}(m, n) \leftrightarrow B_F^{\mathrm{r}'}(m', n') \end{cases} & \text{otherwise} \end{cases}. \tag{15}$$

To verify the validity of the improved version of random pixel exchanging technique, two original images shown in Fig. 1(a) and (b) are tested. The pseudo-random matrices generated by logistic map are shown in Fig. 1(c) and (d) and the pixel scrambling results are shown in Fig. 1(e) and (f). Fig. 1(g) and (h) shows the retrieved images with correct parameters of logistic map. As can be seen from the results, the improved pixel exchanging technique can effectively scramble pixels.

After t iterations of FrFT and pixel scrambling, the ciphertext C is obtained. The flowchart of the proposed scheme is illustrated in Fig. 2(a). The decrypted and fused image F can be reconstructed through the inverse process and OMP algorithm as shown in Fig. 2(b).

As the proposed simultaneous image compression, fusion and encryption scheme uses the FrFT, an optoelectronic hybrid setup designed in Fig. 3 can be applied to accelerate processing speed. The source images are fed into the computer to accomplish the pre-processing operations include sparse representation, pseudo-random measure, measurements fusion. The spatial light modulator (SLM) is used for modulating the fused measurement. Then the fused measurement is transformed with FrFT using Lohmann's type I single-lens optical setup [30]. The charge-coupled device (CCD) captures the transformed measurement and fed into the compute to accomplish the pixel scrambling operation. After several iterations, the final ciphertext can be directly obtained from CCD.

4. Experimental results and analysis

In this section, numerical simulation experiments are carried out to verify the validity and security of the proposed scheme. In general, the multi-modal images contain complementary content and information. For example, the Computed Tomography (CT) image is sensitive to bones and implants structure, while the Magnetic Resonance Imaging (MRI) image can distinctly reveal soft tissues. Therefore, the fused medical image can provide more comprehensive information of human body, which is extremely useful in clinical diagnosis. In addition, the infrared (IR) image records the target objects with different temperatures, while the visible (VIS) image shows much detail information of the background. As a consequence, the visual perception capability of the scene is enhanced by fusing IR and VIS images. In the following

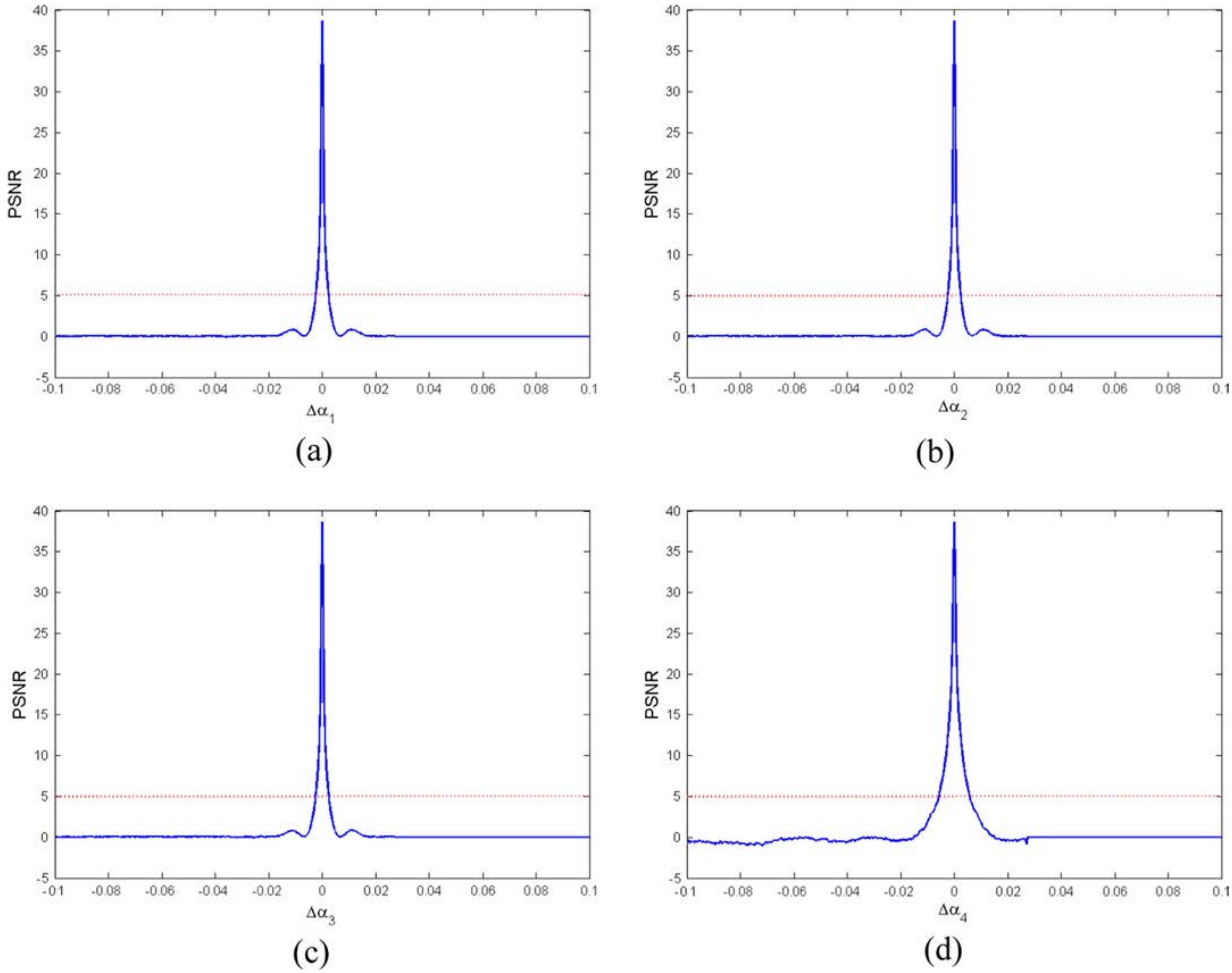


Fig. 9. The PSNR curves versus the deviations of the fractional orders.

experiments, the compressed, fused and encrypted medical images and IR&VIS images are presented and analyzed.

For each kind of image, two pairs of source image are tested. The source images, named as “Med1”, “Med2”, “VIS&IR1” and “VIS&IR2”, are downloaded from imagefusion.org website [31] and the Whole Brain Atlas website [32]. The source images are all with 256 × 256 pixels as shown in the first two columns of Fig. 4. The Symlet basis is used in DWT to sparsely represent source images and the source images are decomposed into eight levels. The sampling ratio adopted in the measure process is 70%. The size of the measurement matrix is 179 × 256, which is generated by the logistic map with parameters $(c_1 = 3.997352, s_1 = 0.6, p_1 = 12,000)$. The two random matrices used to scramble pixels are respectively generated with the parameters $(c_2 = 3.873536, s_2 = 0.55, p_2 = 16,000)$ and $(c_3 = 3.973891, s_3 = 0.72, p_3 = 13,800)$. The iteration number t equals 4 and the four fractional orders of FrFT used in the iterative process are $(\alpha_1 = 0.2, = 0.5, \alpha_3 = 0.3, \alpha_4 = , 0.6)$. The obtained ciphertext are shown in the third column, the size of which is 179 × 128. The decrypted and fused images with correct keys are shown in the fourth column of Fig. 4. It can be seen from the decrypted and fused results that the salient features of source images are preserved and transferred into the reconstructed image, which is more informative than anyone of the corresponding source images.

4.1. Statistical analysis

To verify the ability of resist statistical attacks, image histogram and correlation are analyzed. Fig. 5 shows the histograms corresponding to the images shown in the first three columns of Fig. 4. Although the histograms of the source images are quite different, the histograms of the ciphertext are similar to each other in distribution. By conducting numerous parallel experiments, the ciphertexts all have similar distribution as Fig. 5(a3), which indicates that the attacker cannot acquire useful information from the histogram analysis.

In a meaningful image, the adjacent pixels usually have strong correlation. To test the correlation of the source images and ciphertext, the distribution of 16,002 adjacent pixel pairs in the vertical direction of “VIS&IR1” image set are given in Fig. 6(a) and (b). Fig. 6(c) shows the distribution of the selected 5544 adjacent pixel pairs in the ciphertext. It can be seen from the correlation distributions that the correlations in source images are strong while in the ciphertext are weak. Moreover, the correlation coefficient (CC) is used to compute the correlation of the source images and ciphertext in horizontal, vertical and diagonal directions. The CC is defined as

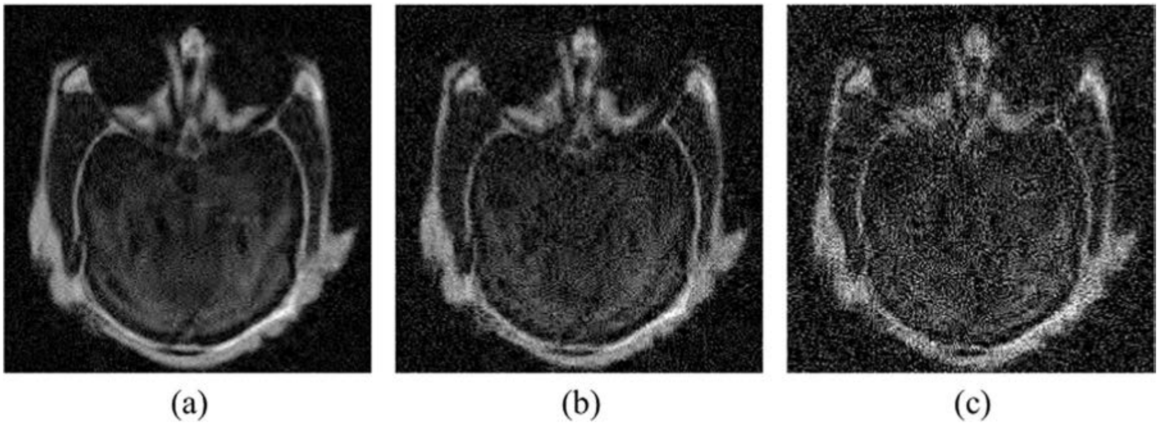


Fig. 10. The reconstructed images with k equals to (a) 0.05, (b) 0.1 and (c) 0.2.

$$\mathrm{CC} = \frac{\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{(\sum_{i=1}^{N}(x_i - \bar{x})^2)(\sum_{i=1}^{N}(y_i - \bar{y})^2)}}, \tag{16}$$

where $\bar{x}$ and $\bar{y}$ denote the mean value of $\{x_i\}$ and $\{y_i\}$, respectively. The CC values are listed in Table 1, from which can be seen that the adjacent pixels in three directions of ciphertext are almost uncorrelated. Based on the above analysis, we can conclude that the proposed scheme can resist statistical analysis attack as the encryption process effectively confuses and diffuses the image pixels.

4.2. Key sensitivity analysis

To evaluate the quality of the reconstructed image, the peak signal to noise ratio (PSNR) is introduced. The PSNR between the reconstructed image and original fused image is defined as

$$\mathrm{PSNR}{=}10\times\ \log\frac{255^2\times M\times N}{\sum_{i=1}^{N}\sum_{j=1}^{M}[F(i,j)-O(i,j)]^2}, \tag{17}$$

where $M\times N$ denotes the size of the image to be evaluated. The $F(i,j)$ and $O(i,j)$ denote the pixel value in the location (i,j) of reconstructed image F and original fused image O, respectively.

In the proposed simultaneous image compression, fusion and encryption scheme, the parameters of logistic map and the fractional orders of FrFT are main keys. Fig. 7 shows the reconstructed images with incorrect parameters, which only have a small deviation of the correct keys. The three columns of the images in Fig. 7 are reconstructed with incorrect parameters c, s and p, respectively. The incorrect parameters used to reconstruct images and the corresponding values of PSNR are listed in Table 2. As illustrated in experimental results, the decrypted image cannot display any useful information of source images when the deviation of parameters up to 10^{-15} magnitude. Consequently, the keys are fairly sensitive to the decryption.

The fractional orders of FrFT are also primary keys in the proposed scheme. The reconstructed images with incorrect fractional orders, the deviation of which are 0.005, are shown in Fig. 8(a)–(d). It can be seen from the reconstructed images that a tiny deviation of the fractional orders will lead to the completely meaningless image. Fig. 9(a)–(d) displays the PSNR curves versus the deviation of the fractional orders. As the reconstructed image will too blurry to recognize the original meaning when the PSNR values below 5 dB, therefore a dashed line at the 5 dB position is marked in the curves. The curves decrease sharply when the fractional orders deviate tiny values from the correct keys, which imply that the fractional orders are sensitive to the decryption. Thus, the orders of FrFT are valid and reliable keys with high sensitivity to ensure the security of the proposed scheme.

4.3. Key space analysis

According to the key sensitive analysis, the parameters of the logistic map and the orders of FrFT are served as keys. The experimental results in Section 4.2 show that the key space

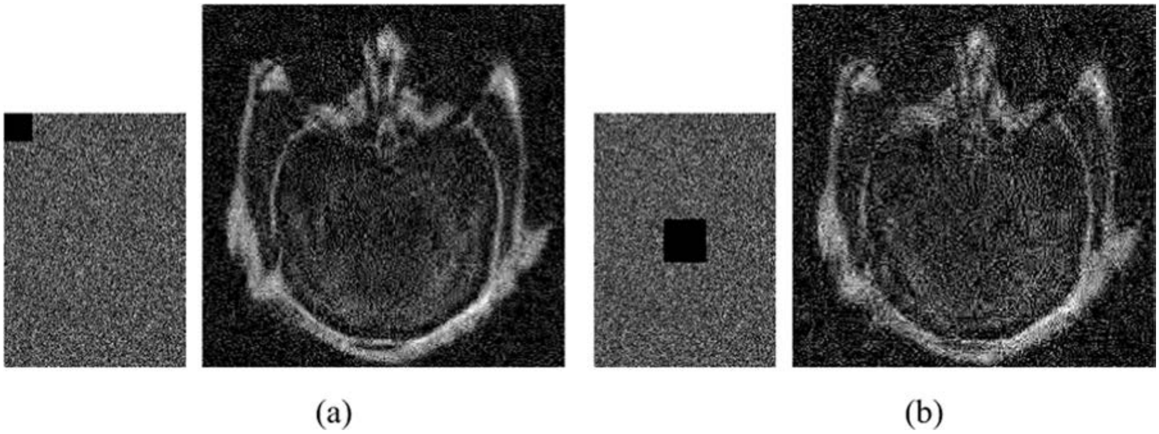


Fig. 11. The reconstructed images with occlusion of the encrypted image, (a) 20 × 20 pixels occlusion, (b) 30 × 30 occlusion.

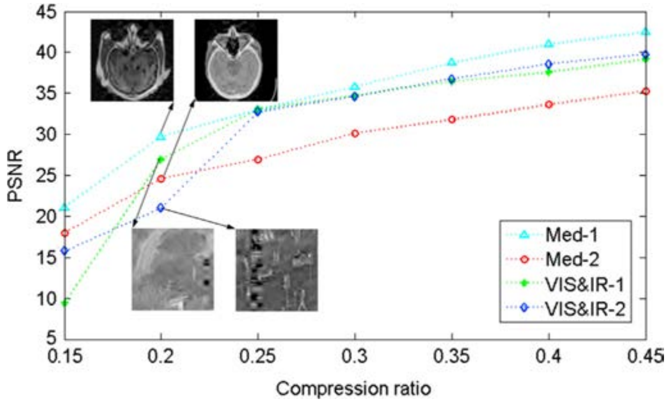


Fig. 12. The PSNR curves under different compression ratios.

constituted with the parameters of logistic map is $S_1 \geq 10^{15+16+15+14+15+15} = 10^{90}$ and the key space constituted with the fractional orders is $S_2 \cong 10^{12}$. Since the keys are independent from each other, the entire key space S is the product of single key space, i.e.

$$S = \prod_{i=1}^{2} S_i \geq 10^{90} \times 10^{12} = 10^{102}, \tag{18}$$

which is huge enough to resist against brute-force attack.

Moreover, the security of the proposed scheme can be further enhanced by increasing the number of iterations. Besides the increase of fractional orders, the random matrices can be changed in each iteration to further enlarge the key space.

4.4. Robustness analysis

In the image transmission and storage processes, it is inevitable that the ciphertext will be affected by noise and even loses partial information. Therefore, the robustness of the proposed scheme is considered. To test the ability of resisting noise attack, different intensity Gaussian noises adjusted by parameter k are added into the ciphertext C as follows,

$$C' = C(1 + kG), \tag{19}$$

where G denote the zero-mean Gaussian noise with standard deviation of 1. Fig. 10(a)–(c) shows the reconstructed images with k equals to 0.05, 0.1 and 0.2, respectively. Although the reconstructed images become fuzzier with the increase of noise strength, the main information can still be recognized.

The performance of the reconstruction from incomplete ciphertext is also examined. The reconstructed images from ciphertext with 20×20 pixels loss and 30×30 pixels loss are shown in Fig. 11(a) and (b), respectively. It can be seen that the recovered images reveal major information of source images, which implies that the proposed scheme can resist occlusion attack to some extent.

4.5. Compression performance analysis

The proposed scheme not only achieves image fusion and encryption but also compressed the image to be transmitted. The compression performance of the scheme is analyzed by changing compression ratios. The PSNR curves with different compression ratios for 4 image sets are shown in Fig. 12. It can be seen from the simulation results that the quality of the reconstructed images are become better with the increase of compression ratio. When the compression ratio equals to 0.2, the main information can still be recognized from the reconstructed images. Therefore, the proposed scheme significantly reduced the data volume to be transmitted and storage.

5. Conclusion

In this paper, a simultaneous image compression, fusion and encryption algorithm has been proposed by incorporating CS with chaotic theory. A fused image with perfect visual effect can be reconstructed from less data through the proposed scheme, which is also secure against various attacks. The introduction of CS achieves efficient and flexible compression to reduce the data volume to be processed and transmitted. The chaotic theory is used to ensure the security of the proposed scheme and simplify the keys to be distributed at the same time. In addition, an optoelectronic setup is realized to speed up the proposed scheme. Experimental results of image fusion and encryption show the validity and reliability of the proposed scheme.

References

[1] S. Juliet, E.B. Rajsingh, K. Ezra, A novel image compression method for medical images using geometrical regularity of image structure, Signal Image Video Process. 9 (7) (2015) 1691–1703.
[2] Y. Jiang, M. Wang, Image fusion with morphological component analysis, Inf. Fusion 18 (2014) 107–118.
[3] N. Zhou, Y. Wang, L. Gong, H. He, J. Wu, Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform, Opt. Commun. 284 (12) (2011) 2789–2796.
[4] N. Zhou, J. Yang, C. Tan, S. Pan, Z. Zhou, Double-image encryption scheme combining DWT-based compressive sensing with discrete fractional random transform, Opt. Commun. 354 (2015) 112–121.
[5] B.K. Natarajan, Sparse approximate solutions to linear systems, SIAM J. Comput. 24 (2) (1995) 227–234.
[6] E.J. Candès, T. Tao, Decoding by linear programming, IEEE Trans. Inf. Theory 51 (12) (2004) 4203–4215.
[7] D.L. Donoho, Compressed sensing, IEEE Trans. Inf. Theory 52 (4) (2006) 1289–1306.
[8] C. Jiang, H. Zhang, H. Shen, L. Zhang, A practical compressed sensing-based pan-sharpening method, IEEE Geosci. Remote Sens. Lett. 9 (4) (2012) 629–633.
[9] G. Liu, Y. Shen, Ultrasonic image fusion using compressed sensing, Electron. Lett. 48 (19) (2012) 1182–1184.
[10] K. Ren, F. Xu, G. Gu, Compressed sensing and low-rank matrix decomposition in multisource images fusion, Math. Probl. Eng. 2014 (2014) 1–7, Article ID 278945.
[11] M. Ghahremani, H. Ghassemian, Remote sensing image fusion using ripplet transform and compressed sensing, IEEE Geosci. Remote Sens. Lett. 12 (3) (2015) 502–506.
[12] Y. Chen, Z. Qin, PCNN-based image fusion in compressed domain, Math. Probl. Eng. 2015 (2015) 1–9 536215.
[13] N. Rawat, B. Kim, I. Muniraj, G. Situ, B.G. Lee, Compressive sensing based robust multispectral double-image encryption, Appl. Opt. 54 (7) (2015) 1782–1793.
[14] X. Huang, G. Ye, H. Chai, Q. Xie, Compression and encryption for remote sensing image using chaotic system, Secur. Commun. Netw. 8 (2015) 3659–3666.
[15] X. Liu, W. Mei, H. Du, Optical image encryption based on compressive sensing and chaos in the fractional Fourier domain, J. Mod. Opt. 61 (19) (2014) 1570–1577.
[16] D. Xiao, S. Chen, Separable data hiding in encrypted image based on compressive sensing, Electron. Lett. 50 (8) (2014) 598–600.
[17] H. Liu, D. Xiao, Y. Liu, Y. Zhang, Securely compressive sensing using double random phase encoding, Optik 126 (20) (2015) 2663–2670.
[18] T. Wan, Z. Qin, An application of compressive sensing for image fusion, Int. J. Comput. Math. 88 (18) (2011) 3915–3930.
[19] Z. Yang, Z. Yang, Novel multifocus image fusion and reconstruction framework based on compressed sensing, IET Image Process. 7 (9) (2013) 837–847.
[20] Z. Liu, H. Yin, B. Fang, Y. Chai, A novel fusion scheme for visible and infrared images based on compressive sensing, Opt. Commun. 335 (2015) 168–177.
[21] N. Zhou, A. Zhang, F. Zheng, L. Gong, Image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing, Opt. Laser Technol. 62 (2014) 152–160.
[22] P. Lu, Z. Xu, X. Lu, X. Liu, Digital image information encryption based on compressive sensing and double random-phase encoding technique, Optik 124 (16) (2013) 2514–2518.
[23] X. Liu, Y. Cao, P. Lu, X. Lu, Y. Li, Optical image encryption technique based on compressed sensing and Arnold transformation, Optik 124 (24) (2013) 6590–6593.
[24] N. Zhou, Y. Wang, L. Gong, Novel optical image encryption scheme based on fractional Mellin transform, Opt. Commun. 284 (13) (2011) 3234–3242.

[25] N. Zhou, H. Li, D. Wang, S. Pan, Z. Zhou, Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform, Opt. Commun. 343 (2015) 10–21.

[26] D. Xiao, H.K. Cai, H.Y. Zheng, A joint image encryption and watermarking algorithm based on compressive sensing and chaotic map, Chin. Phys. B 24 (6) (2015) 060505.

[27] J.A. Tropp, A.C. Gilbert, Signal recovery from random measurements via orthogonal matching pursuit, IEEE Trans. Inf. Theory 53 (12) (2007) 4655–4666.

[28] H.M. Ozaktas, Z. Zalevsky, M.A. Kutay, The Fractional Fourier Transform with Applications in Optics and Signal Processing, Wiley, UK, 2001.

[29] Z. Liu, Y. Zhang, S. Li, W. Liu, W. Liu, Y. Wang, S. Liu, Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains, Opt. Laser Technol. 47 (2013) 152–158.

[30] A.W. Lohmann, Image rotation, Wigner rotation, and the fractional Fourier transform, J. Opt. Soc. Am. A: Opt. Image Sci. 10 (10) (1993) 2181–2186.

[31] Imagefusion.org. ⟨http://www.imagefusion.org⟩ (accessed 14.07.13).

[32] Whole Brain Atlas. ⟨http://www.med.harvard.edu/AANLIB/⟩ (accessed 15.05.16).