Liu and Miao *SpringerPlus (2016)5:289*
DOI 10.1186/s40064-016-1959-1

SpringerPlus
a SpringerOpen Journal

RESEARCH Open Access

A new image encryption algorithm based on logistic chaotic map with varying parameter

Lingfeng Liu[1*] and Suoxia Miao[2]

*Correspondence:
vatanoilcy@163.com
[1] School of software, Nanchang University, Nanchang 330031, People's Republic of China
Full list of author information is available at the end of the article

Abstract

In this paper, we proposed a new image encryption algorithm based on parameter-varied logistic chaotic map and dynamical algorithm. The parameter-varied logistic map can cure the weaknesses of logistic map and resist the phase space reconstruction attack. We use the parameter-varied logistic map to shuffle the plain image, and then use a dynamical algorithm to encrypt the image. We carry out several experiments, including Histogram analysis, information entropy analysis, sensitivity analysis, key space analysis, correlation analysis and computational complexity to evaluate its performances. The experiment results show that this algorithm is with high security and can be competitive for image encryption.

Keywords: Chaos, Image encryption, Dynamical algorithm, Parameter-varied logistic map

Background

With the rapid development in internet technology and multimedia technology, multimedia communication has become more and more important. Therefore, image encryption has become an increasingly serious issue and urgently needed (Ye and Wong 2013). However, traditional encryption algorithms, such as RSA, DES and IDEA, are not suitable for image encryption due to image's intrinsic properties such as bulky data capacity, strong redundancy and strong correlations among adjacent pixels (Wang et al. 2012; Chen et al. 2013; Coppersmith 1994).

Chaotic system has many important properties, such as unpredictability, similar randomness, aperiodicity, sensitive dependence on initial conditions and parameters, these properties make chaotic systems become popular in image encryption (Huang 2012; Wang and Guo 2014; Zhang and Zhao 2014; Zhang and Liu 2011; Hua et al. 2015; Tong et al. 2015; Hussain and Shah 2013). Among all the chaotic encryption image algorithm, the low-dimensional chaotic map are always used for its easily implement, such as logistic map. However, some common weaknesses of the logistic map, including relatively small key space and uneven distribution of sequences, et al, bring some security risks for encryption. On the other hand, for a deterministic chaotic system, the chaos behaviors can be discerned by using some methods in chaos theory. Once we find some

information about the chaotic system, we can use such information to help us finding the secret key. In many chaotic ciphers, such as Kanso and Smaoui (2009), Zhou and Liao (2012), Sun et al. (2010), Pareek et al. (2005), Wong et al. (2003), Liu and Wang (2010), Wang et al. (2012), Patidar et al. (2010), Gonzalez and Hernandez (2013), the ciphertext directly depends on the chaotic orbit of a single chaotic system, the orbit sequence comes to be stationary, so the extraction of such information may be possible by using some chaos theory methods such as phase space reconstruction. In Short (1994), short use the phase space reconstruction method, has successfully attacked almost all the low-dimensional chaotic systems. Wang and Luan (2013) propose a three-dimensional coupled logistic maps to overcome the weaknesses of logistic map, however, the system is still deterministic, and is still under the risk of being attacked by phase space reconstruction.

As we know, varying the parameters can disrupt the phase space of a chaotic system, and improve the security to resist the phase space reconstruction attack. Some varying parameter techniques have been proposed, e.g., Murillo-Escobar et al. (2015) use 32 hexadecimal digits to vary the parameter and initial value of logistic map, and the proposed system can avoid the small key space of low dimensional chaotic systems. This varying technique is given by 32 fixed hexadecimal digits, which is not that secure. Using a prediction technique based on wavelet neural network and multiwavelets neural network can predict the parameter-varying chaotic system whose parameters are varying in a simple way (Xiao and Gao 2006). Wang et al. (2009) use the generated sequences by logistic map to control three kinds of typical two-dimensional chaotic maps, but do not show the performances of their parameter-varied chaotic maps.

Therefore, in order to improve the weaknesses of logistic map and resist the phase space reconstruction attack, we propose an image encryption algorithm based on logistic map with varying parameter. The varying technique is based on the zero-mean logistic map, which can make the parameter varying in a random-like way. We show that the parameter-varied logistic map can cure the weaknesses of logistic map and is capable to resist phase space reconstruction. Furthermore, we use a dynamical algorithm in our encryption algorithm. Our encryption algorithm is related to the plaintext, which can resist known and chosen-plaintext attacks. The experimental results show that the proposed algorithm is with high security, and can be competitive to other proposed algorithms.

The rest of this paper is organized as follows. In "Shuffling algorithm" section, a shuffling algorithm based on parameter-varied logistic system is described. We show that the parameter-varied logistic system can cure the common weaknesses and is capable to resist phase space reconstruction. "Dynamical encryption algorithm" section introduce a dynamical algorithm for the image encryption. The experimental results, analysis and comparison are shown in "Experimental analysis" section. Finally, "Conclusion" section concludes the paper.

Shuffling algorithm

In this section, we propose a shuffling method based on parameter-varied chaotic map. Perhaps, the one-dimensional maps are the simplest mathematical objects to display chaotic behavior (Lasota and Mackey 1994). The logistic maps are one kind of

one-dimensional maps, which were described in May (1976) and have already been widely used in image encryption

$$x_{i+1} = f(x_i) = ax_i(1 - x_i) \tag{1}$$

here, a is the parameter of logistic map, $x_i = f^{(i)}(x_0) \in I$, $i = 0, 1, 2,\ldots$ and f: $I \to I$, where I denotes an interval. For $3.5699 < a \leq 4$, Eq. (1) turns to be chaotic. Using this function, we can obtain a real-valued sequence by iteration of an initial value x_0. Since some researches show that the sequences generated by logistic map are not secure with some weaknesses (Wang and Luan 2013), including relatively small key space, an uneven distribution and easily be attacked by phase space reconstruction, therefore, we use the following parameter-varying logistic map in our algorithm.

$$x_{i+1} = f_k(x_i) = (10^6 - 1) \cdot a_k x_i(1 - x_i) \bmod 1,\ k = 1, 2, \ldots, M \tag{2}$$

here, a_k is the varied parameter, M is the cardinality of the parameter set. We use the following zero-mean logistic map to vary the parameter a_k

$$u_{k+1} = 1 - 2u_k^2\ (-1 \leq u_k \leq 1) \tag{3}$$

Divide the interval $[-1, 1]$ into M sub-intervals τ_i, $i = 0, 1, \ldots, M - 1$. Denote $\tau_i = [t_i, t_{i+1})$, $i = 0, 1, \ldots, M - 2$, and $\tau_{M-1} = [t_{M-1}, t_M]$, where

$$t_i = -\cos\left(\frac{k}{M}\pi\right) \tag{4}$$

Then, $\alpha = \{\tau_0, \tau_1, \ldots, \tau_{M-1}\}$ is a finite measurable partition of I. Denote a correspondence S: $I \to \{0, 1, 2, \ldots, M - 1\}$ from the set I to the set $\{0, 1, 2, \ldots, M - 1\}$. For any u_k, define

$$s(u_k) = i, \quad \text{if } u_k \in \tau_i \tag{5}$$

here $s(u_k)$ is the symbol representation of the real number u_k according to the partition α. Then, the generated integer sequence is denoted as $\{s_k\}$ and can be proved to be uniformly distributed in set $\{0, 1,\ldots, M - 1\}$ (Hu et al. 2004). Let the parameter set be $\{c_1, c_2,\ldots, c_M\}$, we use the sequence $\{s_k\}$ to vary the parameter a as

$$a_k = c_{s_k+1} \tag{6}$$

Then, the parameter a_k of Eq. (2) is varying chaotic in the set $\{c_1, c_2,\ldots, c_M\}$. Let n be the steps of iteration with each parameter a_k, we can generate the chaotic binary sequences by using the following algorithm.

$$b_i = \begin{cases} 0, & x_i \leq 0.5 \\ 1, & x_i > 0.5 \end{cases} \quad i = 0, 1, \ldots \tag{7}$$

Figure 1 shows the main frame of our pseudorandom bit generator. As we seen, the number M of different values of the parameter and the iteration step n for each parameter are two important parameters in our parameter-varied logistic map. Studies show that the logistic map can be reconstructed with delay time 1 and embedding dimension 3 (Han et al. 2015). For each parameter, if we don't generate enough data, the reconstruction will fail. Therefore, we have that $n < 3$ is more suitable. In this paper, we choose

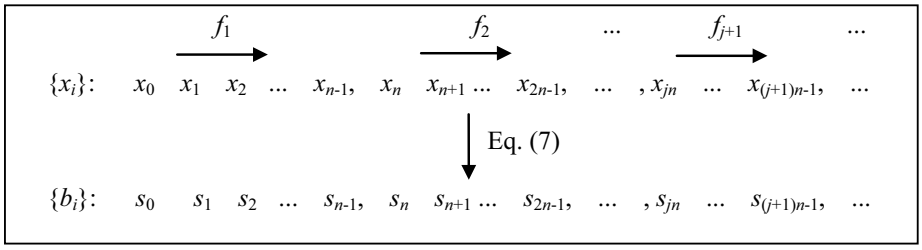

Fig. 1 The output of logistic map with varying parameter

$n = 1$, which can be regarded as a well-known random logistic map. Obviously, the larger the number M is, the more kinds of iterative rule has. However, it is impossible to choose M to be infinite. In order to determine the value M, we use approximate entropy (ApEn) to evaluate the complexity of the generated sequences. Before this experiment, we first calculate the ApEns of sequences generated by different parameter a_k in Fig. 2, which indicates that the generated sequence has approximately the same complexity with different parameter. The ApEns with different M is shown in Fig. 3. From Fig. 3 we have that, when M is close to 9, the complexity approximately remains the same. As the complexity has almost no relation to the value of parameter, thus, is only influenced by the number of different parameters. Therefore, in this paper, we choose $M = 9$.

Next, we show that our logistic map with varying parameter can improve the weaknesses of logistic map. Firstly, the initial values x_0, u_0 and nine different parameters

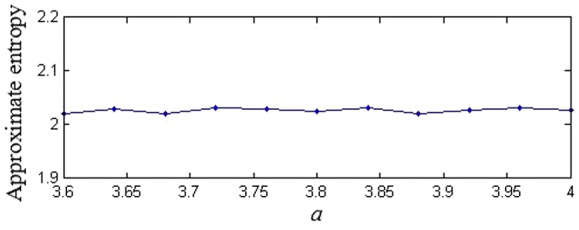

Fig. 2 The ApEns of logistic map with different parameters

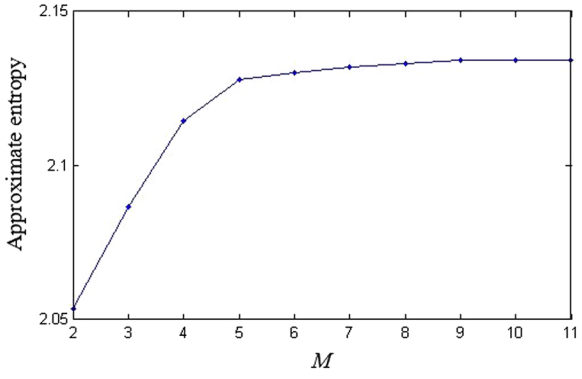

Fig. 3 The ApEns of logistic map with different M

a_1,..., a_9 can be selected as the secret keys, which has greatly improved the key space of logistic map. Then, we have that the distribution of the generated sequences of our logistic map with varying parameter is uniform. We take $x_0 = 0.1$, $u_0 = 0.2$ and $a_k = 3.9 + 0.01{*}k$, $k = 1, 2,..., 9$ as an example, the distribution of the generated sequence is shown in Fig. 4. Furthermore, we would show that our chaotic map can resist the phase space reconstruction. There are two key parameters in the phase space reconstruction, delay time and embedding dimension. By using auto-correlation function and false neighbor method, we have the optimal delay time be 1 and the embedding dimension be 3. We use use these two parameters to reconstruct the phase space in Fig. 5. From Fig. 5 we have that the reconstructed phase space has a significant structure of logistic map, while for the logistic map with varying parameter, the reconstructed phase space is disordered with no significant structure. Thus, the logistic map with varying parameter can resist the phase space reconstruction. Moreover, for other delay time and embedding dimension, the phase space is still disordered with no significant structure, which we do not repeat it here. Finally, we discuss the stable and unstable manifolds proposed in (Ragulskis and Navickas 2011) of our logistic map with varying parameter. For the logistic map, (Ragulskis and Navickas 2011) shows that the misplacement of the

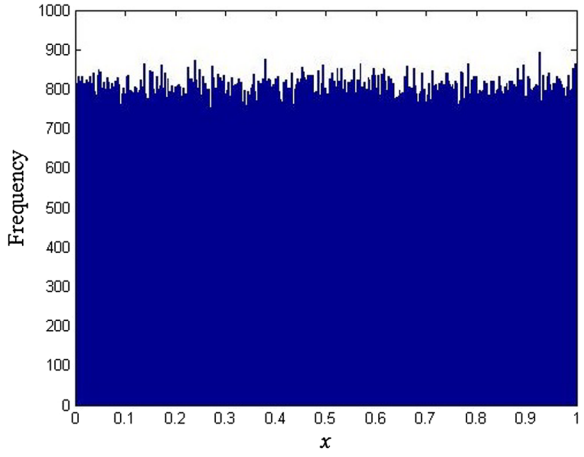

Fig. 4 The distribution of the generated sequence

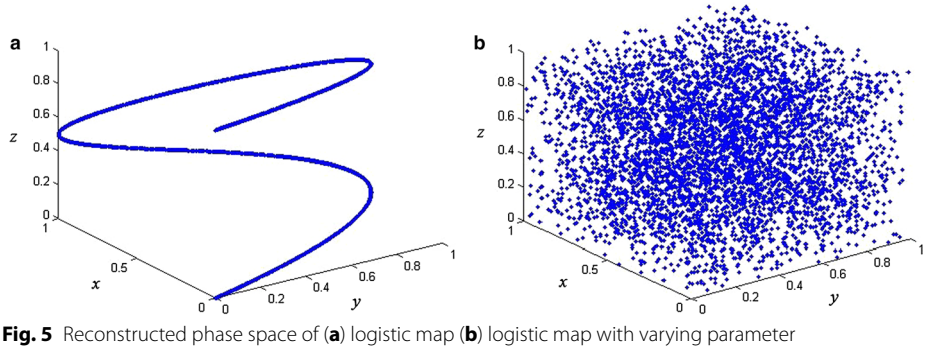

Fig. 5 Reconstructed phase space of (**a**) logistic map (**b**) logistic map with varying parameter

initial condition could potentially lead to the non-asymptotic convergence to a finite length periodic orbit, which makes the logistic sequence weak to be used in encryption. As (Ragulskis and Navickas 2011) shown, the initial conditions leading to the period solution in different forward iterations with different parameters are all different. Thus, our logistic map with varying parameter can naturally overcome such weakness. If the value of x_i falls into the set which will lead to a period solution after several iterations with fixed parameter a, the generated sequence will jump out from the period solution because of the varying of parameter a, as well as the initial conditions leading to the period solution with different parameters are different.

Now we can introduce the shuffling algorithm. Let the size of the gray image g is $p \times q$, and $g(x, y)$ is the value of pixel at the xth row and yth column of the plain image. Reshape the plain image into one-dimensional array $g(i)$, $i = 1, 2, \ldots, p \times q$. By using the binary sequence $\{b_i\}$, we can shuffle the image.

Set L, R, Z be three empty arrays. Begin with $i = 1$, add 1 every time, and end with $i = p \times q$. If $s_i = 1$, $g(i)$ is put into array L in sequence. If $b_i = 0$, $g(i)$ is put into array R in sequence. Merge L and R into the array Z. If round T is odd, put L in front of R, else, put R in front of L. Finally, change the array Z into two-dimensional matrix G with $p \times q$. Then the image G is the shuffled image. This method is first proposed in (Wang and Guo 2014).

Dynamical encryption algorithm

We use the following dynamical algorithm to encrypt the shuffled image G. The steps are

(1) *Initialization:* Denote the initial code book as follow.

$$B_0 = \begin{pmatrix} 1 & 2 & \cdots & 2^N \\ b_1(0) & b_2(0) & \cdots & b_{2^N}(0) \end{pmatrix} \tag{8}$$

here, $B_0(i) = b_i(0)$, and $\{b_i(0)\}$ is an arbitrary permutation from 1 to 2^N.

(2) *Code transformation:* Consider the array $Z(i)$, change $Z(i)$ into binary representation, $Z(i) = (Z_{i1}Z_{i2}\ldots Zi_N)_2$. Denote $q_i = 2^\alpha$ ($\alpha = Z_{i1}Z_{i2}Z_{i3}$), and $w_i = 8^*\beta$ ($\beta = Zi_4Zi_5\ldots Zi_N$). Use the following two algorithms $R(\cdot)$ and $C(\cdot)$ to transform the code book.

$$R(q) = \begin{pmatrix} 1 & 2 & \cdots & M \\ k_1 & k_2 & \cdots & k_M \end{pmatrix}, k_d = \begin{cases} d, & d \in [1, q] \\ d + q - M/2, & d \in [M/2 + 1, M/2 + q] \\ q + d, & d \in [q + 1, M/2] \cup [M/2 + 1 + q, M] \end{cases} \tag{9}$$

$$C(w) = \begin{pmatrix} 1 & 2 & \cdots & M \\ k_1 & k_2 & \cdots & k_M \end{pmatrix}, k_d = \begin{cases} M - 1 - w + d, & d \in [1, w + 1,] \\ d - w - 1, & d \in [w + 2, M] \end{cases} \tag{10}$$

Then $B_{i+1} = B_i(C(w)R(q))^{-1}$.

(3) *Search the code book:* For any driven element $Z(i)$, we have $k(i) = b_{Z(i)}(i)$;

(4) *Stop command:* If $i \neq$ NULL, then $i = i + 1$, back to step 2); Otherwise, stop the algorithm.

Figure 6 shows the main frame of our dynamic algorithm.

The shuffled array $\{Z(i)\}$ is used as the driven sequence. Change the array $\{k(i)\}$ into two-dimensional matrix G' by sequential scanning. The image G' is the ciphered image. In this encryption algorithm, the initial values x_0 and u_0, different parameters a_1,..., a_9, and the initial code book can be selected as the secret keys. Both shuffling and dynamical encryption algorithm are reversible, thus, the decryption algorithm is just the inverse process of the encryption algorithm with using the same secret keys.

Experimental analysis

In our experiments, we select the gray-scale image "Lena.bmp" sized 256 × 256 as the plain image. Choose key parameters $a_k = \{3.991, 3.992, 3.993, 3.994, 3.995, 3.996, 3.997, 3.998, 3.999\}$, $T = 1$, and the initial code book as

$$B_0 = \begin{pmatrix} 1 & 2 & \cdots & 2^N \\ 1 & 2 & \cdots & 2^N \end{pmatrix}.$$

Figure 7 shows the encryption effect of each step in the proposed method. Furthermore, we use several security tests to show the good performances of our algorithm.

Histogram of the image

The distribution of the ciphered image is a major concern. Here, we use the histogram to show the distribution of the plain image and the cipher image. From Fig. 8 we know

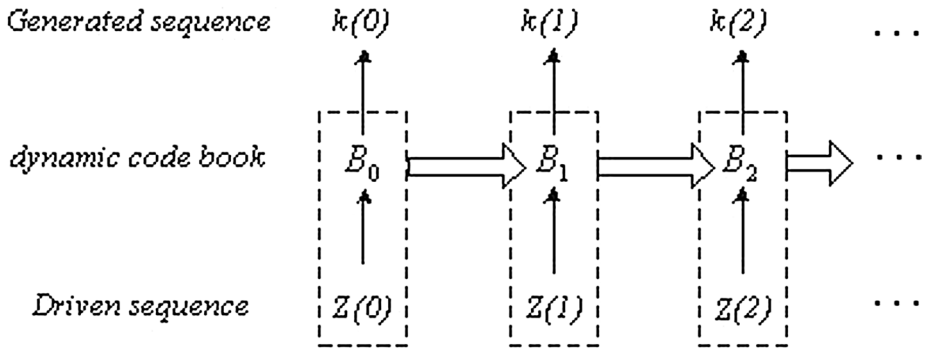

Fig. 6 The main frame of our dynamic algorithm

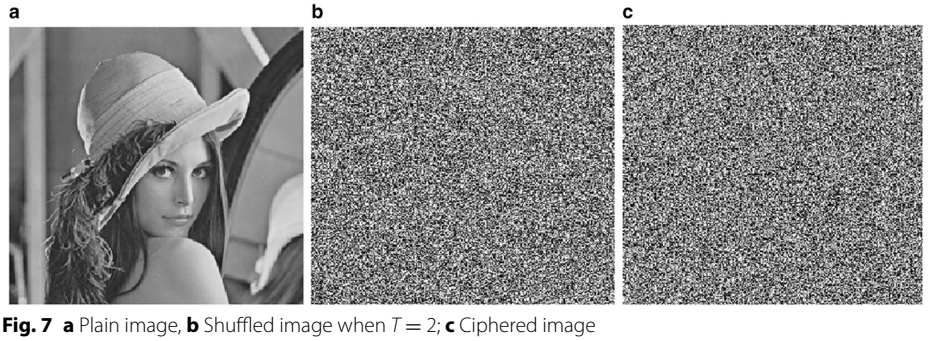

Fig. 7 **a** Plain image, **b** Shuffled image when $T = 2$; **c** Ciphered image

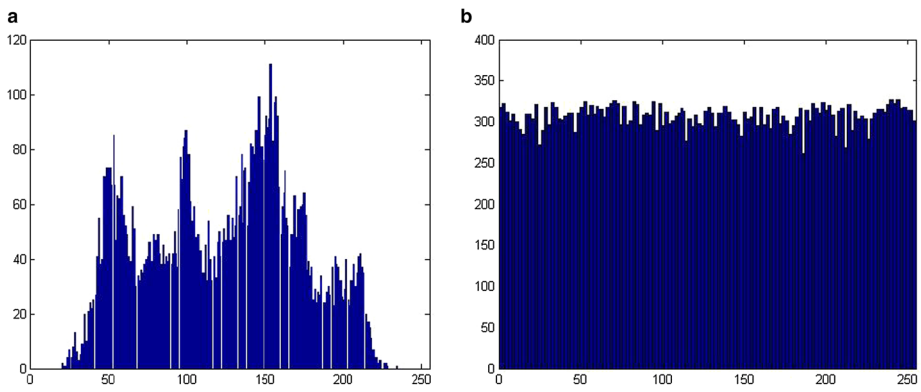

Fig. 8 Histogram of the images **a** Plain image, **b** Ciphered image

that the proposed scheme results in very flat distributions of ciphered images, which can resist cipher-only attack.

Information entropy analysis

Information entropy is the most significant measure to disorder, or unpredictability. The information entropy can be calculated as

$$H(m) = -\sum_{i=1}^{M} p(m_i) \log_2 p(m_i)$$

here, M is the total number if symbols, and $p(m_i)$ is the probability of symbol m_i. For a random image with 256 gray levels, $M = 256$, the entropy should ideally be 8.

The entropies of plain image and ciphered image are calculated. The results are shown in Table 1. From Table 1 we know that the entropies of the ciphered image produced by our algorithm are very close to the value of 8, which means that the ciphered images are close to a random source, and performs better than the algorithms in Wang and Guo (2014), Zhou and Liao (2012) and Sun et al. (2010).

Sensitivity analysis

In order to resist differential analysis, the cipher text should be sensitive to both plain text and secret key.

Table 1 Information entropy of the ciphered images

Different algorithms	$H(m)$
Our algorithm with $T = 1$	7.9995
Our algorithm with $T = 2$	7.9994
Our algorithm with $T = 3$	7.9995
Ref (Wang and Guo 2014)	7.9977
Ref. (Zhou and Liao 2012)	7.9966
Ref. (Sun et al. 2010)	7.9965

Plaintext sensitivity

The Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are commonly used to evaluate the sensitivity to plain text. For two images $x = \{x_1, x_2, \ldots, x_n\}$ and $y = \{y_1, y_2, \ldots, y_n\}$, the NPCR and UACI are defined as follows

$$NPCR = \frac{1}{n}\sum_{i=1}^{n} D(x_i, y_i)$$

$$UACI = \frac{1}{n}\sum_{i=1}^{n} \frac{|x_i - y_i|}{255}$$

here, $D(x_i, y_i) = 0$ if $x_i = y_i$ and $D(x_i, y_i) = 1$ if $x_i \neq y_i$. For the gray image, the ideal value of NPCR and UACI are 0.9961 and 0.3346, respectively.

We randomly change only 1 bit in the original plain image, and use the same secret key to encrypt the modified image and the original image. Then we calculate their NPCR and UACI values. The results are shown in Table 2.

From Table 2 we find that both the NPCR and UACI value are close to the ideal value when shuffling round $T > 1$. This means that the proposed scheme can effectively resist the differential attack and chosen-plaintext attack.

Key sensitivity

We test the sensitivity to secret key using one of the keys that is a little different from the original one. As we shown, the initial values x_0 and u_0, different parameters a_1,..., a_9, and the initial code book can be used as the secret key. We decrypt the encrypted image with x_0 be different with 10^{-14}, the decrypted image is shown in Fig. 9a. The decrypted image

Table 2 NPCR and UACI when *T* takes different values

Round *T*	NPCR	UACI
1	0.9949	0.3156
2	0.9971	0.3398
3	0.9963	0.3371

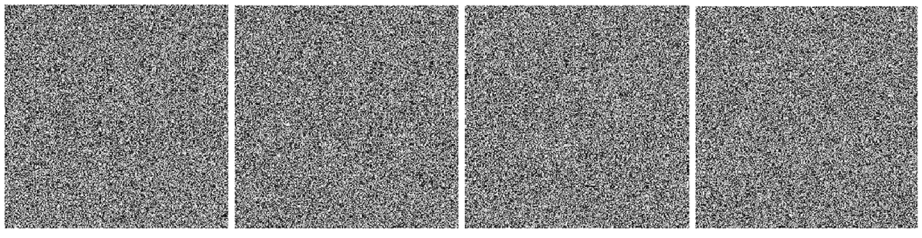

Fig. 9 Key sensitivity analysis. **a** decrypted image with x_0 be different with 10^{-14} **b** decrypted image with u_0 be different with 10^{-14} **c** decrypted image with a_1 be different with 10^{-14} **d** decrypted image by randomly exchanging two codes in the initial code book

with u_0 and a_1 be different with 10^{-14} is shown in Fig. 9b, c, respectively. Furthermore, randomly exchange two codes in the initial code book, the decrypted image is shown in Fig. 9d. From Fig. 9 we can see that all the decrypted images can not be recognized, which indicates that the secret keys are highly sensitive.

Key space

The key space should be large enough to withstand attacks. In our proposed encryption algorithm, the initial values x_0, u_0, the varied parameters a_k and the initial code book can be selected as secret keys. Let the largest precision be 10^{-14}, the key space is about

$$10^{14} \cdot 10^{14} \cdot (0.4 \cdot 10^{14})^9 \cdot 256! \approx 2^{2183}$$

On the other hand, the experimental results show that our scheme is highly sensitive to the secret key. Therefore, The key space of our algorithm is much larger than 2^{128}, and is also larger than 2^{160} of (Wang and Guo 2014) and 2^{140} of (Tong et al. 2015), under the same precision, which concludes that our algorithm can sufficiently resist all kinds of brute-force attacks.

Correlation analysis

A good image encryption algorithm should remove this strong correlation between adjacent pixels. The correlation property can be quantified by means of correlation coefficients as

$$r = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)D(y)}}$$

where

$$\mathrm{cov}(x, y) = \frac{1}{n}\sum_{i=1}^{n}[x_i - E(x)][y_i - E(y)]$$

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

$$E(x) = \frac{1}{n}\sum_{i=1}^{n}x_i$$

x_i and y_i are two adjacent pixels, n is the total number of adjacent pixel pairs (x_i, y_i). Table 3 gives the correlation coefficients of plain image and encrypted image. It is clear that all the correlation coefficients of encrypted images are close to zero, which means that our proposed algorithm can effectively remove the correlations among the adjacent pixels of the plain image, and can resist statistical attacks. Also, our algorithm performs better than the algorithms in Wang and Guo (2014), Hua et al. (2015) and Tong et al. (2015) in this sense.

Table 3 Correlation coefficients of the plain and ciphered images

Images	Horizontal	Vertical	Diagonal
Plain image	0.98496	0.97179	0.96853
Encrypt with $T = 1$	0.0088	0.0083	0.0121
Encrypt with $T = 2$	0.0053	0.0040	0.0062
Encrypt with $T = 3$	0.0021	0.0046	0.0033
Ref. (Wang and Guo 2014)	0.0063	0.0063	0.0069
Ref. (Hua et al. 2015)	0.0024	−0.0086	0.0402
Ref. (Tong et al. 2015)	0.0038	0.0058	0.0133

Table 4 Encryption speed of each scheme

Different algorithms	Encryption time (s)
Our algorithm with $T = 1$	0.05944
Our algorithm with $T = 2$	0.06569
DES	0.59784
AES	0.11297

Computational complexity

Here, we compare the computational complexity of our algorithm with the traditional DES and AES algorithms. All the algorithms are experiment by Matlab R2014a on the computer with 3.6 GHz CPU and 8 GB memory. The test results are shown in Table 4. From Table 4 we can see that the time of our algorithm with $T = 1$ and 2 are both less than the DES and AES algorithms, and is quite acceptable for image encryption. Certainly, the larger the T is, the more the time needed, and more secure the algorithm is. Therefore, users can choose a suitable T for their different security demand.

Conclusions

In this paper, we propose a new image encryption algorithm based on parameter-varied chaotic map and dynamical algorithm. The varied parameters are controlled by zero-mean logistic map and hopping in the given parameter set. We show that the proposed logistic map can overcome the common weaknesses of and is capable to resist phase space reconstruction. We carry out many experiments, including Histogram analysis, information entropy analysis, sensitivity analysis, key space analysis, correlation analysis and computational complexity, to show the security and performance of the proposed image encryption scheme. The experimental results show that our algorithm is with high security, and can be competitive with some other proposed image encryption algorithms.

Authors' contributions
Lingfeng Liu propose this idea and write this paper, Suoxia Miao do the numerical experiments. Both authors read and approval the final manuscript.

Author details
[1] School of software, Nanchang University, Nanchang 330031, People's Republic of China. [2] Faculty of Science, Nanchang Institute of Technology, Nanchang 330029, People's Republic of China.

Competing interests
The authors declare that they have no competing interests.

Received: 20 September 2015 Accepted: 1 March 2016
Published online: 08 March 2016

References

Chen CS, Wang T, Kou YZ, Chen XC, Li X (2013) Improvement of trace-driven I-Cache timing attack on the RSA algorithm. J Syst Softw 86:100–107
Coppersmith D (1994) The data encryption standard (DES) and its strength against attacks. IBM J Res Dev 38:243–250
Gonzalez EI, Hernandez CC (2013) Double hyperchaotic encryption for security in biometric systems. Nonlinear Dyn Syst Theory 13:55–68
Han YJ, Li TF, Yang XQ (2015) Short-term wind power prediction based on logistic mapping neural network of phase space reconstruction. Exp Technol Manag 32:40–45 **(in Chinese)**
Hu HP, Liu SH, Wang ZX, Wu XG (2004) A chaotic poly phase pseudorandom sequence. Math Phys 24:251–256 **(in Chinese)**
Hua ZY, Zhou YC, Pun CM, Philip Chen CL (2015) 2D Sine logistic modulation map for image encryption. Inf Sci 297:80–94
Huang XL (2012) Image encryption algorithm using chaotic chebyshev generator. Nonlinear Dyn 67:2411–2417
Hussain I, Shah T (2013) Application of S-box and chaotic map for image encryption. Math Comput Model 57:2576–2579
Kanso A, Smaoui N (2009) Logistic chaotic maps for binary numbers generations. Chaos Solitons Fractals 40:2557–2568
Lasota A, Mackey MC (1994) Chaos, fractals, and noise. Springer, New York
Liu HJ, Wang XY (2010) Color image encryption based on one-time keys and robust chaotic maps. Comput Math Appl 59:3320–3327
May RM (1976) Simple mathematical models with very complicated dynamics. Nature 261:459–467
Murillo-Escobar MA, Hernandez CC, Perz FA, Gutierrez RML, Acosta Del Campo OR (2015) A RGB image encryption algorithm based on total plain image characteristics and chaos. Signal Process 109:119–131
Pareek NK, Patidar V, Sud KK (2005) Cryptography using multiple one-dimensional chaotic maps. Commun Nonlinear Sci Numer Simul 10:715–723
Patidar V, Pareek NK, Purohit G, Sud KK (2010) Modified substitution-diffusion image cipher using chaotic standard and logistic maps. Commun Nonlinear Sci Numer Simul 15:2755–2765
Ragulskis M, Navickas Z (2011) The rank of a sequence as an indicator of chaos in discret nonlinear dynamical systems. Commun Nonlinear Sci Numer Simul 16:2894–2906
Short KM (1994) Steps toward unmasking secure communications. Int J Bifurc Chaos 4:959–977
Sun F, Lu Z, Liu S (2010) A new cryptosystem based on spatial chaotic system. Opt Commun 283:2066–2073
Tong XG, Wang Z, Zhang M, Liu Y, Xu H, Ma J (2015) An image encryption algorithm based on the perturbed high-dimensional chaotic map. Nonlinear Dyn 80:1493–1508
Wang XY, Guo K (2014) A new image alternate encryption algorithm based on chaotic map. Nonlinear Dyn 76:1943–1950
Wang XY, Luan DP (2013) A novel image encryption algorithm using chaos and reversible cellular automata. Commun Nonlinear Sci Numer Simul 18:3075–3085
Wang Y, Wong KK, Liao XF, Xiang T, Chen GR (2009) A chaos-based image encryption algorithm with variable control parameters. Chaos Solitons Fractals 41:1773–1783
Wang X, Teng L, Qin X (2012a) A novel color image encryption algorithm based on chaos. Signal Process 93:1101–1108
Wang XY, Teng L, Qin X (2012b) A novel colour image encryption algorithm based on chaos. Signal Process 92:1101–1108
Wong KW, Ho SW, Yung CK (2003) A chaotic cryptography scheme for generating short ciphertext. Phys Lett A 310:67–73
Xiao F, Gao XP (2006) An approach for short-term prediction on time series from parameter-varying systems. J Softw 17:1042–1050
Ye G, Wong KW (2013) An image encryption scheme based on time-delay and hyperchaotic system. Nonlinear Dyn 71:259–267
Zhang G, Liu Q (2011) A novel image encryption method based on total shuffling scheme. Opt Commun 284:2775–2780
Zhang XP, Zhao ZM (2014) Chaos-based image encryption with total shuffling and bidirectional diffusion. Nonlinear Dyn 75:319–330
Zhou Q, Liao X (2012) Collision-based flexible image encryption algorithm. J Syst Softw 85:400–407