Encryption algorithm for medical volume data based on three-dimensional Arnold transformation and chaos

Lei Hao
College of Information Science and Technology
Hainan University
Haikou, China
haoleihainu@163.com

Jingbing Li *
College of Information Science and Technology
Hainan University
Haikou, China
Jingbingli2008@hotmail.com

Abstract: **Three-dimensional medical volume data such as high-resolution map of medical CT, advanced optical images of scanners and MRI has increasingly developed to facilitate medicine diagnosis, the information storage, and the transmission, while it also brings security issues. In this paper, an encryption algorithm is presented, considering the security of three-dimensional medical volume data. Firstly, the position of the pixels of the medical volume data is scrambled by three-dimensional Arnold and a chaotic sequence is produced by Logistic map. Secondly, the image feature value is extracted as a key into the encryption process, and then a feedback mechanism was set up to change the pixel values. Finally, the definition of encryption performance indicators in the volume data is promoted. Through simulation, the algorithm has a large key space, which is highly sensitive to the initial value of keys. Furthermore, it can resist statistical, brute-force attack and differential attack effectively. The proposed encryption algorithm in this paper has high security and practical value, giving inspiration on security issues in the future with the large emergence of the three-dimensional volume data.**

Key words: Medical volume data; Chaotic Encryption; Arnold transformation; Image features;

I. INTRODUCTION

In recent years, with the rapid development of communication technology and the Internet, China's health care system is upgrading quickly. A wide variety of multimedia, such as medical data, appears to facilitate the medicine diagnosis, the information storage, and the transmission, while it also brings security issues.

Chaos-based digital image encryption and hiding technology play an important role in branch of cryptography research. Many practical digital image encryption algorithms are put forward in literature [1-4].

Tong and Cui [1] constructed compound chaotic function, and put forward encryption algorithm with three-dimensional Baker mapping. Kanso and Ghebleh [2] proposed grayscale (color) image encryption scheme based on 3D Arnold. Mandal [3] gave the image encryption algorithm based on chaotic sequence and bit operations. Yicong Zhou et al [4] proposed a new one-dimensional chaotic system image encryption.

We proposed an encryption algorithm for medical volume data based on three-dimensional Arnold transformation and chaos, according to the basis of digital image encryption technology and methods existed, and promoted the definition of encryption performance indicators in the volume data.

II. THE FUNDAMENTAL THEORY

A. Logistic map

A chaotic system has a noise like behavior while it is exactly deterministic. One of the most famous chaotic systems is Logistic Map, which is nonlinear return map given by:

$$x_{k+1} = \mu x_k (1- x_k) \qquad (1)$$

where $0 \le \mu \le 4$ and $x_k \in (0,1)$ are the system variable and parameter respectively, and k is the number of iteration. Logistic Map system works under chaotic condition when $3.569945 \le \mu \le 4$. It can be seen that a small difference in initial conditions would lead to a significant difference of chaotic sequences. In this paper, we set μ =4.

B. Three-dimensional Arnold transformation

Cat map was first proposed by Chen G introduced in literature [5]. The two-dimensional map can be expressed as:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \quad A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \qquad (2)$$

It can be promoted for their generalized form:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \quad A = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \qquad (3)$$

It will be extended to three-dimensional map [5]:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} (\bmod N) \qquad (4)$$

$$A = \begin{bmatrix} 1 + a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y a_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x b_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{bmatrix}$$

When $a_x = b_x = a_y = b_y = a_z = b_z = 1$, the above conversion is given by :

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} (\bmod N) \quad A = \begin{bmatrix} 2 & 1 & 3 \\ 3 & 2 & 5 \\ 2 & 1 & 4 \end{bmatrix} \qquad (5)$$

Three Lyapunov characteristic index of matrix A above are: $\sigma_1 = 7.18 > 1, \sigma_2 = 0.24 < 1, \sigma_3 = 0.57 < 1$. So, this mapping is chaotic map.

III. ENCRYPTION AND DECRYPTION ALGORITHMS

Assuming that a grayscale image of medical volume data ranks at the size of hx, hy, hz, in the range of each pixel is an integer from 0 to 255. hx, hy, hz will be used as an internal key.

1) Since the three-dimensional Arnold transformation is a cube transformation, firstly we will convert it to N*N*N cube data:

$$N = ceil((hx \cdot hy \cdot hz)^{1/3}) \qquad (6)$$

Cube date is filled with original data in sequence, and the rest are zero.

2) Position of medical images was scrambled by three-dimensional Arnold. The value A is of exceptions.

3) Chaotic sequence was produced by Logistic map at the length of N*N*N. Here, $\mu = 4$, x_1 is key.

4) Feature value is calculated:

$$s(c) = \sum_{k=1}^{N} \sum_{j=1}^{N} \sum_{i=1}^{N} temp(i, j, k) \bmod 256 \qquad (7)$$

Where, temp(i,j,k) is scrambled cube data. c is the encryption process cycles and each cycle s (c) is different. s are different at the encryption process for each image, and the value of s is internal key for decryption.

5) New chaotic sequence is generated combined with the image features. Chaotic sequence changes based on s at each encryption, and it can improve the capability against differential attack. bl is chaotic sequence provided by the third step , and new chaotic sequence c_seq generating rule is as follows:

$$c\_seq = round(\bmod(K \cdot s^2 \cdot bl + \lambda, 256)) \qquad (8)$$

Where, K is the amplification factor, λ is the adjustment factors, both are the keys.

6) Proceed the scrambled cube data as follows:

$$\begin{cases} temp(1) = \bmod(c\_seq(1) + temp(1), 256) & i = 1 \\ temp(i) = \bmod(c\_seq(i) + temp(i) + temp(i-1), 256) & i \geq 2 \end{cases} \qquad (9)$$

Where, temp(i) is the current processing pixel, and temp(i-1) is the last processed pixel value.

A feedback mechanism is used, so that the encrypted result of each pixel is related with the last pixels. The encryption process is more relevant and more complicated.

After processing, temp(i) is the encrypted image and $x_1, K, \lambda, n, hx, hy, hz$ are the keys passing to cracker by the real-time channel.

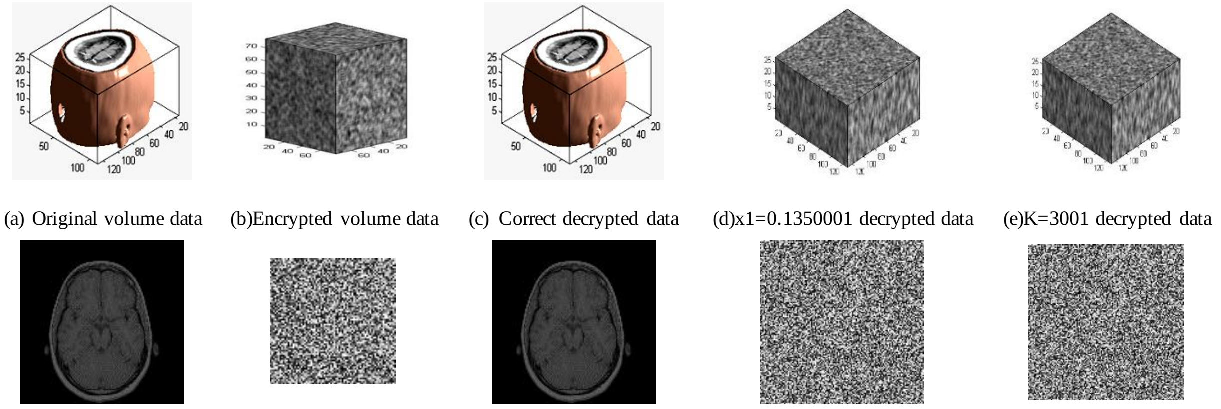
6) Decryption algorithm is the inverse operation of the encryption process.

IV. SIMULATION RESULTS AND PERFORMANCE ANALYSIS

The simulation platform was MATLAB 2012a. The encryption algorithm was analyzed taking the head CT volume data at the size of 128*128*27 for example and was chosen by the formula (1)-(8), x_1, K, λ, n as the encryption key: (0.133, 3000,118,3)

A. Key space and sensitivity analysis

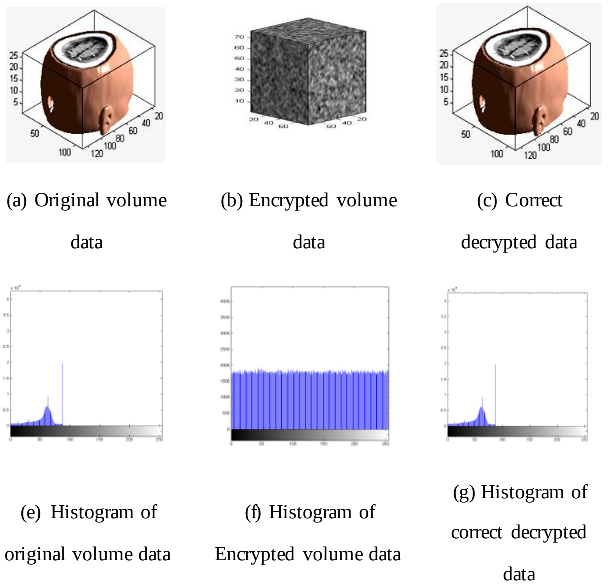
There are four external keys and four internal keys from encryption process. So, key space is large enough. Original encryption keys are (0.135, 3000, 118, 3). We changed the value of one key shown in Fig.1.



(a) Original volume data (b)Encrypted volume data (c) Correct decrypted data (d)x1=0.1350001 decrypted data (e)K=3001 decrypted data

(f) Original slice (g) Encrypted slice (h) Correct decrypted slice (i)x1=0.1350001 decrypted slice (j)K=3001 decrypted slice

Fig.1. The data and slice of the medical body decrypted by the key



(a) Original volume data (b) Encrypted volume data (c) Correct decrypted data

(e) Histogram of original volume data (f) Histogram of Encrypted volume data (g) Histogram of correct decrypted data

Fig.2. Histogram comparison of medical volume data

B. Statistical Characteristics

1) Histogram Analysis

By comparing the two figures, we can find that the histogram is uniform in encrypted data, sharing a big difference with that in original image. The histogram has good disruptive and diffusion, which can resist statistical attacks effectively.

2) Correlation analysis of adjacent pixels

The image has a great correlation between adjacent pixels, which makes it easy to be attacked statistically. One of the encryption aims is to upset correlation between adjacent pixels to resist statistical attack.

Referring to two-dimensional data correlation analysis, six neighboring directions for volume data are defined, respectively x, y, z, xy, yz, xz direction. Correlation is defined as follows in each direction:

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (10)$$

where, $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$

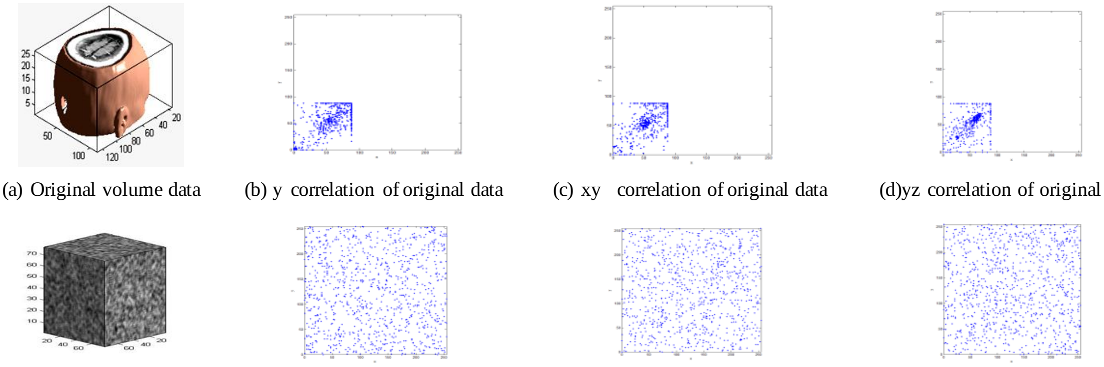
$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$$

$$\operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))$$

1000-3000 adjacent pixels are selected randomly from the x, y, z, xy, yz, xz directions to draw related illustration.

TABLE I. CORRELATION BETWEEN ADJACENT PIXELS BEFORE AND AFTER ENCRYPTION

	x direction	y direction	z direction	xy direction	xz direction	yz direction
Original data	0.8863	0.9472	0.9242	0.9472	0.8896	0.9261
Encrypted data	-0.0002	-0.002	-0.0004	0.0113	0.0120	0.0130



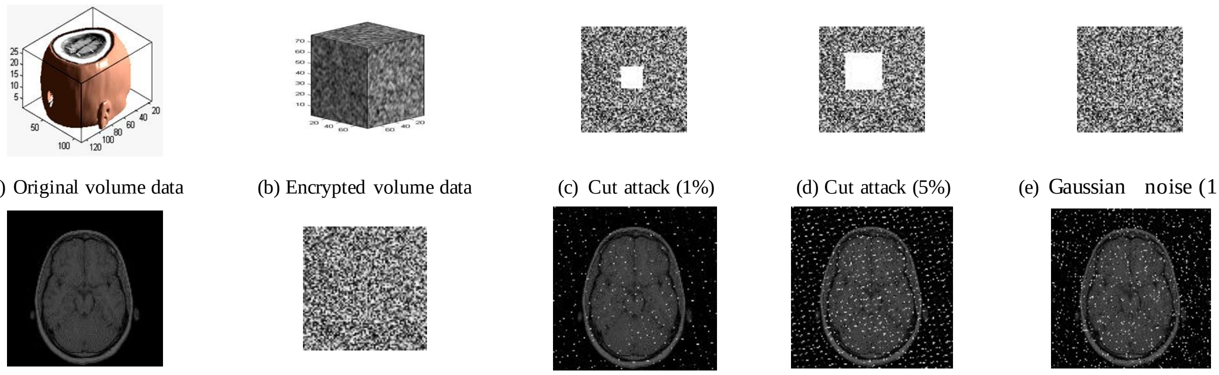
(a) Original volume data (b) y correlation of original data (c) xy correlation of original data (d)yz correlation of original data

(e) Encrypted volume data (f) y correlation of Encrypted data (g) xy correlation of Encrypted data (h) yz correlation of Encrypted data

Fig.3. Correlation illustration of volume data encryption before and after

C. Interference analysis

The encrypted image will suffer devastating attacks such as cut-and-noise attack through transmission channel and network. This algorithm has a good effect against them. After cutting and noise attack in encrypted data, decrypted data has only minor damage shown in Fig.4.



(a) Original volume data (b) Encrypted volume data (c) Cut attack (1%) (d) Cut attack (5%) (e) Gaussian noise (1%)

(f) Original slice (g) Encrypted slice (h) Encryption（1%） (i) Encryption (5%) (j) Encryption (1%)

Fig.4. Decrypted images after the attacks

V. CONCLUSION

Processing method will be promoted with the continuous development of network technology and the appearing of more kinds of volume data. The encryption algorithm for three-dimensional medical volume data in this paper has high security and practical value giving inspiration on security issues in the future with the large emergence of the three-dimensional volume data. Security issues can be studied later on ordinary gray images and color images of volume data.

ACKNOWLEDGMENT

This work is supported by National Natural Science Foundation of China (No. 61263033 and 61363007), and by International Science and Technology Cooperation Project of Hainan (NO. KJHZ201504) and the Institutions of Higher Learning Scientific Research Special Project of Hainan (NO. Hnkyzx2014-2).

REFERENCES

[1] Tong X J,Cui M G.Image encryption scheme based on 3D Baker with dynamical compound chaotic sequence cipher generator[J].Signal Processing, 2009,89;480-491.

[2] Kanso A, Ghenleh M.A novel iamge encryption algorithm based on a 3D chaotic map[J]. Communications in Nonlinear Science Numerical Simulation,2012,17:2943-2959.

[3] M. K. Mandal, G.D. Banik, D. Chattopadhyay et al. An Image Encryption Process based on Chaotic Logistic Map. IETE Technical Review. 2012,29(5),395-404.

[4] Yicong Zhou, Long Bao, C. L. Philip Chen. A new 1D chaotic system for image encryption[J]. Signal Processing , 2014 (97):172-182

[5] Chen Guanrong, Mao Yaobin , Charles K Chui .A symmetric image encryption scheme based on 3D chaotic cat maps[J].Chaos Solution and Fractals, 2004;1:749-761.