SCIENTIFIC REPORTS

OPEN

Novel Image Encryption based on Quantum Walks

SUBJECT AREAS:
COMPUTER SCIENCE
INFORMATION TECHNOLOGY

Received
13 June 2014

Accepted
15 December 2014

Published
14 January 2015

Yu-Guang Yang[1,2], Qing-Xiang Pan[1], Si-Jia Sun[1] & Peng Xu[1]

[1]College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China, [2]State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093).

Correspondence and requests for materials should be addressed to Y.Y. (yangyang7357@bjut.edu.cn)

Quantum computation has achieved a tremendous success during the last decades. In this paper, we investigate the potential application of a famous quantum computation model, i.e., quantum walks (QW) in image encryption. It is found that QW can serve as an excellent key generator thanks to its inherent nonlinear chaotic dynamic behavior. Furthermore, we construct a novel QW-based image encryption algorithm. Simulations and performance comparisons show that the proposal is secure enough for image encryption and outperforms prior works. It also opens the door towards introducing quantum computation into image encryption and promotes the convergence between quantum computation and image processing.

With the advancements of Internet and multimedia communication, the exchange of multimedia data over the Internet plays an important role in modern society in which images are widely used as a good information carrier. Image content security receives more and more attention. Generally encryption can effectively ensure the secure transmission of images through public channels. Many image encryption algorithms have been proposed in recent years[1–27].

There are mainly two branches of image encryption: image encryption on a quantum computer and image encryption on a classical computer. As for the former, some works have been proposed[4,27]. Although there are some advanced proposals for quantum networks[28], the practical and useful quantum network, even quantum computer cannot be realized in the near future. So in this paper, we focus on image encryption on a classical computer.

Due to the attractive features such as high sensitivity to initial conditions, unpredictability, pseudo-randomness and ergodicity, chaotic maps are employed for image encryption. In 1989, Matthews first proposed a chaos-based encryption algorithm[5]. Since then, a variety of chaos-based image encryption algorithms have been proposed[2,6–13]. Unfortunately, most chaotic systems are unstable due to the periodicity of the chaotic mapping[29]. Image encryption systems based on such maps are prone to attacks[6,7].

Another important system, optical systems have been developed extensively for image encryption due to the distinct properties of processing 2D complex data with parallelism and high speed. Optics-based image encryption started from the double random-phase encoding (DRPE) algorithm[14]. Unfortunately, the DRPE method was broken by various attack strategies[15,16,17]. Nowadays, most optical image encryption systems are far satisfactory due to some defects like the huge size, poor flexibility and stability for optical elements used in the free space, and the difficulty of implementation. So, it should be used cautiously in practice.

As we know, the security of an image encryption algorithm depends on the design of the details of the algorithm, in particular the design of the key generation rule. A good key generator is of vital importance to a desirable image encryption algorithm. Obviously, the security of chaos-based image encryption algorithms lies heavily in the chaotic systems' features. However, existing chaotic systems are not perfect, i.e., the instability and periodicity cause most chaos-based image encryption algorithms to be prone to various attacks[6,7].

It is natural to ask whether there exist other chaotic systems with more excellent cryptographic performances. Inspired by the above reasons, we are motivated to seek novel chaotic functions and further construct image encryption algorithms based on such chaotic functions.

Quantum computation is a rapidly growing field and lots of breakthroughs have been achieved during the past decades. As a universal quantum computation model, quantum walks (QW) has been developed as a useful tool for solving various problems, including element distinctness[30], triangle finding[31], and data clustering[32] and so on. Furthermore, the importance of classical random walks in many fields like physics, biology, computer science, finance, etc., implies the possibility that its quantum analog, namely, QW, could be a useful tool for many future applications.

In this paper, we investigate the potential application of QW in image encryption and find that QW can serve as an excellent key generator thanks to its inherent unpredictably ’chaotic’ nonlinear dynamic behavior. Further, we construct a novel QW-based image encryption algorithm. Compared with the previous chaos-based image encryption works, our QW-based proposal has not only the same merits as chaos’ systems like high sensitivity to initial values and system parameters, unpredictability, pseudo-randomness, but also the advantages like stability and non-periodicity. The infinite possibilities of the coin states make QW own an ability of producing a theoretically infinite key space to resist brute-force attacks. Numerical simulations show that the proposal is secure enough for image encryption. It also opens the door towards introducing quantum computation into image encryption and promotes the convergence between quantum computation and image processing.

Results

The chaotic behavior of Quantum walks. There are two types of QWs, continuous[33] and discrete ones, and several studies have highlighted how the properties and dynamics of QWs differ from their classical counterparts[34–36]. The basic discrete QW includes two quantum systems: walker and coin. The state of the walker-coin system is denoted by a vector in the Hilbert space $H_t = H_p \otimes H_c$, where the subscripts p and c stand for walker and coin, respectively. The motion of the walk is conditioned by the coin state via a conditional shift operator

$$\hat{S} = \sum_x (|x+1,0\rangle\langle x,0| + |x-1,1\rangle\langle x,1|), \quad (1)$$

where the summation symbol denotes the sum over all possible positions. The evolution of the total quantum system can be implemented by repeating the sequence of the coin flipping operator and the conditional shift operator in equation (1) step by step (so-called discrete time), expressed by

$$\hat{U} = \hat{S}(\hat{I} \otimes \hat{C}), \quad (2)$$

where $\hat{I}$ is the identity operator of the walker and $\hat{C}$ is the flipping operator applied to the coin state. Hence the final state $|\psi\rangle_r$ after r steps is expressed by

$$|\psi\rangle_r = (\hat{U})^r |\psi\rangle_{initial} = \sum_x \sum_v \lambda_{x,v} |x,v\rangle, \quad (3)$$

and the probability of locating the walker at position x after r steps is

$$P(x,r) = \sum_{v \in \{0,1\}} |\langle x,v|(\hat{U})^r|\psi\rangle_{initial}|^2, \quad (4)$$

where $|\psi\rangle_{initial}$ is the initial state of the total quantum system.

For multi-walker, multi-coin discrete QW, the final state $|\psi\rangle_r = \hat{U} |\psi\rangle_0$ after r steps is expressed by

$$|\psi\rangle_r = (\hat{U})^r |\psi\rangle_0 = \sum_{x_1} \sum_{v_1} \sum_{x_2} \sum_{v_2} \cdots \sum_{x_n} \sum_{v_n} \lambda_{x_1 x_2 \cdots x_n, v_1 v_2 \cdots v_n} |x_1 x_2 \cdots x_n, v_1 v_2 \cdots v_n\rangle, \quad (5)$$

and the probability of locating the n walkers at position $x_1,x_2,\ldots,x_n$ after r steps is

$$P(x_1 x_2 \cdots x_n, r) = \sum_{v_1,v_2,\cdots,v_n \in \{0,1\}} |\langle x_1 x_2 \cdots x_n, v_1 v_2 \cdots v_n|(\hat{U})^r|\psi\rangle_0|^2, \quad (6)$$

where $|\psi\rangle_0$ is the initial state of the total n-walker, n-coin quantum system.

It can be seen that the resulting probability distribution in equation (6) is the sum of squares of the norms of amplitudes so that there exists a non-linearity map between the initial state and the resulting probability distribution. The resulting probability distribution is not only of high sensitivity to initial states, unpredictability, pseudo-randomness, but also of stability and non-periodicity. And different coin states will produce different probability distributions. The infinite possibilities of the coin states make QW own an ability of producing a theoretically infinite key space to resist brute-force attacks, which underlies the image encryption.

Image encryption algorithm based on quantum walks. To demonstrate QW’s utility as an excellent key generator, we further construct a novel image encryption algorithm based on the one-dimensional two-particle discrete-time QW on a circle. The algorithm includes three phases: (i) the generation of the key sequences using the one-dimensional two-particle discrete-time QW on a circle, (ii) the image encryption phase, and (iii) the image decryption phase.

Generation of the key sequences using the one-dimensional two-particle discrete-time QW on a circle.

(i) Choose the parameters (n, (α, β, χ, δ)), r, θ), and run the one-dimensional two-particle discrete QW on a circle of n nodes to generate the corresponding probability matrix with size $n \times n$. Here α, β, χ, δ are the amplitudes of the initial coin state $|\upsilon,\tau\rangle = (\alpha|00\rangle + \beta|01\rangle + \chi|10\rangle + \delta|11\rangle)$. r is the step number and θ is a parameter of the quantum coin operator

$$\hat{C} = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \otimes \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \cdot \theta \in \{0, 2\pi\} \quad (7)$$

(ii) Resize the resulting probability matrix in terms of the size of the original image and multiply all values in the resulting probability matrix by 10^8 modulo 256 to form a random key sequence $K = \{k_1,k_2,\ldots,k_{M \times N}\}$, where $M \times N$ is the size of the original image I.

Image encryption procedure.

(i) Convert the original image I into a vector $P = \{p_1,p_2,\ldots,p_{M \times N}\}$, and then calculate the sum of the original image pixels according to equation (8):

$$sum\_pixels = \sum_{i=1}^{M \times N} P_i. \quad (8)$$

(ii) Calculate c_{i} ($i = 1,2,\ldots,M \times N$) by equation (9):

$$c_i = p_i \oplus \bmod(c_{i-1} + k_i, 256) \oplus \bmod\left(floor\left(\frac{sum\_pixels - sum\_pixels(i)}{256^4} \times k_i \times 10^8\right), 256\right), \quad (9)$$

where $c_0 = 127$. And the cipher image is denoted as $C = \{c_1,c_2,\ldots,c_{M \times N}\}$.

(iii) Select M and N values from the beginning and the end of the key sequence K, respectively, and get two sequences $X = \{X_1,X_2,\ldots,X_M\}$ and $Y = \{Y_1,Y_2,\ldots,Y_N\}$, respectively.

(iv) Order X and Y in an ascending order, respectively, and get two new sequences $I_X = \{I_{X_1}, I_{X_2}, \cdots, I_{X_M}\}$ and $I_Y = \{I_{Y_1}, I_{Y_2}, \cdots, I_{Y_N}\}$.

(v) Permute the cipher image C in terms of I_X and I_Y, respectively, and get the final encrypted image $C^{'}$, i.e.,

$$T_i = C_{I_X},\ i = 1,2,\ldots,M,$$

$$C_i^{'} = T_{I_Y},\ i = 1,2,\ldots,N. \quad (10)$$

Image decryption procedure. The decryption process is the reverse of the encryption one.

(i) Use the same way above to generate I_X and I_Y, and decrypt the cipher image C' into the cipher image C by using I_X and I_Y.

(ii) Generate the random key sequence $K = \{k_1,k_2,\ldots,k_{M\times N}\}$ with the same parameters (n, (α, β, χ, δ), r, θ).

(iii) Recover the image pixels $P = \{p_1,p_2,\ldots p_{M\times N}\}$from $C = \{c_1,c_2,\ldots,c_{M\times N}\}$ by equations (11) and (12):

$$sum\_pixels = sum\_pixels + p_i, \tag{11}$$

$$p_i = c_i \oplus \bmod\,(c_{i-1}+k_i,256) \oplus \bmod \left(floor\left(\frac{sum\_pixels}{256^4}\times k_i\times 10^8\right),256\right), \tag{12}$$

where i is from $M\times N$ to 1 and the initial value of *sum_pixels* is 0.

(iv) Reshape $P = \{p_1,p_2,\ldots,p_{M\times N}\}$ into an image with size $M\times N$, and get the recovered image.

Experimental simulations and performance analyses. *Simulations*. Experiments are performed on a laptop with Intel(R) Core(TM) i3-2370M CPU 2.40 GHz 4 GB RAM running on Windows 7 professional equipped with the MATLAB R2012a environment. Here, we selected ten 256 × 256 gray-scale images taken by Q.-X. Pan as the original images (see Supplementary Figs. S1–S10 online). And we chose the initial key parameters ($n = 5$, ($\alpha = 1/2$, $\beta = 1/2$, $\chi = 1/2$, $\delta = 1/2$), $r = 30$, $\theta = \pi/3$). Using QW as the key generator and the proposed image encryption algorithm, we obtained the cipher images of the ten test images.

From Supplementary Figs. S1–S10 online, we showed that the encrypted image is smoother and more uniform than the original image. Hence, it does not provide any hint for attackers by applying statistical attacks on the proposed image encryption scheme.

Security analyses of the QW-based image encryption algorithm. To analyze the security of the proposed image encryption algorithm, we did from two aspects. On the one hand, we analyzed the statistical properties of the QW-based key generator as a pseudorandom number generator (PRNG). On the other hand, we analyzed the statistical properties of cipher images. To analyze the QW-based PRNG, two main quantifiers are adopted, i.e., (i) quantifiers based on information theory[37–39], (ii) quantifiers based on recurrence plots[40,41].

Statistical complexity measure. Complexity is a measure of off-equilibrium ‘order’. Statistical complexity measures (SCM) were proposed as quantifiers of the degree of physical structure in a signal[37,42,43]. They are null for total random processes. The intensive SCM ($C_J[P]$) quantifies not only randomness but also the presence of correlational structures[43,44] of the dynamical system and can be used to study the intricate structures hidden in the dynamics. The SCM $C_J[P]$ is defined as[44]:

$$C_J[P] = Q_J[P,P_e]\cdot H_S[P], \tag{13}$$

where the normalized entropic measure $H_S[P] = S[P]/S_{\max}$ is associated with the probability distribution P,with $S_{\max} = S[P_e]$ ($0 \leq H_S \leq 1$) for the equilibrium distribution P_e and $S[\cdot]$ is the Shannon entropy. The disequilibrium Q_J is defined in terms of the Jensen-Shannon divergence[38,44] by

$$Q_J[P,P_e] = Q_0\{S[(P+P_e)/2] - S[P]/2 - S[P_e]/2\}, \tag{14}$$

with Q_0 being the normalization constant ($0 \leq Q_J \leq 1$). Thus, the disequilibrium Q_J is an intensive quantity. Following the methodology proposed by Bandt and Pompe[45], the normalized entropy H_S and the intensive SCM C_J as functions of the number of 8 bits and 16 bits-words are shown in Figs. 1(a) and 1(b) respectively. From Fig. 1, when the number of words of the analyzed sequence increases, the statistical complexity and the normalized Shannon entropy tend to 0 and 1 respectively. It can be concluded that, the randomness of the proposed QW-based PRNG is successfully verified.

Recurrence plots. Recurrence is a fundamental property of dynamical systems, which can be exploited to characterize the system's behavior in phase space. In 1987, Eckmann et al. introduced a powerful tool for visualization and analysis of recurrences called recurrence plot (*RP*)[40]. To visualize the recurrences of states of a dynamical system, the *RP* of a trajectory $\underset{i}{\vec{x}} \in \Re^d$ can be formally expressed by the matrix

$$R_{i,j}(\varepsilon) = \Theta\left(\varepsilon - \left\|\vec{x}_i - \vec{x}_j\right\|\right),\ i,j = 1,\cdots,N, \tag{15}$$

where N is the number of measured points $\vec{x}_i$, ε is a threshold distance, $\Theta(\cdot)$ is the Heaviside function (i.e. $\Theta(x) = 0$, if $x < 0$, and $\Theta(x) = 1$ otherwise) and $\|\cdot\|$ is a norm.

*RP*s with different r exhibit visually the recurrences of the QW-based PRNG with an embedding dimension $m = 4$ and the delay $\tau = 1$ (see Supplementary Fig. S11 online). It is shown that the QW-based PRNG causes a rather homogeneous *RP* with numerous single points and some short, diagonal or vertical lines.

Because the visual impact produced by the *RP* is insufficient to demonstrate the quality of the QW-based PRNG because of the 'small-scale' structures[41], several measures of complexity which quantify the small scale structures in *RP*s, have been proposed[46–48] and are known as recurrence quantification analysis (*RQA*). In this paper, these measures based on the recurrence point density and the diagonal and vertical line structures are considered.

Measures based on the recurrence density. The simplest measure of the *RQA* is the recurrence rate (*RR*)

$$RR(\varepsilon) = \frac{1}{N^2}\sum_{i,j=1}^{N} R_{i,j}(\varepsilon), \tag{16}$$

which is a measure of the density of recurrence points in the *RP*. In the limit $N \to \infty$, *RR* is the probability that a state recurs to its ε-neighbourhood in phase space. For PRNGs, the ideal value would be $RR = 0$. It is indicated that the values of the *RR* range from 0.004 to 0.007 for different r, which exhibits the good randomness of the QW-based PRNG (see Supplementary Fig. S12 online).

Measures based on diagonal lines. The measures are related to the histogram $P(\varepsilon,l)$ of the diagonal line lengths l, given by

$$P(\varepsilon,l) = \sum_{i,j=1}^{N}(1-R_{i-1,j-1}(\varepsilon))(1-R_{i+l,j+l}(\varepsilon))\prod_{k=0}^{l-1}R_{i+k,j+k}(\varepsilon). \tag{17}$$

Supplementary Fig. S13 online demonstrates the histogram of the diagonal line lengths of the *RP* in Supplementary Fig. S11 online with $r = 50$. It is shown that the diagonal line lengths are mainly very short exhibiting the good randomness.

Processes with uncorrelated or weakly correlated and stochastic or chaotic behaviors cause none or very short diagonals, whereas deterministic processes cause longer diagonals and less single, isolated recurrence points. Therefore, the ratio of recurrence points that form diagonal structures (of at least length $l_{\min}$) to all recurrence points

$$DET = \frac{\sum_{l=l_{\min}}^{N} lP(\varepsilon,l)}{\sum_{l=1}^{N} lP(\varepsilon,l)}, \tag{18}$$

is introduced as a measure for determinism (or predictability) of the system. The threshold $l_{\min}$ excludes the diagonal lines which are formed by the tangential motion of the phase space trajectory.

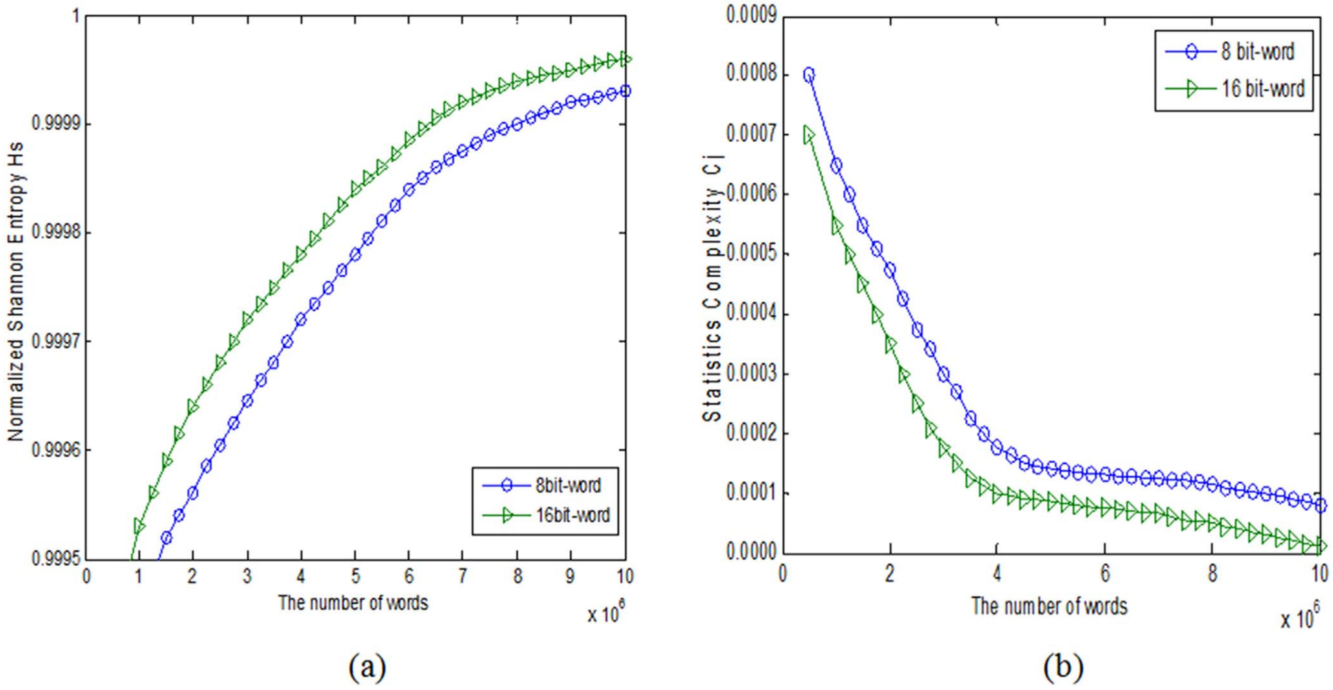

Figure 1 | (a) Normalized Shannon entropy. (b) Intensive statistical complexity measure. The normalized entropy H_S and the intensive statistical complexity measure C_J as functions of the number of 8 bits and 16 bits-words are shown in (a) and (b) respectively. When the number of words of the analyzed sequence increases, the statistical complexity and the normalized Shannon entropy tend to 0 and 1 respectively. (see text in the section entitled Results).

A diagonal line of length l means that a segment of the trajectory is rather close during l time steps to another segment of the trajectory at a different time; thus these lines are related to the divergence of the trajectory segments. The average diagonal line length

$$L = \frac{\sum_{l=l_{\min}}^{N} l P(\varepsilon,l)}{\sum_{l=l_{\min}}^{N} P(\varepsilon,l)}, \qquad (19)$$

is the average time that two segments of the trajectory are close to each other, and can be interpreted as the mean prediction time.

Another *RQA* measure considers the length $L_{\max}$ of the longest diagonal line found in the *RP*,

$$L_{\max} = \max\left(\{l_i\}_{i=1}^{N_l}\right), \qquad (20)$$

where $N_l = \sum_{l=l_{\min}} P(\varepsilon,l)$ is the total number of diagonal lines. These measures are related to the exponential divergence of the phase space trajectory. The faster the trajectory segments diverge, the shorter are the diagonal lines.

The measure entropy refers to the Shannon entropy of the probability $p(l) = P(\varepsilon,l)/N_l$ to find a diagonal line of exactly length l in the *RP*, where $N_l = \sum_{l \geq l_{\min}} P(\varepsilon,l)$ is the total number of diagonal lines.

$$ENTR = -\sum_{l=l_{\min}}^{N} p(l) \ln p(l). \qquad (21)$$

ENTR reflects the complexity of the *RP* in respect of the diagonal lines, e.g. for uncorrelated noise the value of *ENTR* is rather small, indicating its low complexity, as shown in Supplementary Fig. S14 online.

Measures based on vertical lines. The total number of the vertical lines of the length v in the *RP* is then given by the histogram

$$P(v) = \sum_{i,j=1}^{N} (1 - R_{i,j}(\varepsilon))(1 - R_{i,j+v}(\varepsilon)) \prod_{k=0}^{v-1} R_{i,j+k}(\varepsilon). \qquad (22)$$

Supplementary Fig. S15 online shows the histogram of vertical line lengths of the *RP* in Supplementary Fig. S11 online with the parameter $r = 50$. It is shown that the vertical line lengths are mainly very short exhibiting the good randomness.

Analogous to the definition of the determinism in equation (22), the ratio between the recurrence points forming the vertical structures and the entire set of recurrence points can be computed,

$$LAM = \frac{\sum_{v=v_{\min}}^{N} v P(v)}{\sum_{v=1}^{N} v P(v)}. \qquad (23)$$

The computation of *LAM* is realized for those v that exceed a minimal length $v_{\min}$ in order to decrease the influence of the tangential motion. *LAM* will decrease if the *RP* consists of more single recurrence points than vertical structures.

The average length of vertical structures is given by

$$TT = \frac{\sum_{v=v_{\min}}^{N} v P(v)}{\sum_{v=v_{\min}}^{N} P(v)}, \qquad (24)$$

and is called trapping time. *TT* estimates the mean time that the system will abide at a specific state or how long the state will be trapped.

Finally, the maximal length of the vertical lines in the *RP*

$$V_{\max} = \max\left(\{v_l\}_{l=1}^{N_v}\right), \qquad (25)$$

can be defined, analogously to the standard measure $L_{\max}$ (N_v is the absolute number of vertical lines).

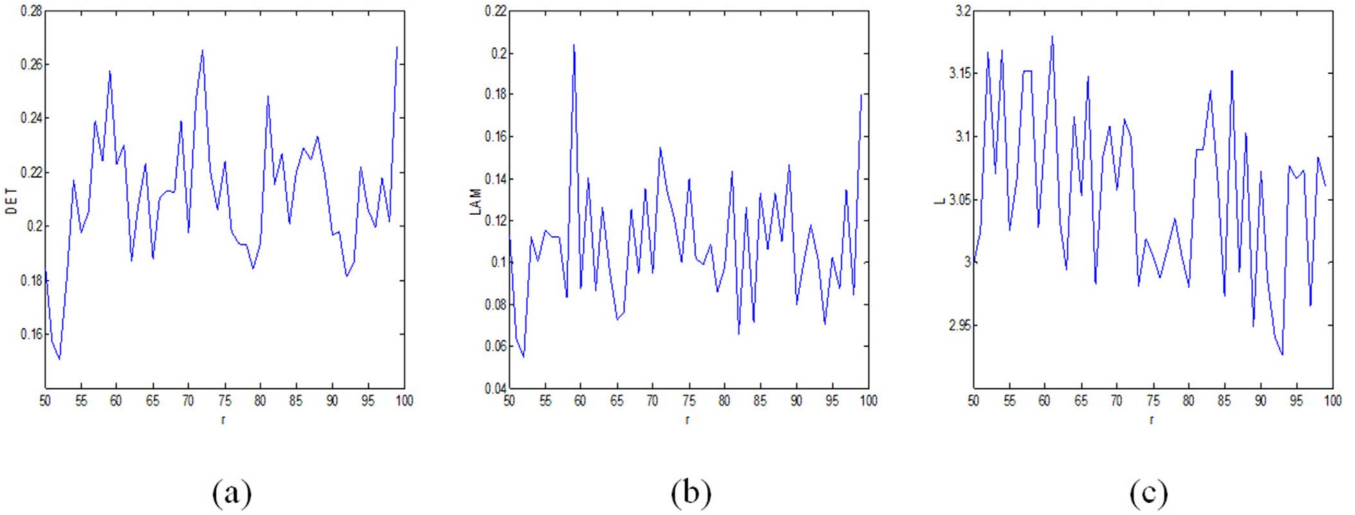

Figure 2 | Selected *RQA* measures: *DET*, $L_{\max}$, and *L*. (a) *DET*, (b) *LAM*, (c) *L*. *DET*, $L_{\max}$, and *L* change with different step number *r* are shown in (a), (b) and (c) respectively. (see text in the section entitled Results).

Figs. 2,3 indicate the *RQA* measures, i.e., *DET*, $L_{\max}$, *L*, *LAM*, $V_{\max}$, and *TT* for different *r* and demonstrate the good statistical properties of the QW-based PRNG.

Degree of non-periodicity. In order to detect and study non-periodicity in the QW-based PRNG, the scale index analysis (SIA) is carried out which is introduced by Benìtez et al.[49]. The SIA method is often used as a framework to enhance the general performance of cryptosystems in designing new chaos-based cryptosystems and PRNGs. For example, recently Akhshani et al. proposed a new scheme for generating good PRNGs based on quantum logistic map[50]. They used the SIA technique to assess the degree of non-periodicity of the chaotic sequences of the quantum map.

The SIA technique is based on the continuous wavelet transform (CWT) and the wavelet multi-resolution analysis[51]. To study non-periodicity of the QW-based PRNG[52], we assumed that the key sequence *f* is compactly supported and is defined over a finite time interval $I=[a,b]$. The CWT of *f* at time *u* and scale *s* is defined as[51]:

$$Wf(u,s):=\langle f,\psi_{u,s}\rangle=\int_{-\infty}^{+\infty}f(t)\psi^{*}_{u,s}(t)dt, \tag{26}$$

and it provides the frequency components (or details) of *f* corresponding to scale *s* and time *t*.

The scalogram of *f* is defined as follows:

$$\zeta(s):=\|Wf(u,s)\|=\left(\int_{-\infty}^{+\infty}|Wf(u,s)|^{2}du\right)^{2}, \tag{27}$$

where $\zeta(s)$ is the energy of the CWT of *f* at scale *s*. The scalogram is a useful tool for studying a signal, since it allows the detection of its most representative scales or frequencies[49,52]. Also, the inner scalogram of *f* at a scale *s* can be defined by:

$$\zeta^{inner}(s):=\|Wf(u,s)\|_{J(s)}=\left(\int_{c(s)}^{d(s)}|Wf(u,s)|^{2}du\right)^{2}, \tag{28}$$

where $J(s)=[c(s),d(s)]\subseteq I$ is the maximal subinterval in *I* for which the support of $\psi_{u,s}$ is included in *I* for all $u\in J(s)$. As the length of *J*(*s*) depends on the scale *s*, the values of the inner scalogram at different scales cannot be compared. Therefore, the inner scalogram should be normalized as follows[49]:

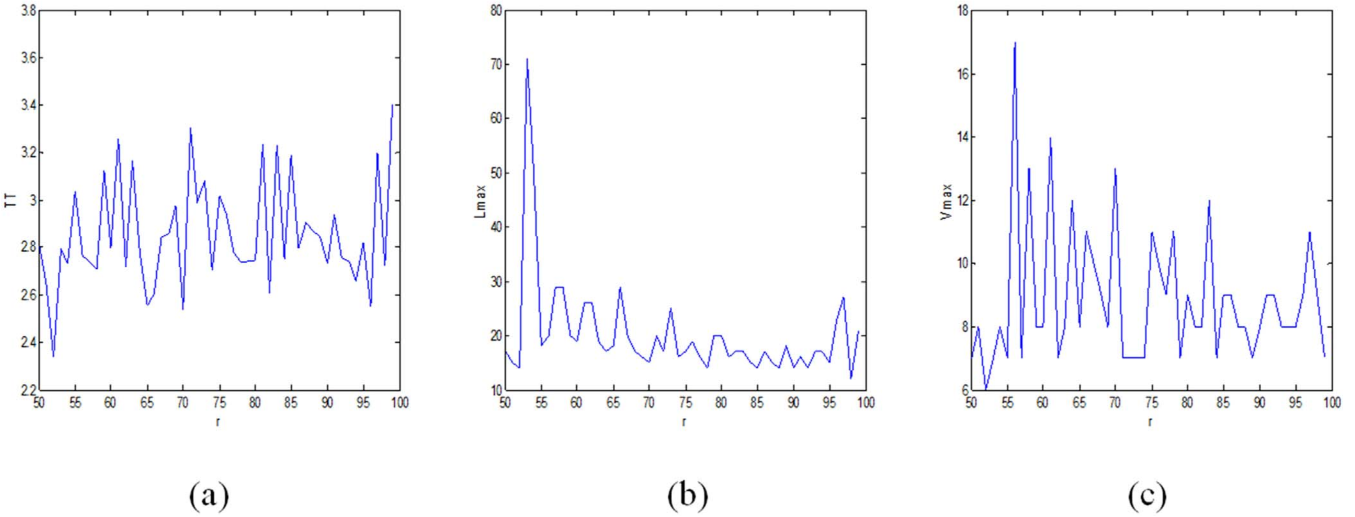

Figure 3 | Selected *RQA* measures: *LAM*, $V_{\max}$, and *TT*. (a) *TT*, (b)$L_{\max}$, (c) $V_{\max}$. *LAM*, $V_{\max}$, and *TT* change with different step number *r* are shown in (a), (b) and (c) respectively. (see text in the section entitled Results).

$$\overset{-inner}{\zeta}(s)=\frac{\zeta^{inner}(s)}{(d(s)-c(s))^{\frac{1}{2}}}. \tag{29}$$

It is shown that the normalized inner scalogram can be a valuable tool for detecting the non-periodicity of the signal, where a signal with details at every scale is non-periodic (see Supplementary Fig. S16 online).

The scale index of f in the scale interval $[s_0,s_1]$ can be defined by:

$$i_{scale}:=\frac{\zeta(s_{\min})}{\zeta(s_{\max})}, \tag{30}$$

where $s_{\max}$ is the smallest scale such that $\zeta(s)\leq\zeta(s_{\max})$ for all $s\in[s_0,s_1]$, and $s_{\min}$ the smallest scale such that $\zeta(s_{\min})\leq\zeta(s)$ for all $s\in[s_{\max},s_1]$. Note that for compactly supported signals only the normalized inner scalogram will be considered[49]. From its definition, the scale index i_{scale} meets $0\leq i_{\mathrm{scale}}\leq 1$ and it can be interpreted as a measure of the degree of non-periodicity of the signal: the scale index will be zero or close to zero for periodic sequences and close to one for highly non-periodic sequences[49]. Fig. 4 shows the SIA of the QW-based key sequence. It can be concluded that the best value of the scale index is $i_{\mathrm{scale}}\approx 0.9$ and remains at this value for all θ. Thus, the key sequence in this state is highly non-periodic and it can be used for any PRNG purposes.

Random tests for the key sequences. We used NIST SP800-22 to test the randomness of the QW-based key sequences (see Supplementary Table S1 online). Each test produces a *P-value* in [0, 1]. If the *P-value* is higher than a preset thresholdα, it means that the cipher image passes the test. In our tests, we set $\alpha = 0.01$. The results of different QW-based key sequences are all 'success' in terms of the average of *P-value* shown in the second column. Hence, our key generator passes the NIST SP800-22 tests.

Information entropy analysis. The information entropy is often used to measure the randomness of the cipher images. The entropy $H(x)$ of a message source m is given by

$$H(X)=-\sum_{i=0}^{L-1}p(x_i)\log_2 p(x_i), \tag{31}$$

where $p(x_i)$ represents the probability of the occurrence of symbol x_i. We compared the information entropy using our proposal and the algorithms using hyper-chaotic system[53,54] (see Supplementary Table S2 online). In terms of the results, the proposed scheme is stable and secure against entropy attack.

Randomness test for the cipher images. We used ten different cipher images with size 1024 × 1024 because of the software NIST requirements for the magnitude 1000000 (see Supplementary Table S3 online). The results of ten different images are all 'success', and we get the average of *P-value* show in the second column. Hence, we can judge that our proposed algorithm passes the NIST SP800-22 tests.

Further, we applied the most stringent test by TestU01[55]. As for tests by TestU01, there are three different types of crush batteries: SmallCrush, Crush and BigCrush. To test the randomness of the cipher images, one should apply SmallCrush, Crush and BigCrush test batteries. For each test, a *P*-value is calculated. If the *P*-value is within the range [0.0001, −0.9999], it implies a success. Or it is considered as a failure. According to Supplementary Table S4 online, the proposed encryption system passes the TestU01 tests.

Speed performance analysis. Speed is an important factor for evaluating the performance of an image encryption algorithm. For the proposed encryption algorithm, we measured the time cost in the running environment: Windows 7, Matlab R2012a, Intel(R) Core(TM) i3-2370M CPU 2.40 GHz 4 GB RAM and the average time cost for cipher images of size 256 × 256 is 0.1371721s or so. Compared with prior image encryption works, our algorithm is not so fast, which should be improved in our future work.

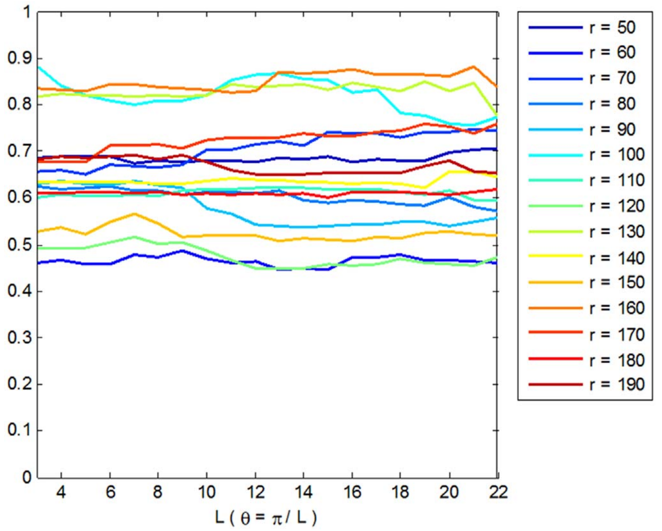

Figure 4 | The scale index of the QW-based key sequence for different *r*. The scale index of the QW-based key sequence change with different step number r and θ, the parameter of the quantum coin operator. Generally, the more the scale index is close to one, the more non-periodic the key sequence is. It can be found that the best value of the scale index is $i_{scale}\approx$ 0.9 and remains at this value for all θ. (see text in the section entitled Results).

Key space analysis. A desirable image encryption scheme should have a sufficiently large key space to resist brute-force attacks. The encryption key of our algorithm can be represented by $(n, (\alpha, \beta, \chi, \delta), r, \theta)$. Although there is an infinite key space theoretically, because of finite precision of digital computers, the key space actually turns out to be finite. Considering that the calculation precision is 10^{-14}, the size of key space for initial conditions and control parameters would be roughly 2^{325}, which is large enough for any encryption purposes and is also large enough to resist all kinds of brute-force attacks.

Comparison with other image encryption techniques. Experimental results of the proposed image encryption scheme will be compared with three classes of image encryption techniques, i.e., the quantum image encryption algorithm[4], the DRPE optical image algorithm[14], the chaos-based image encryption algorithm[56].

Correlation analysis. A desirable image encryption algorithm should produce the cipher image with extremely low correlation between adjacent pixels. We tested the correlation between 10000 pairs of adjacent pixels (in horizontal, vertical and diagonal directions respectively), and drew the correlation distribution of adjacent pixels in the Arch image and its cipher image (see Supplementary Fig. S17 online). It is shown that the cipher image is quite random.

The correlation coefficients r_{xy} of adjacent pixels can be defined by

$$r_{xy}=\frac{E((x-E(x))(y-E(y)))}{\sqrt{D(x)D(y)}}, \tag{32}$$

where $E(x)$ and $D(x)$ are the expectation and variance of variable x, respectively.

The average of the correlation coefficients r_{xy} of adjacent pixels in horizontal, vertical and diagonal directions respectively can be defined as

$$Average(H,V,D)=\frac{H+V+D}{3}, \tag{33}$$

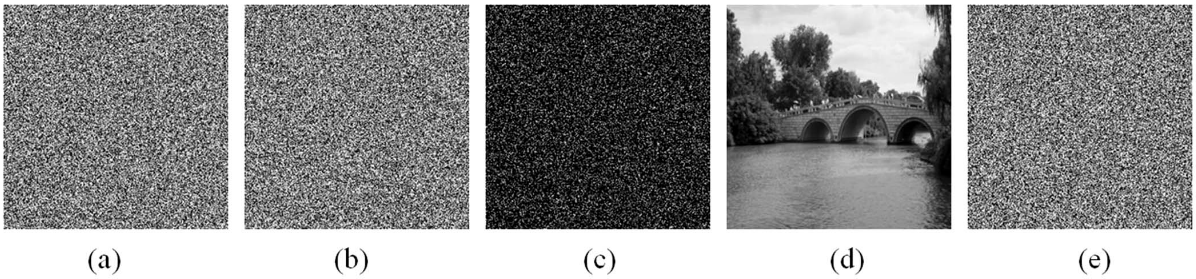

Figure 5 | Key sensitivity tests. (a) Arch image is encrypted with the key ($n = 5$, $(\alpha, \beta, \chi, \delta) = (1/2, 1/2, 1/2, 1/2)$, $r = 100$, $\theta = \pi/3$) to obtain the cipher image in (a); (b) Arch image is encrypted by making a little change with $\theta = \pi/2.99999999$ again to get the cipher image in (b); (c) The differential image between (a) and (b) is drawn in (c); (d) The cipher image of (a) is decrypted with the correct decryption key to obtain the correct original image in (d); (e) The cipher image of (a) is decrypted again with the decryption key with a little change of $\theta = \pi/2.99999999$to obtain the image in (e). (see text in the section entitled Results). We acknowledge Qing-Xiang Pan who took the Arch image in Supplementary Fig. S1(a) online and all figures in Fig. 5 were obtained by simulations using Matlab software by Qing-Xiang Pan.

where H, V, and D are the correlation coefficients of adjacent pixels in horizontal, vertical and diagonal directions respectively.

The comparisons between our algorithm and these three classes of image encryption algorithms are shown in Supplementary Tables S5, S6 and S7 online respectively. It is shown that our algorithm outperforms these three classes of image encryption algorithms in terms of the correlation coefficients, the average and the value of Average (H,V,D) and is secure against statistical attack.

*Sensitivity analysis***.** The difference caused by a little change in the plain image and the key can reflect the relationship between the original image and the cipher image to some extent. In general, two common performance measures are used to test the influence of a little change in the key on the cipher image, i.e., the *number of pixels change rate* (*NPCR*) and the *unified average changing intensity* (*UACI*). *NPCR* is expressed by

$$NPCR = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} D(i,j)}{m \times n} \times 100\%, \qquad (34)$$

where

$$D(i,j) = \begin{cases} 1 & c_1(i,j) \neq c_2(i,j) \\ 0 & otherwise \end{cases}, \qquad (35)$$

and c_1 and c_2 are two cipher images with size $m \times n$.

UACI is defined by

$$UACI = \frac{1}{m \times n}\left[\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(c_1(i,j) - c_2(i,j))}{255}\right] \times 100\%. \qquad (36)$$

In our tests, we considered the influence of slightly different keys and one pixel change on a 256-gray image with size 256 × 256, respectively. Generally two kinds of sensitivity analyses should be made. One is key sensitivity analysis and the other is plaintext sensitivity analysis respectively. Next, we first made a key sensitivity analysis.

We first encrypted Arch image with the key ($n = 5$, $(\alpha, \beta, \chi, \delta) = (1/2, 1/2, 1/2, 1/2)$, $r = 100$, $\theta = \pi/3$) to obtain the cipher image in Fig. 5(a), and then we encrypted Arch image by making a little change with $\theta = \pi/2.99999999$ again and got the cipher image in Fig. 5(b). We drew the differential image between Fig. 5(a) and Fig. 5(b), i.e., Fig. 5(c). By calculation, we got the difference between Figs. 5(a) and 5(b) is 99.6124267578125%, which implies the encryption process is quite sensitive to the encryption key. Moreover, the *NPCR* and *UACI* between cipher images with slightly different keys are calculated in the second and third columns of Supplementary Table S8 online. It can be seen that the average of *NPCR* and *UACI* is 0.9965778100586 and 0.3357151989507, respectively, higher than the one in Ref. 56. It implies that the encryption process is highly sensitive to the encryption key.

To verify the high sensitivity to the decryption key, we first decrypted the cipher image of Fig. 5(a) with the correct decryption key to obtain the correct original image (see Fig. 5(d)), and then we decrypted the cipher image of Fig. 5(a) again with the decryption key with a little change of $\theta = \pi/2.99999999$ to obtain the image in Fig. 5(e). We calculated out the difference between Fig. 5(d) and Fig. 5(e) is 99.5590209960938%. Therefore, the decryption process is also highly sensitive to the decryption key. To sum up, our algorithm can provide a high key sensitivity.

Plaintext sensitivity means that a little change in the plaintext image can cause a large change in the cipher image. Firstly, we encrypted a plaintext image to generate a cipher image. Secondly, we randomly selected a pixel in the same plaintext image to let its pixel value plus one. Thirdly, we encrypted the modified plaintext image by using the same encryption key to generate another encrypted image. Finally, the *NPCR* and *UACI* between the two resulting cipher images with only one pixel difference in their respective original images were calculated in Supplementary Table S8 online respectively. As shown in the fourth and fifth columns, we can see that the average of *NPCR* is over 99.65% and that of *UACI* is over 33.52%, which are higher than the ones in Ref. 56. This also implies that our proposed scheme have a good ability to resist differential attack.

Discussion

In this paper, we investigated the potential application of QW in image encryption. It is found that QW can serve as an excellent key generator thanks to its inherent nonlinear chaotic dynamic behavior. Compared with previous works, our QW-based proposal has the following features:

- It has not only the same merits as chaos' systems like high sensitivity to initial values and system parameters, unpredictability, pseudo-randomness, but also the different advantages like stability and non-periodicity.
- The infinite possibilities of the coin states make the QW own an ability of producing a theoretically infinite key space to resist brute-force attacks.
- It also opens the door towards introducing quantum computation into image encryption and promotes the convergence between quantum computation and image processing.

Although our QW-based algorithm has some advantages over other algorithms, our proposal also has some shortcomings in terms of the encryption speed. That is, the encryption speed of the proposed algorithm is not fast compared to other competitive algorithms. So our future work will focus on the improvement of the proposed algorithm.

Methods

One-dimensional two-particle discrete QW algorithm on a circle of *n* nodes. There is a one-dimensional two-particle discrete QW on a circle of n nodes defined as follows. We choose the quantum coin operators $\hat{C}_1, \hat{C}_2$ and an initial state of the total quantum system

$$|\psi\rangle_0 = |x,y\rangle \otimes |v_1,v_2\rangle. \tag{37}$$

Here

$$|v_1,v_2\rangle = (\alpha|00\rangle + \beta|01\rangle + \chi|10\rangle + \delta|11\rangle), \tag{38}$$

where $|\alpha|^2 + |\beta|^2 + |\chi|^2 + |\delta|^2 = 1$. We define $\hat{U}_1 = \left(I \otimes \hat{S}_1\right)\left(I \otimes \hat{C}_1\right)$ and $\hat{U}_2 = \left(I \otimes \hat{S}_2\right)\left(I \otimes \hat{C}_2\right)$. The difference between a line and a circle is that the circle has only n nodes and is cyclical. The difference of walks on the line and on circles is that the operators $\hat{S}_1$ and $\hat{S}_2$ of two-particle QW on circles becomes

$$\hat{S}_1 = \begin{cases} |2,0\rangle\langle 1,0| + |n,1\rangle\langle 1,1|, & \text{when} \quad x=1; \\ |1,0\rangle\langle n,0| + |n-1,1\rangle\langle n,1|, & \text{when} \quad x=n; \\ |x+1,0\rangle\langle x,0| + |x-1,1\rangle\langle x,1|, & \text{when} \quad x \neq 1,n. \end{cases} \tag{39}$$

Here $\hat{S}_2$ is similar to $\hat{S}_1$.

Here we let

$$\hat{C}_1 = \hat{C}_2 = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}. \ \theta \in \{0, 2\pi\}. \tag{40}$$

The initial value of the QW, i.e., (n, (α, β, χ, δ), r, θ) are tunable parameters. By running the one-dimensional two-particle discrete QW on a circle of n nodes, QW is capable of producing chaotic behavior as the value of (n, (α, β, χ, δ), r, θ) changes.

1. Akhshani, A., Akhavan, A., Lim, S.-C. & Hassan, Z. An image encryption scheme based on quantum logistic map. *Commun. Nonlinear Sci. Numer. Simulat.* **17**, 4653–4661 (2012).
2. Huang, X. L. & Ye, G. D. An efficient self-adaptive model for chaotic image encryption algorithm. *Commun. Nonlinear Sci. Numer. Simulat.* **19**, 4094–4104 (2014).
3. Abd El-Latif Ahmed, A., Li, L., Wang, N., Han, Q. & Niu, X. M. A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. *Signal Process.* **93**, 2986–3000 (2013).
4. Yang, Y.-G., Xia, J., Jia, X. & Zhang, H. Novel image encryption/decryption based on quantum Fourier transform and double phase encoding. *Quantum Inf. Process.* **12**, 3477–3493 (2013).
5. Matthews, R. On the derivation of a 'chaotic' encryption algorithm. *Crypt.* **13**, 29–42 (1989).
6. Li, C., Li, S. & Lo, K. T. Breaking a modified substitution–diffusion image cipher based on chaotic standard and logistic maps. *Commun. Nonlinear Sci. Numer. Simulat.* **16**, 837–843 (2011).
7. Rhouma, R. & Belghith, S. Cryptanalysis of a new image encryption algorithm based on hyper chaos. *Phys. Lett. A* **372**, 5973–5978 (2008).
8. Wong, K. W., Kwok, B. S. H. & Law, W. S. A fast image encryption scheme based on chaotic standard map. *Phys. Lett. A* **372**, 2645–2652 (2008).
9. Patidar, V., Pareek, N. K. & Sud, K. K. A new substitution–diffusion based image cipher using chaotic standard and logistic maps. *Commun. Nonlinear Sci. Numer. Simulat.* **14**, 3056–3075 (2009).
10. Gao, T. & Chen, Z. A new image encryption algorithm based on hyper-chaos. *Phys. Lett. A* **372**, 394–400 (2008).
11. Schack, R. & Caves, C. M. Hypersensitivity to perturbations in the quantum baker's map. *Phys. Rev. Lett.* **71**, 525–528 (1993).
12. Schack, R., D'Ariano, G. M. & Caves, C. M. Hypersensitivity to perturbation in the quantum kicked top. *Phys. Rev. E* **50**,972–987 (1994).
13. Schack, R. & Caves, C. M. Chaos for Liouville probability densities. *Phys. Rev. E* **53**, 3387–3401 (1996).
14. Refregier, P. & Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **20**,767–769 (1995).
15. Qin, W. & Peng, X. Vulnerability to known-plaintext attack of optical encryption schemes based on two fractional Fourier transform order keys and double random phase keys. *J. Opt. A* **11**, 075402 (2009).
16. Carnicer, A., Montes-Usategui, M., Arcos, S. & Juvells, I. Vulnerability to chosen-ciphertext attacks of optical encryption schemes based on double random phase keys. *Opt. Lett.* **30**,1644–1646 (2005).
17. Peng, X., Wei, H. & Zhang, P. Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain. *Opt. Lett.* **31**, 3261–3263 (2006).
18. Guo, Q., Liu, Z. J. & Liu, S. T. Color image encryption by using Arnold and discrete fractional random transforms in IHS space. *Opt. Las. Engineering* **48**, 1174–1181 (2010).
19. Chen, W., Quan, C. & Tay, C. J. Optical color image encryption based on Arnold transform and interference method. *Opt. Commun.* **282**, 3680–3685 (2009).
20. Bourbakis, N. & Alexopoulos, C. Picture data encryption using SCAN pattern. *Pattern Recogn.* **25**, 567–581 (1992).
21. Liu, Z. J., Guo, Q., Xu, L., Ahmad, M. A. & Liu, S. T. Double image encryption by using iterative random binary encoding in gyrator domains. *Opt. Exp.* **18**, 12033–12043 (2010).
22. Chang, C. C., Hwang, M. S. & Chen, T. S. A new encryption algorithm for image cryptosystems. *J. Syst. Soft.* **58**, 83–91 (2001).
23. Chang, H. K. L. & Liu, J. L. A linear quad tree compression scheme for image encryption. *Signal Process.* **10**, 279–290 (1997).
24. Cheng, H. & Li, X. B. Partial encryption of compressed image and videos. *IEEE Trans. Signal Process.* **48**, 2439–2451 (2000).
25. Scharinger, J. Fast encryption of image data using chaotic Kolmogorov flow. *J. Elect. Engineering* **7**, 318–325 (1998).
26. Shen, J. B., Jin, X. G. & Zhou, C. A color image encryption algorithm based on magic cube transformation and modular arithmetic operation. *Adv. Multimedia Inf. Process.* **3768**, 270–280 (2005).
27. Yang, Y.-G., Jia, X., Sun, S. J. & Pan, Q. X. Quantum cryptographic algorithm for color images using quantum Fourier transform and double random-phase encoding. *Inf. Sci.* **277**, 445–457 (2014).
28. Kimble, H. J. The quantum internet. *Nature (London)*, **453**, 1023–1030 (2008).
29. Lou, D. C. & Sung, C. H. A steganographic scheme for secure communications based on the chaos and euler Theorem. IEEE Trans. *Multimedia* **6**, 501–509 (2004).
30. Ambainis, A. Quantum walk algorithm for element distinctness. *SIAM J. Comput.* **37**, 210–239 (2007).
31. Magniez, F., Santhaand, M. & Szegedy, M. Quantum algorithm for the triangle problem. *SIAM J. Comput.* **37**, 413–424 (2007).
32. Li, Q., He, Y. & Jiang, J.-P. A hybrid classical-quantum clustering algorithm based on quantum walks. *Quantum Inf. Process.* **10**,13–26 (2011).
33. Elías V.-Andraca, S. Quantum walks: a comprehensive review. *Quantum Inf. Process.* **11**, 1015–1106 (2012).
34. Kempe, J. Quantum random walks—an introductory overview. *Contemp. Phys.* **44**, 307–327 (2003).
35. Shapira, D., Biham, O., Bracken, A. J. & Hackett, M. One-dimensional quantum walk with unitary noise. *Phys. Rev. A* **68**, 062315 (2003).
36. Blanchard, P. & Hongler, M.-O. Quantum random walks and piecewise deterministic evolutions. *Phys. Rev. Lett.* **92**, 120601 (2004).
37. López-Ruiz, R., Mancini, H. L. & Calbet, X. A statistical measure of complexity. *Phys. Lett. A* **209**, 321–326 (1995).
38. Lamberti, P. W., Martin, M. T., Piastino, A. & Rosso, O. A. Intensive entropy non-triviality measure. *Physica A* **334**, 119–131 (2004).
39. Rosso, O. A., Larrondo, H. A., Martin, M. T., Plastino, A. & Fuentes, M. A. Distinguishing noise from chaos. *Phys. Rev. Lett.* **99**, 154102 (2007).
40. Eckmann, J. P., Oliffson Kamphorst, S. & Ruelle, D. Recurrence plots of dynamical systems. *Europhys. Lett.* **4**, 973–977 (1987).
41. Marwan, N., Romano, M. C., Thiel, M. & Kurths, J. Recurrence plots for the analysis of complex systems. *Phys. Rep.* **438**, 237–329 (2007).
42. Shiner, J. S., Davison, M. & Landsberg, P. T. Simple measure for complexity. *Phys. Rev. E* **59**,1459–1464 (1999).
43. Martin, M. T., Plastino, A. & Rosso, O. A. Statistical complexity and disequilibrium. *Phys. Lett. A* **311**,126–132 (2003).
44. Larrondo, H. A., González, C. M., Martin, M. T., Plastino, A. & Rosso, O. A. Intensive statistical complexity measure of pseudorandom number generators. *Physica A* **356**, 133–138 (2005).
45. Bandt, C. & Pompe, B. Permutation Entropy: A natural complexity measure for time series. *Phys. Rev. Lett.* **88**, 174102 (2002).
46. Marwan, N., Wessel, N., Meyerfeldt, U., Schirdewan, A. & Kurths, J. Recurrence plot based measures of complexity and its application to heart rate variability data. *Phys. Rev. E* **66**, 026702 (2002).
47. Zbilut, J. P. & Webber, C. L. Embeddings and delays as derived from quantification of recurrence plots. *Phys. Lett. A* **171**, 199–203 (1992).
48. Webber, C. L. & Zbilut, J. P. Dynamical assessment of physiological systems and states using recurrence plot strategies. *J. Appl. Physiol.* **76**, 965–973 (1994).
49. Benítez, R., Bolós, V. J. & Ramírez, M. E. A wavelet-based tool for studying non-periodicity. *Comput. Math. Appl.* **60**, 634–641 (2010).
50. Akhshani, A., Akhavan, A., Mobaraki, A., Lim, S.-C. & Hassan, Z. Pseudo random number generator based on quantum chaotic map. *Commun. Nonlinear Sci. Numer. Simulat.* **19**, 101–111 (2014).
51. Mallat, S. A wavelet tour of signal processing. *Academic Press London* (1999).
52. Chandre, C., Wiggins, S. & Uzer, T. Time-frequency analysis of chaotic systems. *Physica D* **181**,171–196 (2003).
53. Zhu, C. X. A novel image encryption scheme based on improved hyper chaotic sequences. *Opt. Commun.* **285**, 29–37 (2012).
54. Ye, G. D. & Zhou, J. W. A block chaotic image encryption scheme based on self-adaptive modelling. *Appl. Soft Comput.* **22**, 351–357 (2014).
55. L'Ecuyer, P. & Simard, R. J. TestU01: A C library for empirical testing of random number generators. *ACM Trans. Math. Soft.* **33**, 22 (2007).

56. Borujeni, S. E. & Eshghi, M. Chaotic image encryption system using phase-magnitude transformation and pixel substitution. *Telecommun. Sys.* **52**, 525–537 (2013).

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant No. 61003290); Beijing Natural Science Foundation (Grant No. 4122008); The Importation and Development of High-Caliber Talents Project of Beijing Municipal Institutions (No.CIT&TCD201304039); National Cipher Development Fund during the 12th Five-Year Plan Period (No.MMJJ201401006); Postgraduate Science and Technology Innovation Foundation of Beijing University of Technology (No.ykj-2014-11167).

Author contributions

Y.Y.G. proposed the theoretical method and wrote the main manuscript text. P.Q.X., S.S.J. and X.P. made the numerical simulations. All authors reviewed the manuscript.

Additional information

Supplementary information accompanies this paper at http://www.nature.com/scientificreports

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Yang, Y.-G., Pan, Q.-X., Sun, S.-J. & Xu, P. Novel Image Encryption based on Quantum Walks. *Sci. Rep.* **5**, 7784; DOI:10.1038/srep07784 (2015).