Wang et al. BioMed Eng OnLine (2016) 15:118
DOI 10.1186/s12938-016-0239-1

BioMedical Engineering OnLine

RESEARCH Open Access

Simultaneous encryption and compression of medical images based on optimized tensor compressed sensing with 3D Lorenz

Qingzhu Wang[1*], Xiaoming Chen[1], Mengying Wei[1] and Zhuang Miao[2]

*Correspondence: 150681573@qq.com; wangqingzhu@mail.nedu.edu.cn
[1] School of Information Engineering, Northeast Dianli University, Jilin 132012, China
Full list of author information is available at the end of the article

Abstract

Background: The existing techniques for simultaneous encryption and compression of images refer lossy compression. Their reconstruction performances did not meet the accuracy of medical images because most of them have not been applicable to three-dimensional (3D) medical image volumes intrinsically represented by tensors.

Methods: We propose a tensor-based algorithm using tensor compressive sensing (TCS) to address these issues. Alternating least squares is further used to optimize the TCS with measurement matrices encrypted by discrete 3D Lorenz.

Results: The proposed method preserves the intrinsic structure of tensor-based 3D images and achieves a better balance of compression ratio, decryption accuracy, and security. Furthermore, the characteristic of the tensor product can be used as additional keys to make unauthorized decryption harder.

Conclusions: Numerical simulation results verify the validity and the reliability of this scheme.

Keywords: Encryption and compression, Hither order singular value decomposition, 3D Lorenz, Medical images

Background

In recent years, numerous studies on encryption of medical images, such as computed tomography (CT) and magnetic resonance imaging (MRI), have been reported [1–6], although most of them did not consider compression during encryption. The storage, transmission, and retrieval of massive bio-information should meet several compulsory requirements [7]: (1) high efficiency for rapid transmission and prompt retrieval; (2) strict information security to guarantee users' privacy; and (3) high data fidelity to preserve the pathological information. It requires decreasing the quantity of data to be transmitted (compression) and protecting such data against unauthorized access (encryption). Therefore, simultaneous compression and encryption technology of medical images that are represented as three-dimensional (3D) volumes has additional meanings.

BioMed Central

© The Author(s) 2016. This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The Creative Commons Public Domain Dedication waiver (http://creativecommons.org/publicdomain/zero/1.0/) applies to the data made available in this article, unless otherwise stated.

Existing simultaneous compression and encryption algorithms are typically applied to ordinal images rather than medical images, because they refer to lossy compression. Alfalou et al. proposed a series of representative algorithms for the simultaneous compression and encryption of 3D images. The latest and most effective algorithm is based on spectral fusion and discrete cosine transform (DCT) [8]. However, the decryption error increases rapidly along with the increase of the number of images, indicating that it cannot handle large amounts of images simultaneously. Emerging algorithms for simultaneous encryption and compression are based mainly on compressed sensing (CS), which can activate compression during the sampling process [9]. An example being Valerio et al., who proposed a multiclass encryption by CS to withstand the common attack [10, 11]. To further enhance security, CS-based encryption algorithms were constructed by combining the chaos map and some optical encryption techniques, such as double random phase encryption (DRPE), fractional Fourier transform (FrFT), and fractional Mellin transform (FrMT) [12–19].

The medical images are different from other images because of their particular properties. There are legal and strict regulations applied to medical multimedia information due to the health of a patient depending on the correctness and accuracy of this information [20]. The quality of the decrypted and compressed data must be adequate to allow for a correct diagnosis when it is reconstructed. However, the existing algorithms did not meet this requirement because most of them have not been applicable to 3D images intrinsically represented by tensors. Conventional CS theory relies on data representation in the form of one-dimensional vectors. Application of CS to higher dimensional data representation is typically performed by conversion of the data to very long vectors that must be measured using very large sampling matrices, thus destroying the intrinsic structure and imposing a huge memory burden.

Recently, Cesar et al. propose a tensor CS (TCS) based on higher order singular value decomposition (HOSVD) that introduces a direct reconstruction formula to recover a tensor from a set of multi-linear projections, which are obtained by multiplying the data tensor by a different sensing matrix in each mode [21]. This HOSVD-based TCS achieved more accurate and efficient reconstruction results when compared to other existing sparsity-based TCS methods [22–24]. Indeed, we believe that, if it was used to design TCS-based encryption of 3D images better performance would occur.

We further introduce alternating least squares (ALS) into HOSVD-based TCS [21], and control the measurement matrices by 3D Lorenz [25–27]. Such a simultaneous compression and encryption algorithm for 3D medical images has two main advantages: (1) the preservation of intrinsic structures of the tensor data for the purpose of reducing the decryption error and increasing the compression ratio; (2) the keys consist of those generated by tensor decomposition, and 3D Lorenz. Particularly, the order of the tensor product used in the TCS can be used as additional keys to make unauthorized decryption harder.

This paper is organized as follows: in "Theory" section, the related notation, definition and basic results used throughout the paper, are introduced; in "Proposed encryption" section, the encryption and decryption algorithms are proposed; in "Numerical simulation results" section, several numerical results based on 3D lung CT images are provided, to corroborate our theoretical results and evaluate the stability and robustness

of our proposed scheme, in "Conclusion" section, the main conclusions drawn from the present work are outlined.

Theory

HOSVD

The higher-order singular value decomposition (HOSVD) provides a generalization of the low-rank approximation of matrices to the case of tensors [28–30]. To facilitate the distinction between scalars, vectors, matrices and higher dimensional tensors, the type of a given quantity will be reduced by its representation: scalars are denoted by lower-case letters (a), vectors are written as capitals ($\mathbf{a}$), matrices corresponding to bold-face capitals ($\mathbf{A}$) and tensors are written as calligraphic letters ($\mathcal{A}$).

A tensor is a multidimensional array with the number of modes represented by the tensor order. For instance, tensor $\mathcal{A} \in R^{M_1 \times \cdots \times M_d}$ has order d and the dimension of its i-th mode is M_i.

1. Mode-i product: A mode-i product of a tensor $\mathcal{A}$ and a matrix $\Phi \in R^{M_i \times m}$ is denoted by $\mathcal{A} \times_i \Phi$ and is of size $m \times (M_1 \cdots M_{i-1} \cdot M_{i+1} \cdots M_d)$ matrix.
2. Mode-i unfolding: The mode-i unfolding $\mathbf{A}_{(i)}$ of $\mathcal{A}$ arranges the mode-i fibers to be the columns of the resulting matrix.
3. HOSVD: The decomposition and reconstruction of $\mathcal{A}$ can be written as the product:

$$\begin{cases} \mathcal{W} = \mathcal{A} \times_1 \Phi_1^T \cdots \times_{M_d} \Phi_{M_d}^T \\ \widehat{\mathcal{A}} = \widehat{\mathcal{W}} \times_1 \Phi_1 \cdots \times_{M_d} \Phi_{M_d} \end{cases} \tag{1}$$

   where $\Phi_i \in R^{M_i \times m_i}$, and $\mathcal{W}$ is a complex $(m_1 \times m_2 \times \cdots \times m_d)$-tensor of which the subtensors obtained by corresponding singular values.
4. Tucker-TCS: in [21], a more stable, robust and accuracy tensor reconstruction of CS is proposed:

$$\widehat{\mathcal{A}} = \widehat{\mathcal{W}} \times_1 \mathbf{Z}_1 \mathbf{W}_{(1)}^{\dagger} \cdots \times_{M_d} \mathbf{Z}_{M_d} \mathbf{W}_{(M_d)}^{\dagger} \tag{2}$$

   where "†" stands for the MP pseudo-inverse of a matrix. We assume that the following sets of compressive multi-way measurements $\mathbf{Z}^{(n)}$ are available:

$$\mathbf{Z}^{(n)} = \mathcal{A} \times_1 \Phi_1^T \times_2 \cdots \times_{n-1} \Phi_{n-1}^T \times_{n+1} \Phi_{n+1}^T \times_{n+2} \cdots \times_{M_d} \Phi_{M_d}^T \tag{3}$$

$$\mathbf{Z}_n = \left(\mathbf{Z}^{(n)}\right)_{(n)} \tag{4}$$

3D Lorenz

Mohmad et al. [25, 26] propose a 3D discrete Lorenz system, which has a high order and also low complexity when implemented in digital hardware. The discrete Lorenz attractor employed here is given by the following difference equations

$$\begin{cases} U_{k+1} = g1(A(V_k - U_k)) + U_k \\ V_{k+1} = g2(BU_k - V_k - 20U_k W_k) + V_k \\ W_{k+1} = g3(5U_k V_k - CW_k) + W_k \end{cases} \tag{5}$$

where U, V, W are three state variables, A, B, C are parameters, and $g1,\ g2,\ g3$ are gains (step size). The calculating method of (5) is finite difference.

Proposed encryption

The proposed system can be split into encryption and decryption algorithms as illustrated in Fig. 1. The compression and decompression procedures are embedded in the encryption and decryption, respectively.

Encryption

For the initial 3D image $\mathcal{A} \in R^{M_1 \times M_2 \times M_3}$, the encryption process consists of the following steps:

1. Initialize randomly the three Gaussian sensing matrices $\Phi_i^{(0)} \in R^{M_i \times m_i}$ $(m_i < M_i,\ i = 1, 2, 3)$. To accurately decrypt $\mathcal{A}$, the optimal Φ_i should satisfy:

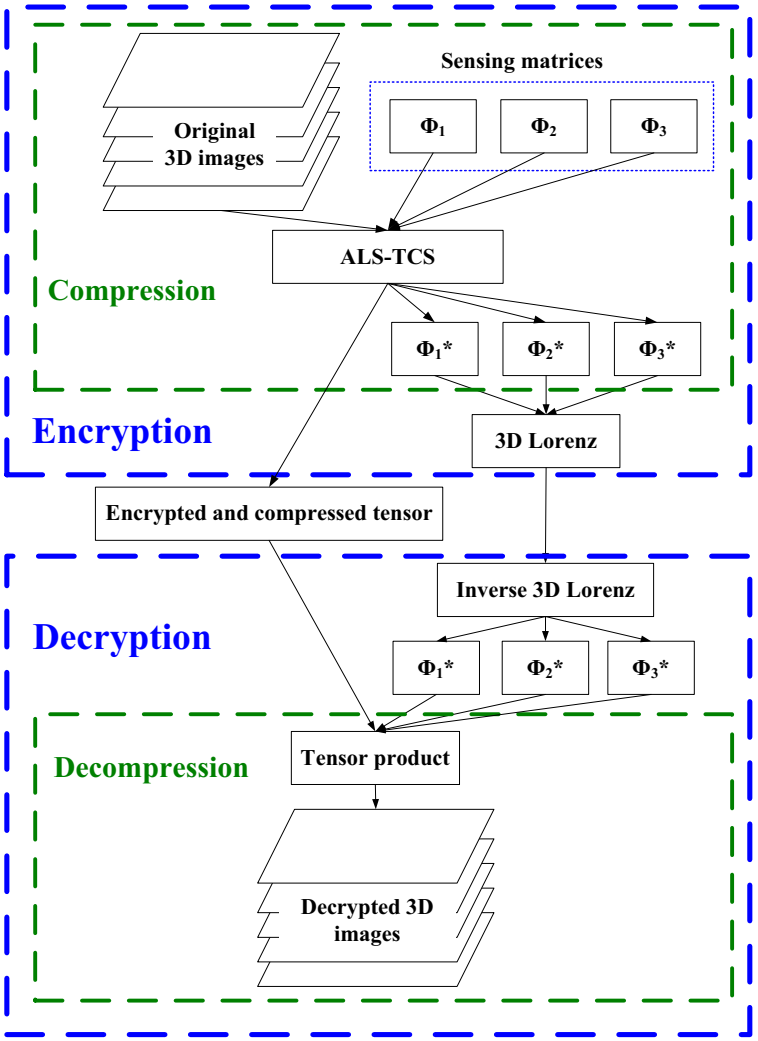

Fig. 1 Illustration of the proposed simultaneous compression and encryption system of 3D images

$$\{\Phi_1^*,\ \Phi_2^*,\ \Phi_3^*\} = \arg\min \|\mathcal{A} - \mathcal{W} \times_1 \Phi_1 \times_2 \Phi_2 \times_3 \Phi_3\|_F^2 \tag{6}$$

As in [28], this problem can be converted to

$$\{\Phi_1^*,\ \Phi_2^*,\ \Phi_3^*\} = \arg\max \left\|\mathcal{A} \times_1 \Phi_1^T \times_2 \Phi_2^T \times_3 \Phi_3^T\right\|_F^2 \tag{7}$$

To solve this problem, it is sufficient to find Φ_i's satisfying $\Phi_i^T \Phi_i = I$. The reconstruction algorithm as Eq. (2) of HOSVD-based TCS achieved a more accurate solution than that as Eq. (1) of HOSVD. To further improve the reconstruction accuracy, we use an alternating least squares (ALS) approach to solve Eq. (7).

2. For $k = 0$, iterate Eqs. (8)–(11) until Φ_i converges or the maximum iteration is achieved:

$$\begin{cases} \mathbf{Z}^{(1)} = \mathcal{A} \times_2 \Phi_2^{(k)T} \times_3 \Phi_3^{(k)T} \\ \mathbf{Z}^{(2)} = \mathcal{A} \times_1 \Phi_1^{(k)T} \times_3 \Phi_3^{(k)T} \\ \mathbf{Z}^{(3)} = \mathcal{A} \times_1 \Phi_1^{(k)T} \times_2 \Phi_2^{(k)T} \end{cases} \tag{8}$$

$$\mathbf{Z}_i = \left(\mathbf{Z}^{(i)}\right)_{(i)} \tag{9}$$

$$\mathbf{Z}_i \approx \mathbf{U}_{i,m_i} \mathbf{\Sigma}_{i,m_i} \mathbf{V}_{i,m_i}^T \tag{10}$$

where $\mathbf{\Sigma}_{m_i} = diag\{\sigma_1, \ldots, \sigma_{m_i}\}$ is the diagonal matrix containing the m_i largest singular value $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_{m_i}$ of $\mathbf{Z}_i$, and $\mathbf{U}_{m_i}$ and $\mathbf{V}_{m_i}$ are matrices whose columns are the leading m_i left and right singular vectors of $\mathbf{Z}_i$, respectively. Let

$$\Phi_i^{(k+1)} = \mathbf{U}_{i,m_i} \tag{11}$$

Then the optimal Φ_1^*, Φ_2^* and Φ_3^* are obtained.

3. Compute the compressed core tensor

$$\mathcal{W} = \mathcal{A} \times_1 \Phi_1^T \times_2 \Phi_2^T \times_3 \Phi_3^T \tag{12}$$

4. Unfold $\mathcal{W}$ into its n-mode $\mathbf{W}_{(n)}$. The mode n is a private key which has three possible values: 1, 2 and 3.
5. Φ_1, Φ_2 and Φ_3 are synchronously constructed by 3D Lorenz as Eq. (5).

$$E_{\Phi_i} = L(\Phi_i) \tag{13}$$

where $E_{\Phi_i} \in R^{M_i \times m_i}$. Hence the compression ratio is given by:

$$\gamma = \frac{m_1 m_2 m_3 + m_1 M_1 + m_2 M_2 + m_3 M_3}{M_1 M_2 M_3} \approx \frac{m_1 m_2 m_3}{M_1 M_2 M_3} \tag{14}$$

The details of how to synchronize the image by 3D Lorenz system are introduced below. One data sample $\varphi_{i,k}$ is inserted into U, which gives

$$\begin{cases} U_{k+1} = g1\big(A(V_k - U_k) + \varphi_{i,k}\big) + U_k \\ V_{k+1} = g2(BU_k - V_k - 20U_k W_k) + V_k \\ W_{k+1} = g3(5U_k V_k - CW_k) + W_k \end{cases} \tag{15}$$

where $\varphi_{i,k}$ is the k-th element of ϕ_i(ϕ_i is the vectorization of Φ_i, i.e. $\phi_i = vec(\Phi_i)$). The initial conditions U_0, V_0, W_0, parameters A, B, C, and $g1$, $g2$, $g3$ are known by both transmitter and receiver. The transmitted signal is the U state variable, and the objective is to retrieve $\varphi_{i,k}$ from this signal at the receiver. Feedback is used to update the state variables at the receiver to synchronize the system and allow decryption of subsequent data values.

$$\tilde{\varphi}_{i,k} = \frac{U_{k+1} - U_k}{g1} - A(V_k - U_k) \tag{16}$$

After $\tilde{\varphi}_{i,k}$ is obtained, the receiver state equations can be updated, thus achieving synchronization with the transmitter.

$$\begin{cases} U_{k+1} = g1\left(A(V_k - U_k) + \tilde{\varphi}_{i,k}\right) + U_k \\ \tilde{V}_{k+1} = g2(BU_k - V_k - 20U_k W_k) + V_k \\ \tilde{W}_{k+1} = g3(5U_k V_k - CW_k) + W_k \end{cases} \tag{17}$$

Decryption

The decryption process consists of the following steps:

1. E_{Φ_i} are inverse transformed by 3D Lorenz:

   $$D_{\Phi_i} = L^{-1}\left(E_{\Phi_i}\right) \tag{18}$$

   $L^{-1}(\cdot)$ is computed during Eq. (16).
2. $\mathbf{W}_{(n)}$ and the obtained D_{Φ_i} are multiplied in the correct order to recover $\mathcal{A}'$. There are three feasible ways to achieve this:

   $$\mathbf{A}'_{(n)} = \begin{cases} D_{\Phi_1} \cdot \mathbf{W}_{(1)} \cdot \left(D_{\Phi_2} \otimes D_{\Phi_3}\right)^T \\ D_{\Phi_2} \cdot \mathbf{W}_{(2)} \cdot \left(D_{\Phi_3} \otimes D_{\Phi_1}\right)^T \\ D_{\Phi_3} \cdot \mathbf{W}_{(3)} \cdot \left(D_{\Phi_1} \otimes D_{\Phi_2}\right)^T \end{cases} \tag{19}$$

   where '$\otimes$' represents the Kronecker product.
3. Then, fold $\mathbf{A}'_{(n)}$ into $\mathcal{A}'$ according to the private key n.

It is obvious that besides the secret keys of measurement matrices, the unfolding model n (order of tensor product) can be used as an additional key.

Numerical simulation results

Numerical simulations were conducted with Matlab2011 on a work station with an Intel Core i7 CPU and 64 GB RAM. The decryption error and compression ratio of the proposed system are introduced in "Decryption accuracy and compression ratio" section, the histograms are analyzed in "Histograms and statistical analysis" section, the secret keys are illustrated in "Rate-distortion" section, and the robustness is stated in "Secret keys" section.

Decryption accuracy and compression ratio

Our experiments are conducted on lung CT sequences in lung image database consortium (LIDC) [31]. Each frame of one CT sequence is preprocessed to have 512×512, where 512 frames were chosen. The CT sequence together is represented by a $512 \times 512 \times 512$ tensor and has 134,217,728 voxels in total. The randomly constructed Gaussian measurement matrix for each mode is now of size $512 \times m_i$ $(i = 1, 2, 3)$. Thus, the compression ratio is given by:

$$\gamma = \frac{m_1 m_2 m_3}{512 \times 512 \times 512}$$

The quantitative measure of the decryption error is the peak signal noise ratio (PSNR), which is based on the root mean square error (RMSE) between the decrypted data and ground truth and can be represented as:

$$PSNR = 20 \log_{10} \frac{255}{RMSE} \tag{20}$$

To further evaluate the performance of decryption, the structural similarity index (SSIM) is used as another indicator.

In this section, we compare the proposed algorithm with state of the art algorithms to show its superiority. These algorithms are presented briefly as follows:

1. As demonstrated previously [13], an encryption based on 2D_CS in the FrMT domain (algorithm 1) stands out for its efficient, robust, and secure encryption performance. In this algorithm, the 2D CS is based on a 2D wavelet, measuring matrices with Logistic map and a 2D NSL_0 reconstruction algorithm. Notably, although the security of FrMT is better than that of FrFT, its decryption accuracy is less than the later. In order to verity the decryption accuracy and compression ratio of our tensor-based algorithm, we replaced FrMT with FrFT in algorithm 1.
2. Additionally, we chose an encryption algorithm based on HOSVD-TCS [21] with FrFT (algorithm 2).
3. Also, as previously shown [8], an encryption algorithm based on spectral fusion and DCT obtained a better PSNR when compared with previous compression-encryption implementations. Accordingly, this became algorithm 3.

A visual evaluation of the decryption results under frames 117, 138 and 159 of one CT sequence at the compression $\gamma = 0.125$ is shown in Figs. 2, 3, 4, 5, 6. As shown in Fig. 3, all the tissues within the lung volume are clear. Our clinical experts did not find distinct differences between the decrypted and the original CT images. The quantitative summaries of the above algorithms are shown in Tables 1, 2 and Fig. 7, where the advantages of the proposed algorithm are highlighted. It is evident that the advantages of the proposed algorithm over the other methods increase with the compression ratio. Case in point is in algorithm 3, where improving the compression ratio requires a large number of frames. However, the PNSR rapidly decreases with the increase of the number of frames. Thus, the algorithm cannot handle large number of frames.

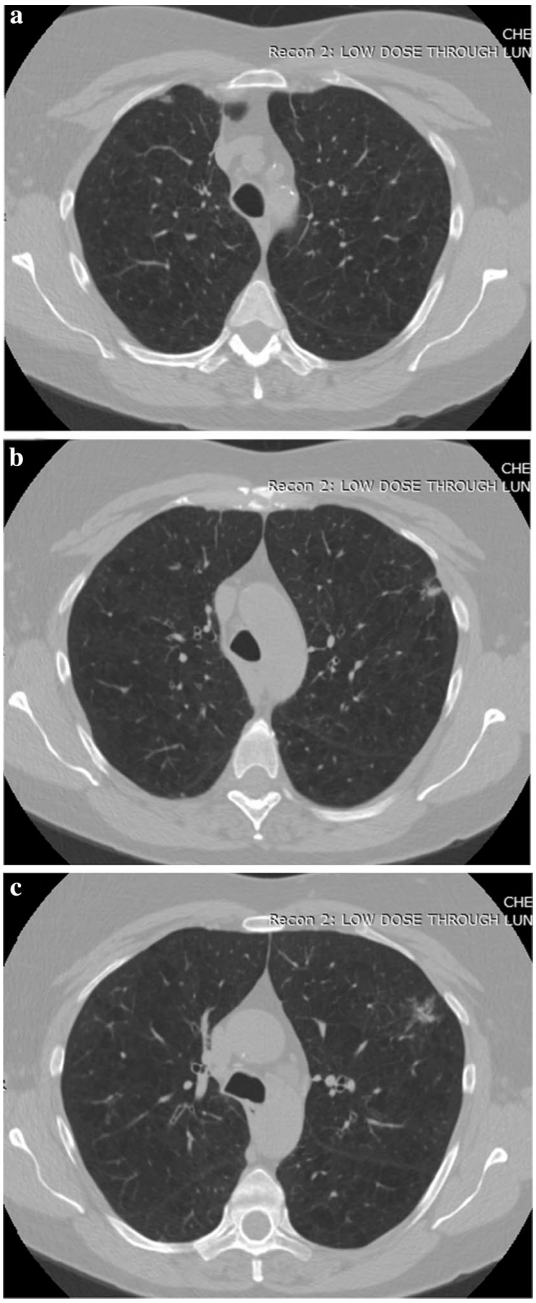

Fig. 2 Original CT frames. **a** Frame 117, **b** Frame 138, **c** Frame 159

We also compared the computation times (the average computation time of the experiments with all compression ratio and noise level) required in each case. The comparison shows that algorithm 3 provides a much faster computation (Table 3), while the proposed algorithm requires slightly longer computation time because it contains a procedure of iteration. Fortunately, this iteration is much simpler than those of algorithms 1 and 2.

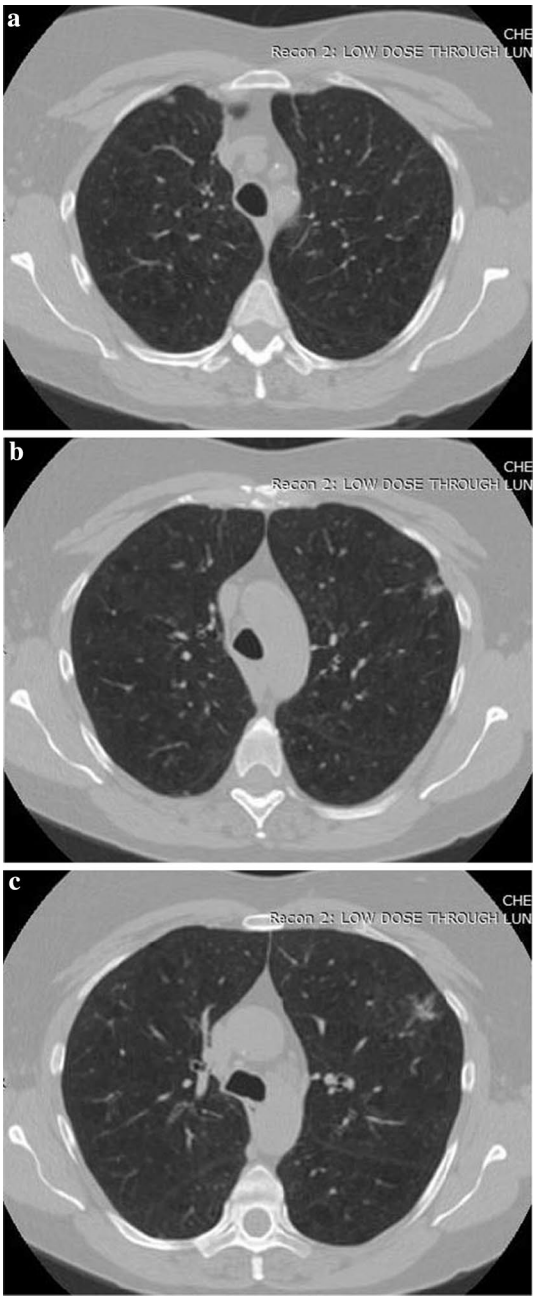

Fig. 3 Decrypted frames by the proposed algorithm. **a** Frame 117, **b** Frame 138, **c** Frame 159

Histograms and statistical analysis

Histograms

The histograms of two CT sequences and the encrypted images of their composed parts are shown in Figs. 8 and 9, respectively. The intensity distribution of the histograms of the encrypted images is completely dissimilar from that of the histogram of the original CT, which indicates that an intruder cannot perceive any useful information based on statistical properties. The histograms of the two original CT sequences are evidently

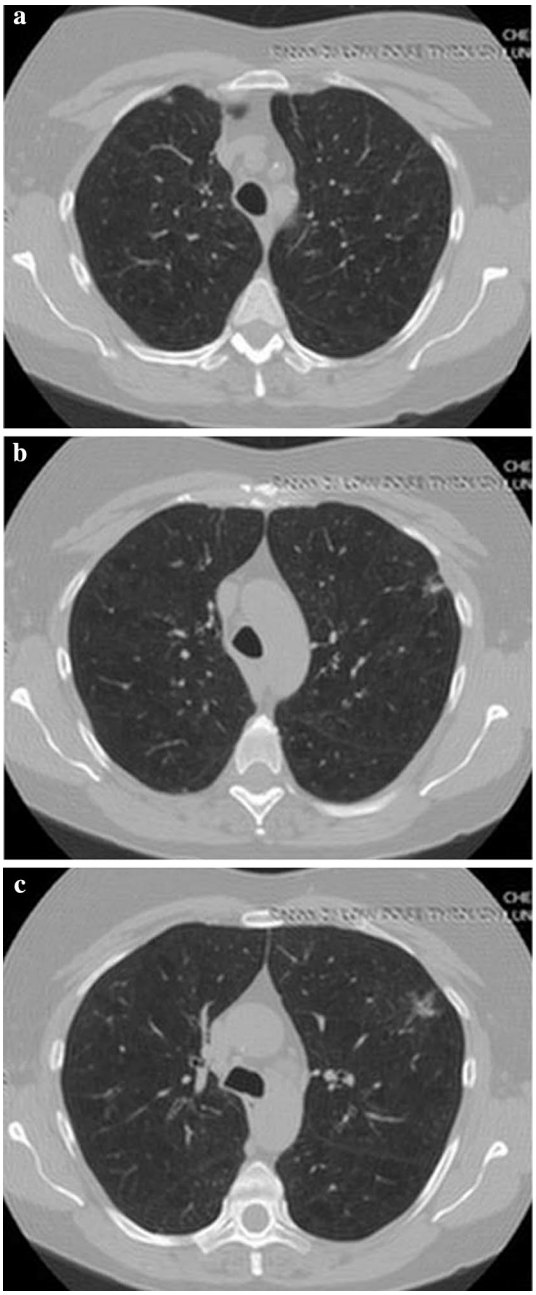

Fig. 4 Decrypted frames by algorithm 3. **a** Frame 117, **b** Frame 138, **c** Frame 159

different from each other, whereas the histograms of their corresponding encrypted images are similar. The security analysis effectively illustrates the robustness of the proposed method.

Statistical analysis

Statistical properties of the images can also be evaluated by the computation of the correlation between two adjacent pixels. By selecting randomly P pixels of the image, the correlation coefficient is computed as:

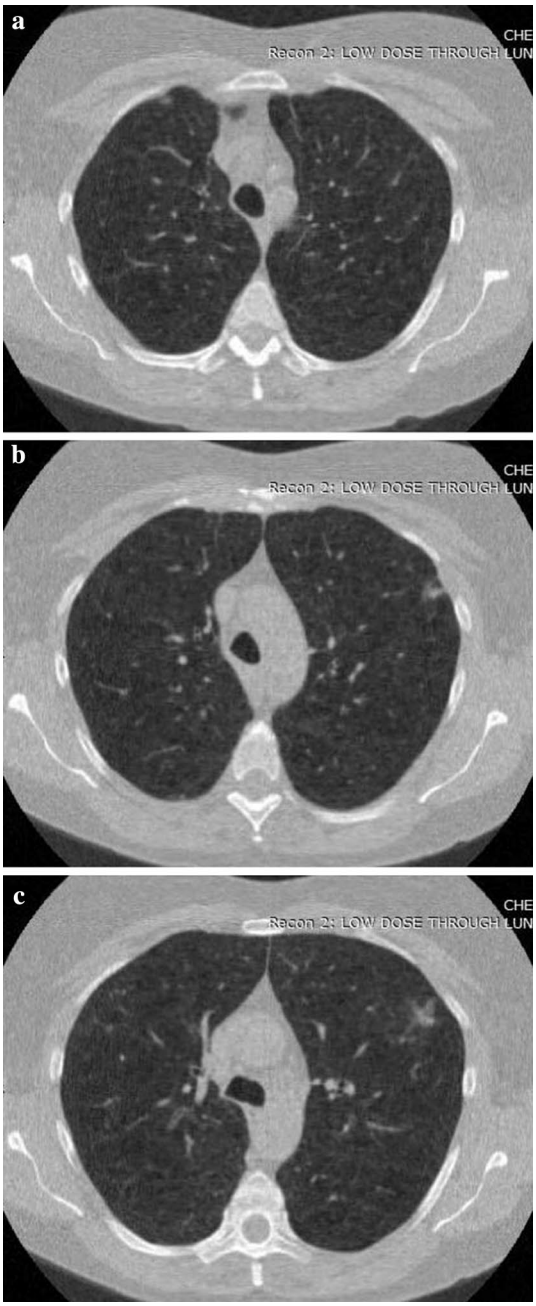

Fig. 5 Decrypted frames by algorithm 2. **a** Frame 117, **b** Frame 138, **c** Frame 159

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)D(y)}} \tag{21}$$

where x is the value of a selected pixel and y is the value of the correspondent adjacent pixel, $D(x)$ is the mean square error.

It is expected that an image will have a correlation coefficient close to 1 before being submitted to the encryption; it is desirable that the correlation coefficient of a ciphered image be as close to 0 as possible. In Table 4, where the simulation results for

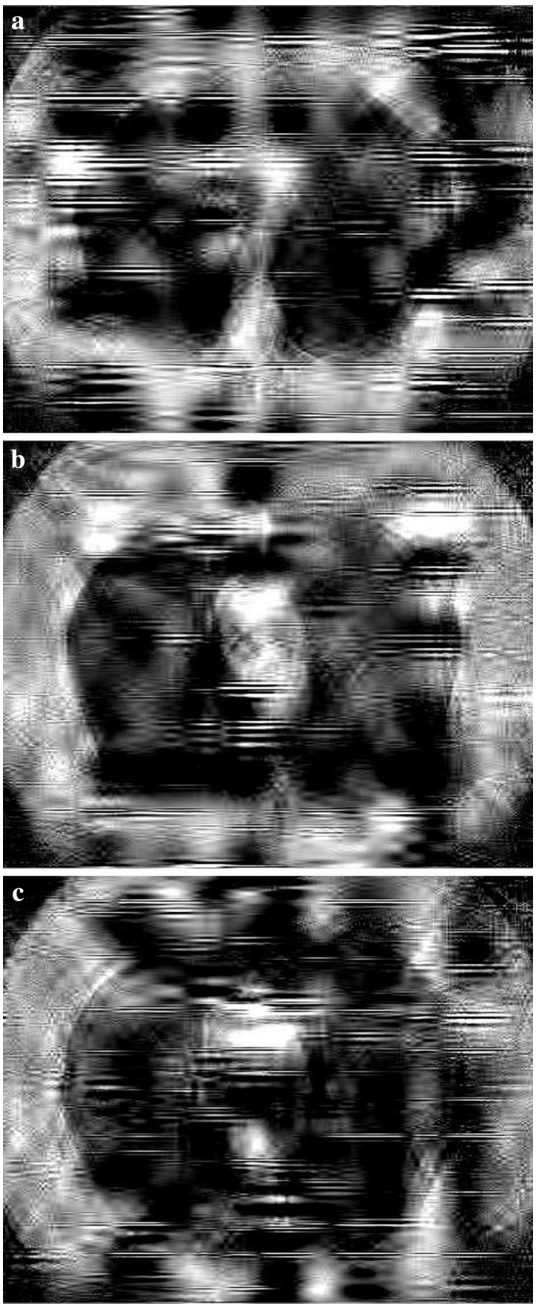

Fig. 6 Decrypted frames by algorithm 1. **a** Frame 117, **b** Frame 138, **c** Frame 159

$P = 125{,}000$ are shown, we verify that the above described premise is satisfied. This indicates that the proposed encryption scheme is secure against statistical attacks.

Normalized entropy

The normalized entropy [6] of the ciphered image is defined as

$$\bar{H} = \frac{\sum_{i=0}^{P-1} \frac{N_i}{N} \log \frac{N}{N_i}}{\log_2 P} \tag{22}$$

Table 1 PSNR at different compression ratio of the CT sequence

Methods	Compression ratio					
	$\frac{(256)^3}{(512)^3} = 0.125$	$\frac{(352)^3}{(512)^3} = 0.33$	$\frac{(384)^3}{(128)^3} = 0.42$	$\frac{(416)^3}{(512)^3} = 0.54$	$\frac{(448)^3}{(512)^3} = 0.67$	$\frac{(480)^3}{(512)^3} = 0.82$
Algorithm 1	6.72	11.26	12.22	19.29	24.00	30.49
Algorithm 2	31.12	36.12	38.00	40.34	43.01	47.28
Algorithm 3	24.55	27.78	28.74	30.03	32.30	34.67
Proposed algorithm	37.76	43.17	45.56	48.43	51.95	57.26

Table 2 Comparison of SSIM between the proposed algorithm and state to the art methods

Methods	Compression ratio					
	$\frac{(256)^3}{(512)^3} = 0.125$	$\frac{(352)^3}{(512)^3} = 0.33$	$\frac{(384)^3}{(128)^3} = 0.42$	$\frac{(416)^3}{(512)^3} = 0.54$	$\frac{(448)^3}{(512)^3} = 0.67$	$\frac{(480)^3}{(512)^3} = 0.82$
Algorithm 1	0.1406	0.2198	0.3060	0.4378	0.6090	0.8000
Algorithm 2	0.8293	0.9004	0.9195	0.9157	0.9259	0.9312
Algorithm 3	0.7474	0.8664	0.8945	0.9165	0.9314	0.9474
Proposed algorithm	0.9122	0.9468	0.9508	0.9533	0.9544	0.9549

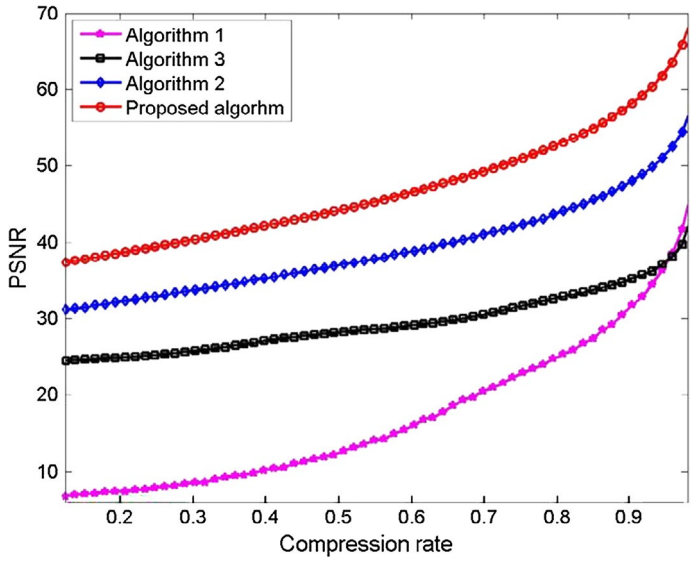

Fig. 7 PSNR (dB) comparison of the four algorithms at compression ratio values ranging from 0.125 to 0.98

Table 3 Comparison of computation time (s) between the proposed algorithm and state to the art methods

Methods	Computation time (s)
Algorithm 1	896
Algorithm 2	188
Algorithm 3	164
Proposed algorithm	220

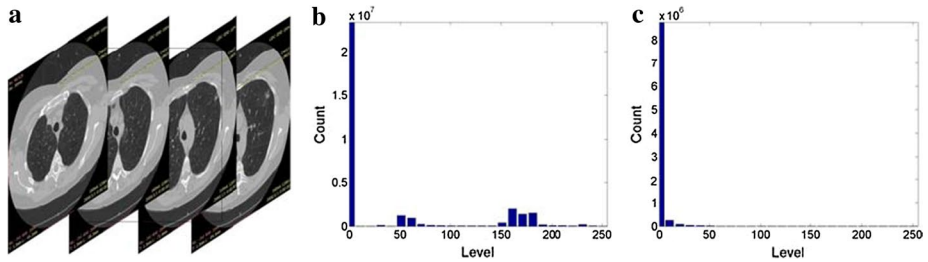

Fig. 8 Histograms of 3D images and encrypted parts of CT No. 1. **a** Original CT sequence No.1. **b** Histogram of original CT. **c** Histogram of ciphertext

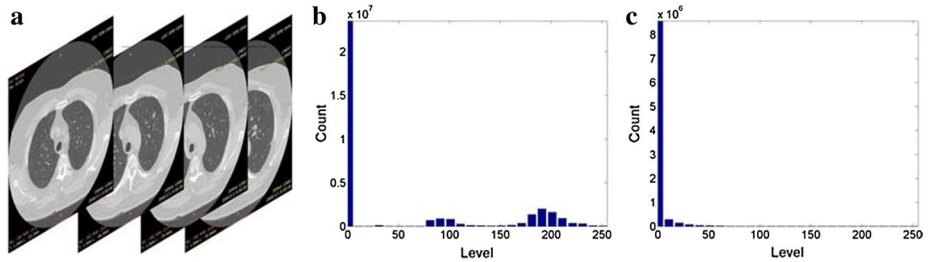

Fig. 9 Histograms of 3D images and encrypted parts of CT No. 2. **a** Original CT sequence No.1. **b** Histogram of original CT. **c** Histogram of ciphertext

Table 4 Correlation coefficients of the original volume (r_{xy}) and the corresponding ciphered volume ($\tilde{r}_{xy}$); (v), (h) and (d) are related to vertical, horizontal and diagonal adjacency respectively

$r_{xy}(v)$	$\tilde{r}_{xy}(v)$	$r_{xy}(h)$	$\tilde{r}_{xy}(h)$	$r_{xy}(d)$	$\tilde{r}_{xy}(d)$
0.9838	−0.0006	0.9863	−0.0002	0.9958	0.0005

where P is the number of different values that the pixels of the ciphered image can assume, N_i is the amount of pixels of the ciphered image that assume value i, and N is the total amount of pixels of the ciphered image. During the experiments, we found that the ciphered pixels' intensity of all the algorithms mentioned in the paper are almost equiprobable, so their normalized entropy are all approximate to 1.

Rate-distortion

Rate-distortion (RD) is an important indicator to evaluate the performance of compression. In a previous study [32], the following mathematical model of CS RD was constructed:

$$D^{CS}(R) = \gamma \frac{\mu}{\mu - 1} \sigma_\theta^2 2^{-2R} \tag{23}$$

The proposed TCS-based algorithm falls into the CS category, so the model in Eq. (23) applies for our algorithm. Because there are some differences between traditional vector-based CS and the proposed tensor-based CS, we recalculate some parameters as follows:

$$D^{TCS}(R) = \gamma' \frac{\mu'}{\mu' - 1} \sigma_\Phi^2 2^{-2R} \tag{24}$$

where $\gamma' = \frac{K}{m_1 m_2 m_3}$, $\mu' = \frac{M_1 M_2 M_3}{K}$, σ_Φ is the singular value of the measurement matrix and R is the rate. It is important to note that in 3D case, there is $\sigma_{\Phi_1} \approx \sigma_{\Phi_2} \approx \sigma_{\Phi_3}$ because the three matrices obey a uniform Gaussian distribution. The RD diagram at several compression ratio points is shown in Fig. 10.

Secret keys

Key space

The keys of the proposed algorithm consist of those generated by the three measurement matrices with 3D Lorenz and the unfolding mode n of the core tensor $\mathcal{W}$. The Key that are used on Φ_i with 3D Lorenz are the initial values for the three state variables, the U_0, V_0 and W_0, the parameters A, B and C, and g_i for each of the state equations. As shown in [25], the key length is 39 decimal digits, with a key space of 10^{39}. The order of the tensor product can be used as an additional key, which has 18 combinations (which will be introduced in detail in "Key sensitivity").

The total key space of the proposed algorithm is larger than $10^{39} \cdot 18 >> 2^{30}$, which is large enough to withstand a brutal attack.

Key sensitivity

The key sensitivity of measurement matrices with 3D Lorenz has been analyzed in detail to demonstrate their advantages [15, 24–26]. Here we emphasize the key sensitivity of the order of the tensor product. Although $\mathbf{W}_{(n)}$ is easy to be distinguished from $D_{\Phi n}$, the ciphertexts are still difficult to decode due to both $\mathbf{W}_{(n)}$ and $D_{\Phi n}$ having three models. Hence there are a totally of 18 combinations of all $\mathbf{W}_{(n)}$ and $D_{\Phi n}$. Equation (16) indicates that only three combinations are correct, with 15 wrong combinations listed in the following:

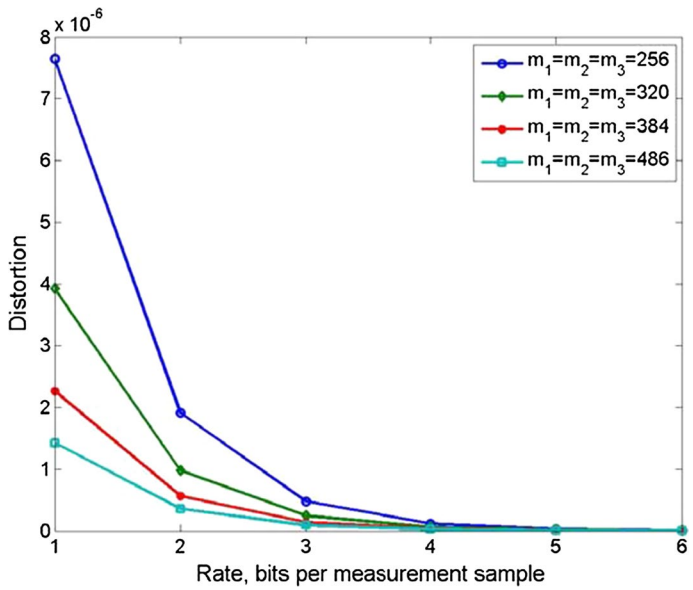

Fig. 10 RD diagram at varying compression ration

$D_{\Phi_1} \cdot \mathbf{W}_{(1)} \cdot \left(D_{\Phi_3} \otimes D_{\Phi_2}\right)^T$, $D_{\Phi_2} \cdot \mathbf{W}_{(1)} \cdot \left(D_{\Phi_1} \otimes D_{\Phi_3}\right)^T$, $D_{\Phi_2} \cdot \mathbf{W}_{(1)} \cdot \left(D_{\Phi_3} \otimes D_{\Phi_1}\right)^T$, $D_{\Phi_3} \cdot \mathbf{W}_{(1)} \cdot \left(D_{\Phi_1} \otimes D_{\Phi_2}\right)^T$, $D_{\Phi_3} \cdot \mathbf{W}_{(1)} \cdot \left(D_{\Phi_2} \otimes D_{\Phi_1}\right)^T$, $D_{\Phi_1} \cdot \mathbf{W}_{(2)} \cdot \left(D_{\Phi_2} \otimes D_{\Phi_3}\right)^T$, $D_{\Phi_1} \cdot \mathbf{W}_{(2)} \cdot \left(D_{\Phi_3} \otimes D_{\Phi_2}\right)^T$, $D_{\Phi_2} \cdot \mathbf{W}_{(2)} \cdot \left(D_{\Phi_1} \otimes D_{\Phi_3}\right)^T$, $D_{\Phi_3} \cdot \mathbf{W}_{(2)} \cdot \left(D_{\Phi_1} \otimes D_{\Phi_2}\right)^T$, $D_{\Phi_3} \cdot \mathbf{W}_{(2)} \cdot \left(D_{\Phi_2} \otimes D_{\Phi_1}\right)^T$, $D_{\Phi_1} \cdot \mathbf{W}_{(3)} \cdot \left(D_{\Phi_2} \otimes D_{\Phi_3}\right)^T$, $D_{\Phi_1} \cdot \mathbf{W}_{(3)} \cdot \left(D_{\Phi_3} \otimes D_{\Phi_2}\right)^T$, $D_{\Phi_2} \cdot \mathbf{W}_{(3)} \cdot \left(D_{\Phi_1} \otimes D_{\Phi_3}\right)^T$, $D_{\Phi_2} \cdot \mathbf{W}_{(3)} \cdot \left(D_{\Phi_3} \otimes D_{\Phi_1}\right)^T$, $D_{\Phi_3} \cdot \mathbf{W}_{(3)} \cdot \left(D_{\Phi_2} \otimes D_{\Phi_1}\right)^T$.

The average MSE of the 15 wrong combinations is 7.2895×10^3. It is clear from the MSE values of the different combinations that the proposed system is sensitive to the order of the tensor product.

The 3D Lorenz system is similar to that in [26]. The 3D image is encrypted with initial conditions $U_0 = 0.1$, $V_0 = 0$, $W_0 = 0$, and parameters $A = 10$, $B = 28$, $C = 8/3$, and $g1 = g2 = g3 = 0.01$. The maximum Lyapunov value according to the parameters and initial conditions is 0.8024 (larger than 0), the system is chaotic. The 3D distribution of the Lorenz system is also depicted in Fig. 11. Table 5 gives the sensitivity of each parameter. Any change in a parameter greater than its sensitivity will prevent an eavesdropper from decrypting message.

Resistance against attacks

Common attacks include known-plaintext attack and chosen-plaintext attacks. It has been proven [10, 11] that despite the linearity of its encoding, CS may be used to provide a limited form of data protection. The TCS used in the paper is a multi-linear (nonlinear) extension of the traditional CS, which further enhances the anti-attack ability. Although the attackers have access to some plaintext-ciphertext pair, they will be unable to reproduce the system without knowledge of the order of tensor product. Furthermore, the 3D Lorenz, which was introduced in the system, has the ability to withstand these common attacks [25, 26]. Therefore, the proposed system based on TCS with 3D Lorenz has the ability to resist these common attacks.

We ran an experiment on known-plaintext attack to evaluate the anti-attack performance. The decryption result of known-plaintext attack with the keys generated from a chosen CT sequence, which was treated as fake tensor, is displayed in Fig. 12. The frame

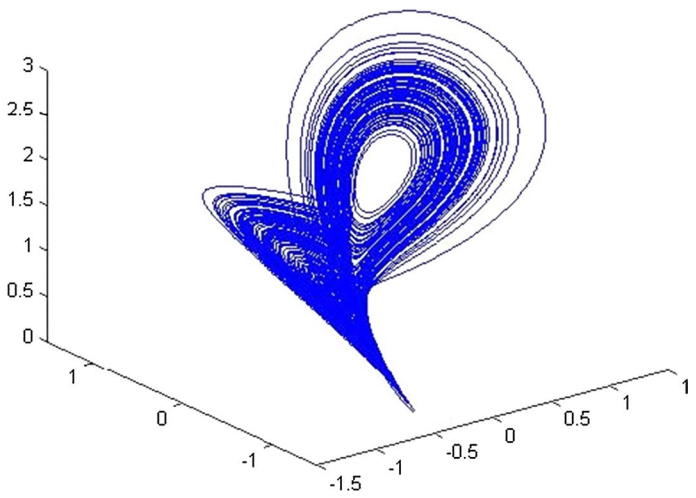

Fig. 11 3D distribution of Lorenz system

Table 5 Key sensitivity of measurement matrices with 3D Lorenz

Keys	$\Delta U_0 = 10^{-6}$	$\Delta V_0 = 10^{-6}$	$\Delta W_0 = 10^{-6}$	$\Delta A = 10^{-4}$	$\Delta B = 10^{-4}$	$\Delta C = 10^{-4}$	$\Delta g1 = 10^{-7}$	$\Delta g2 = 10^{-7}$	$\Delta g3 = 10^{-7}$
MSE	8.50×10^3	8.39×10^3	8.61×10^3	9.01×10^3	8.67×10^3	8.22×10^3	8.96×10^3	9.00×10^3	8.65×10^3

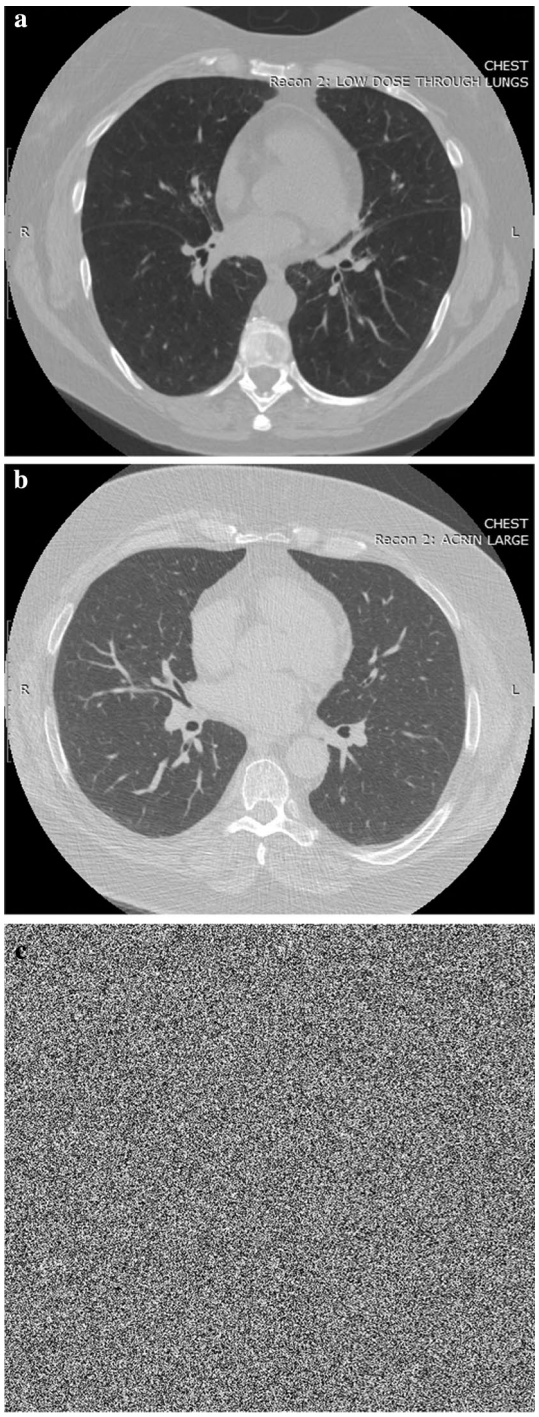

Fig. 12 Decryption result of known-plaintext attack with the keys generated from a chosen CT sequence. **a** Original image. **b** Image used for attack. **c** Decrypted image with fake decryption keys

256 of the original and fake CT sequences are shown in Fig. 12a, b, respectively. The attack result using fake decryption keys with all correct parameters is shown in Fig. 12c. It can be seen that the retrieved image is noise-like signal. We first analyze the number of pixels rate: all pixels assumed to be an even distribution, because the retrieved image

was noise-like signal. The unified average changing intensity was also used to evaluate the difference among the original and decrypted images:

$$\xi = \frac{1}{M_1 M_2 M_3} \sum_{k=1}^{M_3} \sum_{j=1}^{M_2} \sum_{i=1}^{M_1} \left| \mathcal{A}'(i,j,k) - \mathcal{A}(i,j,k) \right| \tag{25}$$

We used the gray level to represent intensity, ranging from 0 to 255. Because the intensity value per pixel of the tensor was up to $\xi = 80$, we assume that there is a substantial difference between the original and retrieved images.

Conclusions

In this paper, we proposed an algorithm of simultaneous encryption and compression, as applied to 3D CT volumes. This scheme has the advantages of TCS and 3D Lorenz. Its outstanding advantage is that it achieves a high precision of decryption at a big compression ratio. The security of the proposed algorithm conformed to the requirements of the common encryption technology. Moreover, the unfolding mode, which is a unique feature of the tensor product, can be used as an additional secrete key other than traditional encryption algorithms to make unauthorized decryption harder.

Authors' contributions

Conceived and designed the experiments: QW. Performed the experiments: XC and MW. Analyzed the data: ZM. Wrote the paper: QW. All authors read and approved the final manuscript.

Author details

[1] School of Information Engineering, Northeast Dianli University, Jilin 132012, China. [2] Department of Neurosurgery, China-Japan Union Hospital of Jilin University, Changchun, China.

Acknowledgements

Not applicable.

Availability of data and materials

The LIDC datasets used in the experiments of this article are available for download, upon request, from https://public.cancerimagingarchive.net/ncia/dataBasketDisplay.jsf. If the users have opened the website, they can tap the submenu "Simple search" of menu "Search images", and then chose the "LIDC-IDRI" of item "Collection(s)". The Subject ID of the CT set used in the paper is "LIDC-IDRI-1004".

Competing interests

The authors declare that they have no competing interests.

Ethics approval and consent to participate

This experiment was approved by the China-Japan Union Hospital of Jilin University Medical Research Ethics Committee, Changchun, China.

Funding

This study was funded by National Natural Science Foundation of China (61301257).

Received: 10 April 2016 Accepted: 26 October 2016
Published online: 04 November 2016

References

1. Kanso A, Ghebleh M. An efficient and robust image encryption scheme for medical applications. Commun Nonlinear Sci Numer Simul. 2015;24:98–116.
2. Karakis R, Guler I, Capraz I, et al. A novel fuzzy logic-based image steganography method to ensure medical data security. Comput Biol Med. 2015;67:172–83.
3. Chen L, Wang SH. Differential cryptanalysis of a medical image cryptosystem with multiple rounds. Comput Biol Med. 2015;65:69–75.
4. Ye CH, Xiong ZG, Ding Y, et al. Joint fingerprinting/encryption for medical image security. Int J Secur Appl. 2015;9(1):409–18.
5. Zhang LB, Zhu ZL, Yang BQ, et al. Medical image encryption and compression scheme using compressive sensing and pixel swapping based permutation approach. Math Probl Eng. 2015;2015:1–9.

6. Lima JB, Madeiro F, Sales FJR. Encryption of medical images based on the cosine number transform. Sig Process Image Commun. 2015;35:1–8.
7. Ma JL, Zhang TT, Dong MC. A novel ECG data compression method using adaptive fourier decomposition with security guarantee in e-health applications. IEEE J Biomed Health Inform. 2015;19(3):986–94.
8. Alfalou A, Brosseau C, Abdallah N. Simultaneous compression and encryption of color video images. Opt Commun. 2015;338:371–9.
9. Donoho DL. Compressed sensing. IEEE Trans Inf Theory. 2006;52(4):1289–306.
10. Cambareri V, Marngia M, Pareschi F, Rovatti R, Setti G. On known-plaintext attacks to a compressed sensing-based encryption: a quantitative analysis. IEEE Trans Inf Forensics Secur. 2015;10(10):2182–95.
11. Cambareri V, Mauro M, Fabio P, et al. Low-complexity multiclass encryption by compressed sensing. IEEE Trans Signal Process. 2015;63(9):2183–95.
12. Zhou NR, Zhang A, Zheng F, et al. Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. Opt Laser Technol. 2014;62:152–60.
13. Zhou NR, Li HL, Wang D. Image compression and encryption scheme based on 2D compressive sensing and fractional mellin transform. Opt Commun. 2015;343:10–21.
14. Rawat N, Hwang I, Shi Y, Lee BG. Optical image encryption via photon-counting imaging and compressive sensing based ptychography. J Opt. 2015;17(6):1–11.
15. Zhao SM, Wang L, Liang WQ, Cheng WW, Gong LY. High performance optical encryption based computational ghost imaging with QR code and compressive sensing technique. Opt Commun. 2015;353:90–5.
16. Lang J, Zhang J. Optical image cryptosystem using chaotic phase-amplitude masks encoding and least-data-driven decryption by compressive sensing. Opt Commun. 2015;338:45–53.
17. Ran QW, Yuan L, Zhao TY. Image encryption based on nonseparable fractional fourier transform and chaotic map. Opt Commun. 2015;348:43–9.
18. Nitin R, Byoungho K, Inbarasan M, et al. Compressive sensing based robust multispectral double-image encryption. Appl Opt. 2015;54(7):1782–93.
19. Nitin R, Byoungho K, Rajesh K, et al. Fast digital image encryption based on compressive sensing using structurally random matrices and Arnold transform technique. Optik. 2016;127:2282–6.
20. Bairagi VK, Sapkal AM. Automated region-based hybrid compression for digital imaging and communication in medicine magnetic resonance imaging images for telemedicine applications. IET Sci Meas Technol. 2012;6(4):247–63.
21. Cesar FC, Andrzej C. Stable, robust, and super fast reconstruction of tensors using multi-way projections. IEEE Trans Signal Process. 2015;63(3):780–93.
22. Marco FD, Richard GB. Kronecker compressive sensing. IEEE Trans Image Process. 2012;21(2):494–504.
23. Friedland S, Li Q, Schofeld D. Compressive sensing of sparse tensors. IEEE Trans Image Process. 2014;23(10):4438–46.
24. Sidiropoulos ND, Kyrillidis A. Multi-way compressed sensing for sparse low-rank tensors. IEEE Signal Process Lett. 2012;19(11):757–60.
25. Mohamed FH, Gulliver TA. Real-time image encryption using a low-complexity discrete 3D dual chaotic cipher. Nonlinear Dyn. 2015;82:1523–35.
26. Mohamed FH, Gulliver TA. A new 3D chaotic cipher for encrypting two data streams simultaneously. Nonlinear Dyn. 2015;81:1053–66.
27. Suryadi MT, Eva N, Dhian W. Performance of chaos-based encryption algorithm for digital image. TELKOMNIKA. 2014;12(3):675–82.
28. Bernard NS, Yousef S. Higher order orthogonal iteration of tensors (HOOI) and its relation to PCA and GLRAM. Proceedings of the 7th SIAM international conference on data mining. 2007. p. 355–65.
29. Wang L, Bai J, Wu J, et al. Hyperspectral Image compression based on lapped transform and tucker decomposition. Sig Process Image Commun. 2015;36:63–9.
30. Ballester RR, Suter SK, Pajarola R. Analysis of tensor approximation for compression-domain volume visualization. Comput Graph. 2015;47:34–47.
31. Lung Image Database Consortium (LIDC), National Cancer Institute. http://imaging.cancer.gov/programsandresources/InformationSystems/LIDC. Accessed 3 Nov 2016.
32. Coluccia G, Roumy A, Magli E. Operational rate-distortion performance of signal-source and distributed compressed sensing. IEEE Trans Commun. 2014;62(6):2022–33.

Submit your next manuscript to BioMed Central and we will help you at every step:

- We accept pre-submission inquiries
- Our selector tool helps you to find the most relevant journal
- We provide round the clock customer support
- Convenient online submission
- Thorough peer review
- Inclusion in PubMed and all major indexing services
- Maximum visibility for your research

Submit your manuscript at
www.biomedcentral.com/submit