IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 17, 2019, accepted February 28, 2019, date of publication March 5, 2019, date of current version March 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2902873

A Class of Quadratic Polynomial Chaotic Maps and Its Application in Cryptography

SHUQIN ZHU[1], CONGXU ZHU[2], HUANQING CUI[3], AND WENHONG WANG[1]

[1]School of Computer Science, Liaocheng University, Liaocheng 252059, China
[2]School of Computer Science and Engineering, Central South University, Changsha 410083, China
[3]Shandong Key Laboratory of Wisdom Mine Information Technology, Shandong University of Science and Technology, Qingdao 266590, China

Corresponding author: Congxu Zhu (zhucx@csu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61472451, in part by the Shandong Province Nature Science Foundation under Grant ZR2017MEM019, in part by the Scientific research Projects of Universities in Shandong Province under Grant J18KA336, and in part by the Science Research Fund of Liaocheng University under Grant 318011606.

ABSTRACT At present, the probability density of most chaotic systems is unknown, and the statistical characteristics of chaotic sequences cannot be described by the probability density of chaotic maps. This paper constructs a class of quadratic polynomial chaotic maps with three system parameters, which are topologically conjugated with Tent maps. The probability density functions of this kind of chaotic maps are given. Then, an arcsine function is designed to transform the chaotic sequence generated by the quadratic polynomial chaotic map into a new random sequence, which obeys the uniform distribution on the interval $(-0.5, 0.5)$. In order to show the application of the new uniform random numbers, the applications of it in generating random arrangement, Gaussian measurement matrix of compressed sensing, and pseudo random number generator are discussed.

INDEX TERMS Quadratic polynomial chaotic maps, probability density function, random arrangement, Gaussian measurement matrix, pseudo random. number generator.

I. INTRODUCTION

With the arrival of the era of big data and the openness and sharing of the network, the security of multimedia information has become a research hotspot [1], [2]. The methods to protect information security mainly include information encryption [3], [4], authentication [5], digital watermarking [6], searchable encryption [7], etc. Among them, information encryption is widely used in secure communications [8], cloud storage [9], wireless mesh networks [10], Edge Computing Environment [11], and other occasions. Information encryption is the most basic means of information security technology. Chaos is a unique nonlinear dynamical phenomenon, which has the characteristics of extreme sensitivity to the initial state and system parameters, unpredictability, ergodicity, mixing and so on. These meaningful properties make chaotic systems widely used in many fields, including meteorology, sociology, physics, computer science, engineering, economics, and many others, especially in designing cryptographic algorithms [12]–[17]. Zheng *et al.* [3] proposed a lightweight authenticated encryption scheme with associated data based on a novel discrete chaotic S-box coupled map lattice (SCML), which avoids the dynamic degradation of the digital chaotic system and low efficiency of the chaos-based cryptosystem. Yu *et al.* [4] presented a novel four-image encryption scheme based on the quaternion Fresnel transforms computer generated hologram and the 2D Logistic-adjusted-Sine map.

Theoretically, a chaotic behavior will never close or repeat in the phase plane, However, from a practical point of view, the chaotic system is digital rather than analog, which makes the chaotic behavior degenerate into periodic behavior, which cause negative impact to the chaos-based applications [18], [19]. For example, some common insecurity problems in the field of chaotic image encryption are found in some encryption algorithms based on chaos because of the short orbits of the digital chaotic system [18]. In order to counteract the degeneration of chaos, Hua *et al.* [20] presented a sine chaotification model (SCM) as a general framework to enhance the chaos complexity of existing one-dimensional (1-D) chaotic maps. Li *et al.* [21] analyzed the dynamics behavior of digital chaotic maps via

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

state-mapping networks, which can facilitate counteracting the undesirable degeneration of chaotic dynamics in finite-precision domains.

The key indicators of random numbers are randomness, independence, and even distribution. At present, the long-term statistical characteristics of chaotic systems can not be described by means of probability theory, that is, the probability density of most chaotic systems is unknown, and the statistical characteristics of chaotic sequences can not be described by the probability density of chaotic maps. So the judgment of the independence and uniform distribution of random numbers generated by chaotic systems depends on the experimental simulation results, lacking theoretical basis. In chaotic systems, only the probability density functions of several simple chaotic maps, such as Chebyshev map [22], Tent map [23] and Logistic map [24], are known. In this paper, we construct a class of quadratic polynomial chaotic maps which is topologically conjugate with Tent maps and has three system parameters and the probability density function of this kind of chaotic map is derived according to the probability density function of Tent mapping. Then, according to the corresponding probability density function, an arcsine function is designed. By using the transformation of the arcsine function, the random number sequences generated by the quadratic polynomial chaotic map is transformed into a new sequence and the new sequence is subject to the uniform distribution in the interval $(-0.5, 0.5)$. Finally, the applications of the new random number sequences in generating random arrangement, Gaussian measurement matrix of compressed sensing and pseudo random number generator are discussed. The innovation of this paper lies in the following two aspects. First, we construct a class of chaotic maps of quadratic polynomial chaotic maps with three system parameters which are topologically conjugated with Tent maps, and the probability density function of this kind of chaotic maps is given. This greatly enriches the one-dimensional chaotic mapping systems and provides a method of generating uniform random numbers by chaotic mapping. Second, we provide a new method to construct Gaussian measurement matrix in compressed sensing. The method overcomes the shortcomings of the previous Gaussian matrix which requires large storage space and high computational complexity.

The remainder of the paper is organized as follows. Section II introduces a class of quadratic polynomial chaotic maps and their probability density functions. Several examples of chaotic mapping are demonstrated in Section III. The applications of quadratic polynomial chaotic maps are discussed in Section IV. Section V concludes the investigation.

II. A CLASS OF QUADRATIC POLYNOMIAL CHAOTIC MAPS AND THEIR PROBABILITY DENSITY FUNCTIONS

Definition 1 [25]: Let two maps be expressed as

$$x_{k+1} = f(x_k)\ (x \in I), \tag{1}$$
$$y_{k+1} = g(y_k)\ (y \in J). \tag{2}$$

We say that the maps (1) and (2) are topologically conjugated whenever there is a homeomorphism h: I $\to$ J such that for each $x \in$ I one has

$$g(h(x)) = h(f(x)) \tag{3}$$

The map h is called a topological conjugation.

Theorem 1: If the parameters a, b, c, d, e of the two functions

$$g(x) = ax^2 + bx + c, \quad (x \in (e-d|, e+d) \tag{4}$$

and

$$h(x) = d \times \cos(\pi x) + e, \quad (x \in (0, 1)) \tag{5}$$

satisfy the condition

$$\begin{cases} d \neq 0; \\ ad = 2; \\ 2ae + b = 0; \\ 2d + be + 2c = 2e. \end{cases} \tag{6}$$

then the function $g(x)$ and Tent maps are topologically conjugate with respect to the functions h(x).

Proof: The tent map is expressed as

$$f(x) = \begin{cases} 2x, & 0 \le x \le 1/2, \\ 2 - 2x, & 1/2 \le x \le 1. \end{cases} \tag{7}$$

On the one hand

$$\begin{aligned} h(f(x)) &= \begin{cases} d\cos 2\pi x + e, & 0 \le x \le \frac{1}{2} \\ d\cos\pi(2-2x) + e, & \frac{1}{2} \le x \le 1. \end{cases} \\ &= d\cos 2\pi x + e = h(2x). \end{aligned} \tag{8}$$

On the other hand

$$\begin{aligned} &g(h(x)) = ah^2(x) + bh(x) + c \\ &= a(d\cos\pi x + e)^2 + b(d\cos\pi x + e) + c \\ &= ad^2\cos^2\pi x + (2ade + bd)\cos\pi x + ae^2 + be + c \\ &= ad^2\frac{1+\cos 2\pi x}{2} + (2ade + bd)\cos\pi x + ae^2 + be + c \\ &= \frac{ad^2}{2}\cos 2\pi x + (2ade + bd)\cos\pi x + ae^2 + be + c + \frac{ad^2}{2} \end{aligned} \tag{9}$$

If $g(h(x)) = h(f(x)) = h(2x)$, if and only if conditions are established

$$\begin{cases} \frac{ad^2}{2} = d; \\ 2ade + bd = 0; \\ ae^2 + be + c + \frac{ad^2}{2} = e. \end{cases} \tag{10}$$

$d \neq 0$, simplify the formula (10) to get the formula (6). The proof is over.

Reference [25] points out that two topologically conjugate mappings have the same Lyapunov exponent. So, if the parameters in $g(x)$ satisfies the condition of equation (6), the Lyapunov exponent of $g(x)$ is the same as the Lyapunov

exponent of Tent mapping, which is ln2. Therefore, $g(x)$ is a chaotic system.

The quadratic polynomial chaotic map generated by Theorem 1 is defined as

$$x_{k+1} = g(x_k) = ax_k^2 + bx_k + c, \quad (x_0 \in (e - |d|, e + |d|)) \tag{11}$$

Here, the parameters a, b, c, d and e should satisfy the condition of Theorem 1.

Lemma 1 [25]: If the mapping $f(x)$ and $g(x)$ are topologically conjugate with respect to the function $h(x)$, and $\rho_f(x)$ is the probability density function of the mapping $f(x)$, then the probability density function of the mapping g(x) is expressed as

$$\rho_g(x) = \rho_f\left(h^{-1}(x)\right)\left|\frac{dh^{-1}(x)}{dx}\right| \tag{12}$$

Theorem 2: The probability density function of chaotic map (11) is expressed as

$$\rho_g(x) = \begin{cases} \dfrac{|d|}{\pi d}\dfrac{1}{\sqrt{d^2 - (x-e)^2}}, & x \in (e - |d|, e + |d|) \\ 0, & others. \end{cases} \tag{13}$$

Proof: the probability density function of Tent mapping is expressed as

$$\rho_T(x) = 1, \quad x \in (0, 1) \tag{14}$$

Theorem 1 shows that the chaotic map (11) and Tent map are topologically conjugate with respect to the functions (5). And

$$h^{-1}(x) = \frac{1}{\pi}\arccos\left(\frac{x-e}{d}\right) \tag{15}$$

$$\frac{dh^{-1}(x)}{dx} = \frac{|d|}{\pi d}\frac{-1}{\sqrt{d^2 - (x-e)^2}} \tag{16}$$

According to **lemma 1**, the probability density function of chaotic map (11) is expressed as

$$\rho_g(x) = \rho_f\left(h^{-1}(x)\right)\left|\frac{dh^{-1}(x)}{dx}\right| = \frac{|d|}{\pi d}\frac{1}{\sqrt{d^2 - (x-e)^2}} \tag{17}$$

The proof is over.

Theorem 2 shows that the sequences generated by the quadratic polynomial chaotic mapping (11) are not subject to uniform distribution and have obvious statistical characteristics. We can transform the non-uniformly distributed random sequence into uniformly distributed random sequence through a nonlinear transformation.

Theorem 3: Assuming that X is a random variable generated by a chaotic map (11), then the random variable Z is subject to uniform distribution in the interval $(-0.5, 0.5)$.

$$Z = \frac{1}{\pi}\arcsin\left(\frac{X}{d} - \frac{e}{d}\right) \tag{18}$$

Proof: From **theorem 2,** we know that the probability density function of random variable X is expressed as formula (13). Suppose the distribution function of random variable Z is $F_Z(z)$, then

$$\begin{aligned} F_Z(z) &= p(Z \le z) \\ &= p\left(\frac{1}{\pi}\arcsin\left(\frac{X}{d} - \frac{e}{d}\right) \le z\right) \\ &= p\left(\frac{X}{d} - \frac{e}{d} \le \sin \pi z\right) \\ &= p(X \le d\sin \pi z + e) \\ &= \int_{-\infty}^{d\sin \pi z + e} \rho_g(x)\, dx \end{aligned} \tag{19}$$

Then, the probability density function $\rho_Z(z)$is the derivative function of $F_Z(z)$, that is

$$\begin{aligned} \rho_Z(z) &= F_Z'(z) \\ &= \rho_g(d\sin(\pi z) + f)(d\sin(\pi z) + e)' \\ &= \frac{|d|}{\pi d}\frac{1}{\sqrt{d^2 - (d\sin(\pi z))^2}} d\pi\cos(\pi z) \\ &= 1, \quad z \in (-0.5,\ 0.5). \end{aligned} \tag{20}$$

Therefore, the density function of random variable Z is expressed as

$$\rho_Z(z) = \begin{cases} 1, & z \in (-0.5, 0.5) \\ 0, & others \end{cases} \tag{21}$$

III. SIMULATION EXAMPLES

Example 1: According to the condition of Theorem 1, we take $a = 2, b = -2, c = 0, d = 1, e = 0.5$. Then a new discrete chaotic map obtained, which is expressed as

$$x_{k+1} = 2x_k^2 - 2x_k,\ x_0 \in \left(-\frac{1}{2}, \frac{3}{2}\right) \tag{22}$$

The chaotic map (22) and Tent map are topologically conjugate with respect to $h(x) = \cos(\pi x) + 0.5,\ x \in (0, 1)$.

The probability density function of chaotic map (22) is $\rho_g(x)$, which is

$$\rho_g(x) = \frac{|d|}{\pi d}\frac{1}{\sqrt{d^2 - (x-e)^2}} = \frac{1}{\pi}\frac{1}{\sqrt{1 - (x-0.5)^2}}$$

We take the initial value $x_0 = 0.43765$, and the results obtained by 6000 iterations of Eq. (22) is shown in Fig. 1(a).

Example 2: According to the condition of Theorem 1, we take $a = -3, b = 6, c = -4/3, d = -2/3, e = 1$. Then a new discrete chaotic map is obtained, which is expressed as

$$x_{k+1} = -3x_k^2 + 6x_k - (4/3), \quad x_0 \in \left(\frac{1}{3}, \frac{5}{3}\right) \tag{23}$$

Chaotic map (23) and Tent map are topologically conjugate with respect to $h(x) = (-2/3)\cos \pi x + 1, x \in (0, 1)$.

The probability density function of chaotic map (23) is $\rho_g(x)$, which is

$$\rho_g(x) = \frac{|d|}{\pi d}\frac{1}{\sqrt{d^2 - (x-e)^2}} = \frac{-1}{\pi}\frac{1}{\sqrt{(4/9) - (x-1)^2}}$$

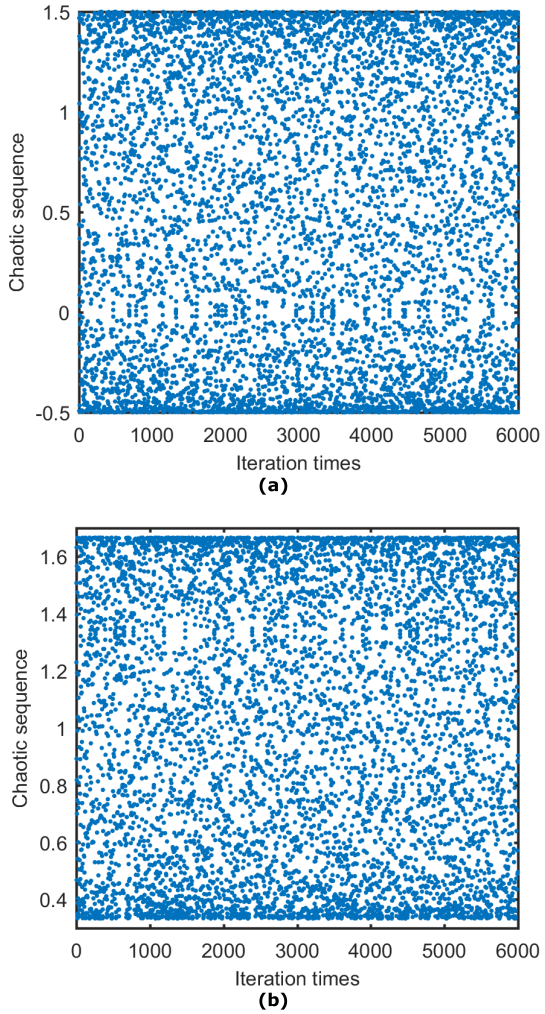

FIGURE 1. Iterative results of chaotic maps. (a) Iterative results of chaotic maps (22). (b) Iterative results of chaotic maps 23).

We take the initial value $x_0 = 1.23$, and the results obtained by 6000 iterations of Eq. (23) is shown in Fig. 1(b). It can be seen from Fig. 1(a) and Fig. 1(b) that the iteration value is full of the whole interval, which shows that systems (22) and (23) have chaotic characteristics of pseudo-random, bounded, ergodicity and so on.

IV. THE APPLICATION OF QUADRATIC POLYNOMIAL CHAOTIC MAPS

From the Theorem 3, it is known that the random sequence X generated by the chaotic mapping of quadratic polynomials is transformed into the random sequence Z by an arcsine transformation, and Z is subject to the uniform distribution In the interval $(-0.5, 0.5)$. The random sequence Z has many applications, such as constructing random arrangement sequence, Gaussian measurement matrix in compressed sensing, and random sequence with good uniformity and independence.

A. GENERATION OF RANDOM PERMUTATIONS IN IMAGE ENCRYPTION

Scrambling is an important technology for image encryption preprocessing. At present, there are a variety of scrambling algorithms for choice, such as Baker mapping method [26], piecewise linear chaotic map (PWLCM) method [27], combined 1D chaotic maps [28], high dimensional Arnold transform and Fibonacci-Q transform [29], Hilbert method, cellular automata method, affine transformation, magic square transformation, Knight cruising transformation, chaotic location exchange method, chaos ranking method [30] and so on, and the new digital image scrambling algorithm may be put forward constantly. In these methods, the chaos ranking method is widely used because it makes full use of the characteristics of chaos, such as ergodicity and initial value sensitivity. The disadvantage of this algorithm is that it needs to compare the $n\log(n)$ ranking. In this paper, a new random ranking algorithm based on chaotic uniform distribution position exchange is proposed.

Theorem 4: Suppose that U obeys uniform distribution on intervals (0, 1), then

$$X = floor(nU) + 1 \tag{24}$$

takes any one of $1, 2, \ldots, n$ with equal probability. Where, $floor(x)$ rounds the elements of x to the nearest integers less than or equal to x.

Proof: Consider that U obeys uniform distribution in interval (0, 1), and define that

$$X = \begin{cases} 1, & 0 < U < 1/n \\ 2, & 1/n \le U < 2/n \\ \quad \cdots\cdots & \\ n, & (n-1)/n \le U < 1 \end{cases} \tag{25}$$

If $0 < a < b < 1$, then $P(a \le U < b) = b - a$. Therefore, $P(X = j) = P((j-1)/n \le U < j/n) = 1/n$. This proves that X takes any one of $1, 2, \ldots n$ with equal probability.

From the above Theorem 3 and Theorem 4, we can get the specific steps of obtaining random permutations obeying uniform distribution.

Step (1): Setting the x_0 as the initial value of the chaotic system (22) to get a chaotic sequence X of length n.

Step (2): A new random sequences U is constructed by random sequences X as shown by

$$Z = \frac{1}{\pi}\arcsin\left(\frac{X}{d} - \frac{e}{d}\right) = \frac{1}{\pi}\arcsin(X - 0.5) \tag{26}$$

$$U = 2 \times |Z| \tag{27}$$

According to **Theorem 3,** it is known that Z is subject to uniform distribution in intervals $(-0.5, 0.5)$, then U is subject to uniform distribution in intervals (0, 1). $U = [U(1), U(2), \ldots, U(n)]$.

Step (3): Let $T = [t_1, t_2, t_3, \ldots, t_n] = [1, 2, 3, \ldots, n]$, $k = n$.

Step (4): Let $i = floor(k \times U(n - k + 1)) + 1$.

Step (5): Exchange the location of t_i and t_k.

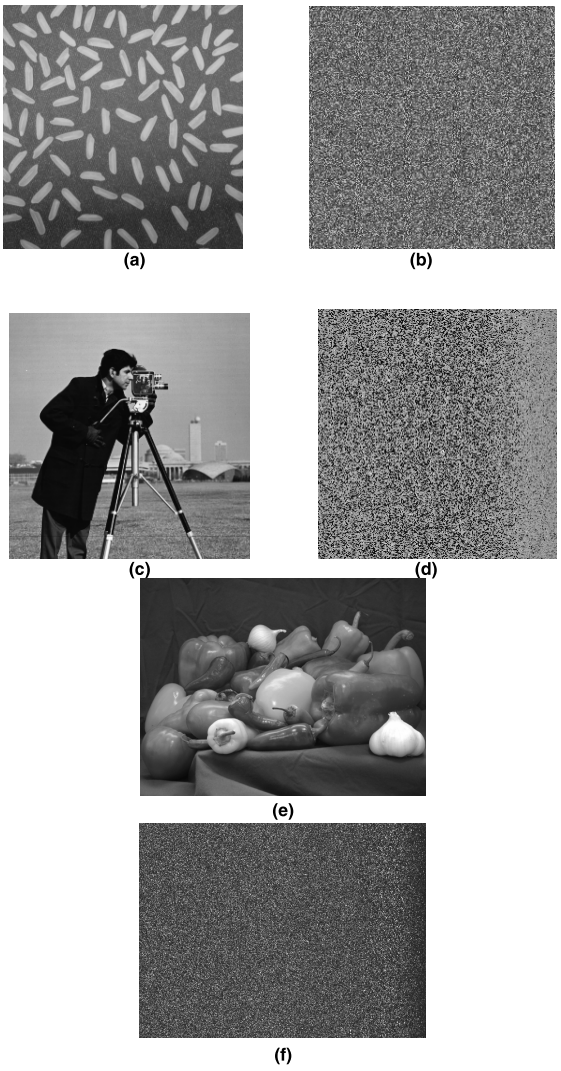

FIGURE 2. Scrambling effect: (a), (c), (e) are three plaintext images. (b), (d), (f) are corresponding scrambled images.

Step (6): Let $k = k - 1$.

Step (7): If $k > 0$, then repeat the above **Steps** (4) - (6). As the result, the new sequence T has the characteristics of equal probability. In this way, a random permutation sequence T can be generated only by n times of exchange. Compared with the chaotic sequence sorting algorithm, the computational complexity is greatly reduced.

Step (8): Transform the plaintext image matrix $P_{m\times n}$ to one dimensional vector $P = [p(1), p(2), \ldots, p(l)]$, where, $l = m \times n$. According to the random sequence T, P is scrambled as follows: $temp = P(i)$, $p(i) = P(t_i)$, $P(t_i) = temp$.

Step (9): Transform P into matrix of size $m \times n$, then the scrambled image is obtained.

Fig. 2 shows three experimental examples of image scrambling by using the random permutations sequence T. It can be seen that no information of the plaintext image can be obtained from the scrambled image, and the scrambling effect is excellent.

B. GENERATION OF GAUSS MEASUREMENT MATRIX IN COMPRESSED SENSING

The theory of compressed sensing was formally put forward in 2006 by Donoho [31] and Donoho and Wakin [32], and it has increasing applications in various fields such as image processing, pattern recognition, cloud computing, and internet of things, especially in the field of image encryption [33], [34]. It mainly includes three aspects [35]: (1) Sparse representation of signals. Find a basis Ψ, so that the signal x is sparse on Ψ, and obtain the transformation coefficient: $S = \Psi^{\mathrm{T}}x$, where S is the equivalent or approximate sparse representation of x. The selection of transform basis Ψ can be a basis which has been widely used, such as wavelet basis, Fourier basis, local Fourier basis and so on [9], [10]. (2) Design of measurement matrix. Restricted Isometry Property (RIP) [36] is an important criterion to judge whether a matrix can be a measurement matrix in compressed sensing theory. References [37] and [38] have proved that most random matrices satisfy RIP, such as Gaussian random measurement matrix and Bernoulli random measurement matrix. Reference [39] points out that in a sense, selecting random measurements is the best strategy for sparse matrices. (3) Reconstruction algorithm. Since the number of observations m is far less than the signal length n, reconstruction can be transformed into solving an underdetermined system of equations. There are many commonly used reconstruction algorithms: Orthogonal Matching Pursuit (OMP), Subspace Pursuit (SP) and Smoothing l0 Norm (SL0) algorithm [40].

The design of measurement matrix is the key to ensure the quality of signal sampling, and it is also the key to decide the difficulty of hardware implementation of compression sampling. Common measurement matrices include Gaussian matrix, Bernoulli matrix, partial hadamard matrix, partial Fourier matrix, sparse random matrix, toplitz matrix and cyclic matrix [41]. Candes *et al.* [42] proved that the Gaussian random measurement matrix with independent identical distribution can be a universal compressed sensing measurement matrix. The advantages of this kind of matrix are that it is irrelevant to most sparse signals and the number of measurements needed for accurate reconstruction is small. In this paper, Chaotic map (23) is used to generate the measurement matrix which obeys Gauss distribution. Once the parameters and initial values of chaotic mapping (23) are determined, the Gaussian measurement matrix is determined, which overcomes the shortcomings of the previous Gaussian matrix which requires large storage space and high computational complexity.

Lemma 2: [43] Suppose that U_1 and U_2 are two independent random variables and obey uniform distribution on (0, 1),

$$Z_1 = \sqrt{-2\ln(U_1)} \times \cos(2\pi U_2) \tag{28}$$

$$Z_2 = \sqrt{-2\ln(U_1)} \times \sin(2\pi U_2) \tag{29}$$

are two independent random variables, and they all obey the standard Gauss distribution.

From the above Theorem 3 and Lemma 2, The specific steps of constructing Gauss measurement matrix are as follows.

Step (1): Set the initial value x_0 of the chaotic map (23), iterate the chaotic map to generate a chaotic sequence X_1 of length $L = m \times n$, then, generate another chaotic sequence X_2 of the same length in the same way by setting another initial value x_0 of the chaotic map (23).

Step (2): Two new random sequences U_1 and U_2 are constructed by transforming random sequences X_1 and X_2, as shown in Eqs. (30) and (31). U_1 and U_2 obey uniform distribution on the interval (0,1),

$$U_1 = 2 \times \left| \frac{1}{\pi} \arcsin\left(-\frac{3}{2} X_1 + \frac{3}{2} \right) \right| \tag{30}$$

$$U_2 = 2 \times \left| \frac{1}{\pi} \arcsin\left(-\frac{3}{2} X_2 + \frac{3}{2} \right) \right| \tag{31}$$

Step (3): By using formulas (28) and (29), the sequences U_1 and U_2 are transformed into two sequences Z_1 and Z_2. Then Z_1 and Z_2 are independent of each other and obey the standard normal distribution. Converting any of Z_1 or Z_2 into a matrix of size $M \times N$, which is used as the measurement matrix ϕ in compressed sensing.

The histograms of sequence U_1, U_2, Z_1 and Z_2 are shown in Fig. 3. It can be seen that U_1 and U_2 obey uniform distribution on the interval (0,1), while Z_1 and Z_2 obey standard Gaussian distribution.

The core idea of compressed sensing is to project the transformed high-dimensional signal into a low-dimensional space by a measurement matrix unrelated to the transform basis, and then reconstruct the original signal with high probability from these few projections [44]. sparse signal representation, compression measurement and signal reconstruction are the three main components of CS theory. In this paper, discrete wavelet transform (DWT) is used as sparse representation methods. Orthogonal Matching Pursuit (OMP) is used as signal reconstruction algorithm and the Gauss matrix ϕ constructed in this paper is used as the measurement matrix. The natural image Cameraman is used for testing. the corresponding compressed ciphertext images and decompressed restored images with different compression rates CR are shown in Fig. 4. The compression ratio *CR* is computed by

$$CR = \frac{C\_height \times C\_width}{I\_height \times I\_width} \tag{32}$$

where *I_height* and *I_width* denote the height and width of the original image, respectively. And *C_height* and *C_width* are the corresponding height and width of the cipher image.

C. DESIGN OF PSEUDO RANDOM NUMBER GENERATOR BASED ON QUADRATIC POLYNOMIAL CHAOTIC MAP

Random numbers are widely used in encryption and signature. Random number generator is also often used to generate the initial population of genetic algorithm [45]. Their random

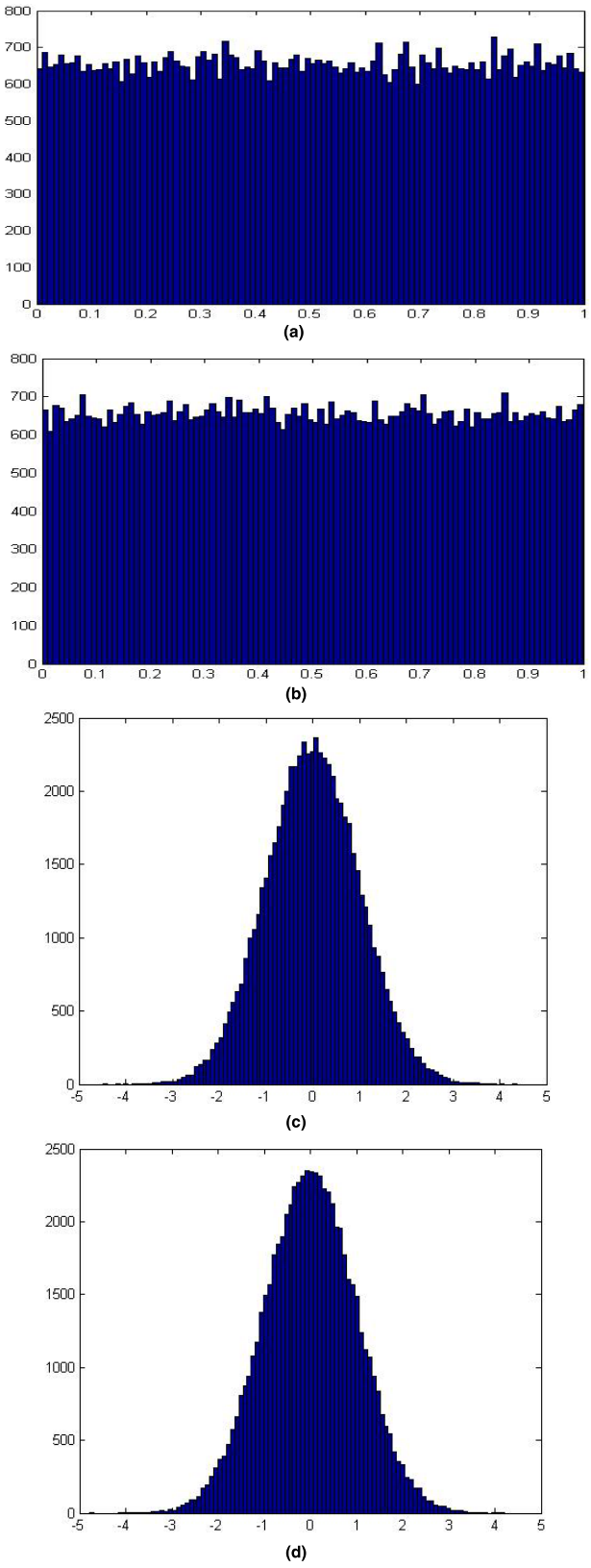

FIGURE 3. The histograms of sequence U_1, U_2, Z_1 and Z_2. (a) The histogram of U_1, (b) The histogram of U_2, (c) The histogram of the measurement matrix Z_1, (d) The histogram of the measurement matrix Z_2.

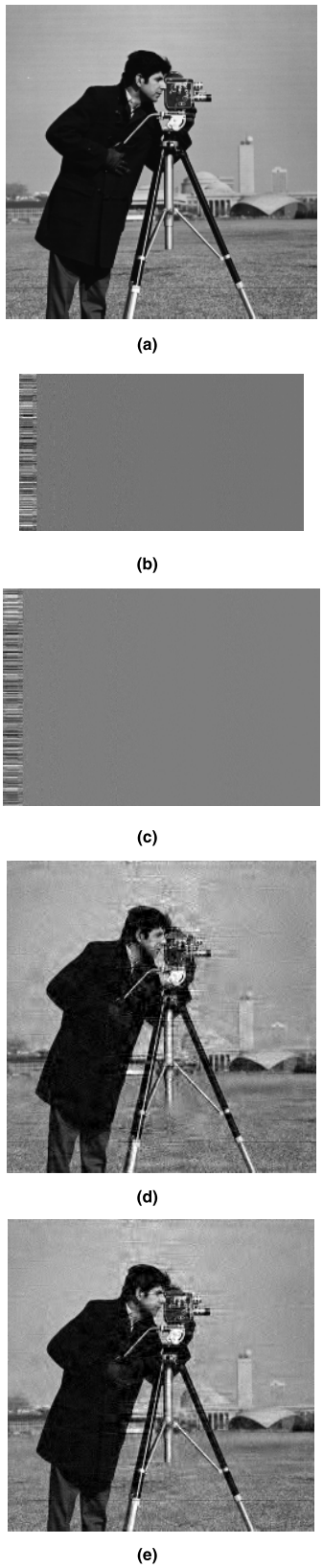

FIGURE 4. Experimental simulation results. (a) Plain image cameraman. (b) Cipher image of (a) with CR = 0.5. (c) Cipher image of (a) with CR = 0.65. (d) Decryped image for (b). (e) Decryped image for (c).

performance affects the security of encryption and signature schemes. Therefore, it is necessary to study and construct a good random number generator. The random number generator mainly includes the true random number generator and the pseudo random number generator. True Random Number Generator (RNG) is generally generated by physical method, which is vulnerable to external environmental impact and high cost. The study of pseudo random number generator is a hot topic. Chaos is a definite, unpredictable complex dynamic phenomenon. Chaotic maps are sensitive to initial values and exhibit unpredictable and random-like properties, which are widely used in the construction of pseudo-random number generators. References [46]–[48], pseudorandom number generators are constructed by using piecewise logistic mapping, k-modal mapping and improved logistic mapping, respectively. These pseudo random number generators improve the random performance of generated sequences, but their computation is large. Several combinations of Logistic mappings was proposed [49], [50] to further improve the random performance of sequences, but in the process of digitization, the influence of chaotic degradation on the randomness of sequences can not be overcome. Liu *et al.* [51] used Chen continuous hyperchaotic system to improve the random performance of output sequence by increasing the computational cost. Bahi *et al.* [52] proposed perturbation optimization and Dastgheib and Farhang [53] constructed a chaos-based digital pseudo-random number generator by an additive piecewise-constant perturbation to extend the period of random sequence. Zhu *et al.* [54] proposed a pseudo-random number generator based on hyperchaotic system. In this chapter, a pseudo-random number generator is designed by using the method of interval partition. The generated random numbers have good randomness, uniformity and independence.

1) DESIGN OF THE RANDOM NUMBER GENERATOR

Theorem 3 shows that the random sequence X generated by the quadratic polynomial chaotic mapping is transformed into the random sequence Z by an arcsine transformation. Z obeys the uniform distribution on the interval $(-0.5, 0.5)$. Therefore, the pseudo-random number generator can be designed by using the method of interval partition. The specific steps are as follows

1) Use chaotic maps (11) to generate random sequences $X = [x_1, x_2, \ldots x_n]$.
2) Through nonlinear transformation, the random sequence X is transformed into the random sequence $Z = [z_1, z_2, \ldots z_n]$. Z obeys the uniform distribution on the interval $(-0.5, 0.5)$, which is calculated by Eq.(18).
3) Divide the interval $(-0.5, 0.5)$ equally into $N = 2^m$ subintervals τ_i, $\tau_i = [t_i, t_{i+1})$. $t_i = -0.5 + i/N, i = 0, 1, \ldots, N-1, t_N = 0.5$. If $z_k \in \tau_i$, then $s_k = i$. Then, a random sequence of $\{s_k | \, k = 1, 2, \cdots, l\}$ is generated.

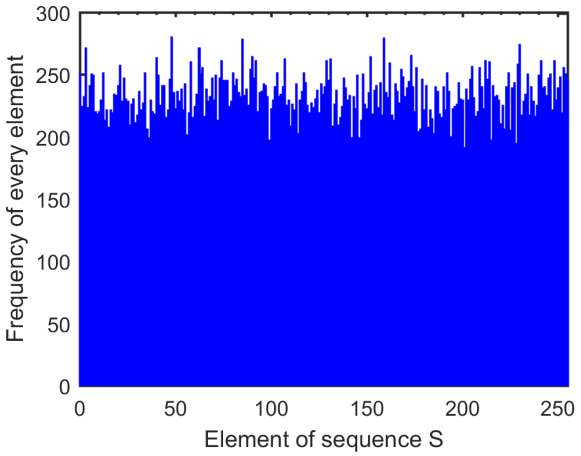

FIGURE 5. The histogram of sequence S.

Take $m = 8$, then $s_k \in \{0, 1, 2, \ldots, 255\}$. To iterate chaotic map (23) with 60000 times ($l = 60000$), then a random sequence of $S = \{s_1, s_2, \ldots, s_{60000}\}$ is generated. Fig.5 is the numerical distribution curve of S. The abscissa represents the value of a random sequence and the ordinate represents the frequency of each value in the sequence. From Fig. 5, we can see that the distribution of sequence S is very uniform, and it has good pseudo-randomness.

2) PERFORMANCE ANALYSIS OF THE CHAOTIC PSEUDO-RANDOM NUMBER GENERATOR

In this section, initial value sensitivity analysis, information entropy, Chi-Square Test and NIST SP 800-22 test are used to verify the uniformity, complexity and randomness of the generated random numbers.

a: KEY SENSITIVITY ANALYSIS

The pseudo random number generator constructed by chaos should maintain the sensitivity of chaos to initial value. Bit rate of change is the ratio of the pseudo-random sequence generated after only minor changes in the key to the number of changes in the previous pseudo-random sequence. It is used to measure the sensitivity of the chaotic pseudo-random number generator to the initial value. When the key changes slightly, the ideal bit rate is 50%. In the simulation process, the initial keys are 0.43270, $0.43270 + 10^{-15}$ and $0.43270 - 10^{-15}$, respectively, to generate three random sequences with a length of 60000, and then convert them into binary sequences T1, T2, T3 with a length of 480000. The change rate of the three sequences is shown in table 1, and the rate of change is close to 50%. Therefore, a small change in the key will cause a huge change in the generation of pseudo-random sequences, which shows that the random sequences generated by this method are highly sensitive to the key.

b: INFORMATION ENTROPY ANALYSIS OF RANDOM SEQUENCES

Shannon proposed the concept of information entropy, which is used to characterize the uncertainty of source. In this paper, information entropy is used to measure the degree of uncertainty of the sequence$\{s_k|k = 1, 2, \cdots, l\}$, $s_k \in \{i|i = 0, 1, \cdots, 2^m - 1\}$. The formula of information entropy is defined as

$$H = -\sum_{i=0}^{2^m-1} p_i \log_2(p_i) \tag{33}$$

where p_i is the probability of the occurrence of value i. For $m = 8$, when the probability distribution of values have equal probability, then all p_i is equal to 1/256 ($i = 0, 1, \ldots, 255$). Thus, the maximum entropy is $H_m = 8$. To test the information entropy of the random sequences, we select 100 different initial values to genarate 100 different random sequences. Let $m = 8$, then the maximum information entropy, the minimum information entropy and the average information entropy of the 100 random sequences S are 7.9998, 7.8993 and 7.9995 respectively, which is very close to the ideal value.

TABLE 1. Sensitivity analysis of pseudo random sequence initial value.

Key changes	Bit rate of change
1.236589->1.236589+10^{-15}	49.92%
1.236589->1.236589-10^{-15}	49.98%
1.236589+10^{-15}->1.236589-10^{-15}	50.04%

c: CHI-SQUARE TEST

Fig. 5 shows that the histogram of the random sequences S is uniformly distributed, which can be proved by the Chi-Square Test [55]. The means of Chi-Square test is described by

$$\chi^2 = \sum_{k=1}^{256} \frac{(v_k - e)^2}{e} \tag{34}$$

where v_k is the actual frequency of each value in S, and e is the expected frequency of each value.

For chaotic system (23), 10 sets of different initial values are selected to generate 10 chaotic key stream sequences of length 100000 for Chi-Square test. The results are shown in Table 2. The smaller the Chi-square value, the better the uniformity of the sequences. For the confidence level $a = 0.05$, if the chi square value does not exceed 295.25, it is considered to pass the test. It can be seen that the chi-square value of the sequences are less than 295.25, which means that all sequences have passed Chi-square test for confidence level $= 0.05$.

d: NIST RANDOMNESS TEST

The Random Number Generator Test Standard is the Federal Information Processing Standard issued by the National Institute of Standards and Technology (NIST) [56]. The NIST test suite includes 15 tests, which focus on a sort of different types of non-randomness that could exist in a sequence. Some tests include two sub-tests, namely, The tests of Cumulative Sums and Serial have two sub-tests. This statistical test suite is suitable for both the randomness test of encryption algorithm and the performance test of the random number generator.

TABLE 2. Chi-test results of 30 encrypted images under confidence level is 0.05.

The initial value x_0 of chaotic map	Length of sequence	The chi square value,	Test results
0.43270	100000	223.7590	pass
0.56727	100000	265.7128	pass
0.93456	100000	268.0110	pass
1.03456	100000	252.4769	pass
1.05456	100000	198.7795	pass
1.06734	100000	261.1179	pass
1.12673	100000	253.7692	pass
1.10226	100000	252.0410	pass
1.23232	100000	259.0321	pass
1.09120	100000	259.7714	pass

Usually, the NIST test requires 1000 sequences and each one has 1000000 bits. NIST test software mainly uses two performance indicators: pass rate and *P-value* to determine the random performance of the sequence.

Since each test is independent of each other, the pass rate of the sequences can be tested. The sequences to be tested are 1000, the significant level $a = 0.01$. If the *P-value*s of 985 sequences are greater than 0.01, then the pass rate is $985/1000 = 0.985$. The confidence interval used to test the pass rate is defined as:

$$1 - a \pm \sqrt{a(1-a)/m} \tag{35}$$

where $a = 0.01$. If each test pass rate is within the confidence interval, then the random sequence generation algorithm tested can be considered to have high trust. On the contrary, it indicates that the measured data is not random. Using the above formula, when $a = 0.01$ and $m = 1000$, the confidence interval is $1-0.01 \pm 3\sqrt{0.01 \times 0.99/1000} = 0.99 \pm 0.0094393 = [0.980561, 0.9994393]$, which indicates that the sequence pass rate must be larger than 0.980561.

The purpose of testing the *P-value* is primarily to detect the uniformity of the sequence distribution. First, calculate the chi-square value of the m groups independent random sequences:

$$\chi^2 = \sum_{i=1}^{10} \frac{(F_i - m/10)^2}{(m/10)} \tag{36}$$

where F_i is the number of *P-value* falling within the interval $[(i-1) \times 0.1, i \times 0.1]$. Then, the P_value_T of each test *P-value*s is obtained by

$$P\_value_T = igamc(9/2,\ \chi^2/2) \tag{37}$$

where $igamc(n,\ x)$ is an incomplete Gamma function. If $P_value_T \geq 0.01$, it can be determined that the *P-value* of the measured sequence is uniformly distributed. According to this, the sequence has good random performance.

To test the random performance of sequences generated by our sheme, we set the initial value $x(0)$ of chaotic map (23) varies from 1.0005 to 1.5 with a variable step size of 0.0005. With each initial value $x(0)$, chaotic map (23) iterates 1000,000 times. Hence, we can generate 1000 sequences, each of which contains 1000000 values. Each original chaotic real sequence $X = [x(i)]$ generated by chaotic map (23) is transformed into a sequence $Z = [z(i)]$ by using Eq.(18), then each sequence Z is transformed into a binary sequence $S = [s(i)]$ by using the following conversion rules: If $z(i) \geq 0$, then $s(i) = 1$. If $z(i) < 0$, then $s(i) = 0$. $i = 1, 2, \ldots, 1000000$. By this way, 1000 sequences of 1000000 bits were produced. The results from all statistical tests are given in Table 3. The *P-value* in Table 3 is actually the P_value_T calculated by Eq. (37). The calculation method of the *P-values* in Table 3 is described in detail below, which is illustrated by calculating the *P-value* of "Frequency (monobit)" as a example. In the tests of 1000 sequences ($m = 1000$), the results obtained by the NIST suite showed that there are 101 sequences have *p-value*s fell in the interval [0, 0.1], 100 sequences have *p-value*s fell in the interval [0.1, 0.2], 93 sequences have *p-value*s fell in the interval [0.2, 0.3], ..., 101 sequences have *p-value*s fell in the interval [0.9, 1.0]. So we get $F = [F_1, F_2, \ldots, F_{10}] = [101, 100, 93, 110, 80, 101, 98, 115, 101, 101]$. Then we obtain $\chi^2 = 7.8200$ by using Eq.(36). Finally, we obtain $P\_value_T = 0.6744$ by using Eq.(37), which is the first value in the first row of Table 3. The other results are calculated in the same way.

TABLE 3. NIST statistical test suite results for 1000 sequences of size 1 million bits each generated by new pseudo-random scheme.

NIST statistical test	*P-value*	Pass rate	Results
Frequency (monobit)	0.6744	985/1000	pass
Block Frequency ($m = 128$)	0.1818	985/1000	pass
Cumulative Sums (Forward)	0.3902	981/1000	pass
Cumulative Sums (Reverse)	0.9774	985/1000	pass
Runs	0.7507	987/1000	pass
Longest Run of Ones	0.2634	988/1000	pass
Rank	0.9091	987/1000	pass
FFT	0.7507	985/1000	pass
Non-Overlapping Templates ($m = 9$, $B = 000000001$)	0.6276	987/1000	pass
Overlapping Templates ($m = 9$)	0.6521	988/1000	pass
Universal	0.1919	981/1000	pass
Approximate Entropy($m = 10$)	0.2108	981/1000	pass
Random-Excursions	0.8711	604/609	pass
Random-Excursions Variant	0.7409	602/609	pass
Serial Test 1 ($m = 16$)	0.6707	989/1000	pass
Serial Test 2 ($m = 16$)	0.5838	992/1000	pass
Linear complexity ($M = 500$)	0.3331	991/1000	pass

Table 3 shows that the entire NIST test is passed successfully: all the *P values* from all 1000 sequences are distributed uniformly in the 10 subintervals and the pass rate is also in an acceptable range. The minimum pass rate for each statistical test with the exception of the Random -Excursions Variant test is 981 for a sample size of 1000 binary sequences. The minimum pass rate for the Random -Excursion Variant test is 602 for a sample size of 609 binary sequences.

e: TESTU01 TEST

TestU01 is a software library implemented in the ANSI C language, which offers a collection of utilities for the

TABLE 4. Summary results of the TestU01 tests.

Test type	Number of bits	Number of statistics	Number of Failures
Rabbit	1048576	38	0
Alphabit	1048576	17	0
Rabbit	100000000	40	1
Alphabit	100000000	17	1

empirical statistical testing of uniform random number generators (RNGs). The tests can be applied to instances of the generators predefined in the library, or to user-defined generators, or to streams of random numbers produced by any kind of device or stored in files. There are three predefined batteries of tests for bit sequences in TestU01, namely, Rabbit, Alphabit and BlockAlphabit. They were originally designed to test a finite sequence contained in a binary file.

When invoking the batteries of tests, one must specify the number *nb* of bits available for each test. When the bits are in a file, *nb* must not exceed the number of bits in the file, and each test will reuse the same sequence of bits starting from the beginning of the file (so the tests are not independent). Rabbit and Alphabit apply 38 and 17 different statistical tests, respectively. BlockAlphabit applies the Alphabit battery of tests repeatedly to a generator or a binary file after reordering the bits by blocks of different sizes (with sizes of 2, 4, 8, 16, 32 bits). Sometimes, Alphabit test computes more than one statistic and its *p-value*, so the number of statistics in Alphabit may be larger than 38. In our tests, 100 sequences with length of 1000000 bits were produced in the same way as the NIST Statistical test, and save the 100×1000000 bits in a binary file named MyData.bin. Here, Rabbit and Alphabit tests are done with two cases. In the first case, we use at most 1048576 (= 2^20) bits from the binary file. The summary results of the test is shown in the first and second row of Table 4, which show that all tests were passed. In the second case, we use at most 100000000 (= 10^8) bits from the binary file and the summary results of the test is shown in the third and fourth row of Table 4, which show that only one test for each test is failed with a *p-value* outside [0.001, 0.9990].

For the measurement of randomness or complexity of chaotic sequences, besides the above measures, there are some other measures, such as entropy algorithm [57], [58].

D. COMPLEXITY OF THE PROPOSED SOLUTION

The test programs are run on a machine with a 3.3 GHz Intel processor running under Windows 7 operation system and Matlab R2016b software development platform.

1) FOR GENERATING OF RANDOM PERMUTATION SEQUENCE T

By using the method introduced in sub-Section A, a random permutation sequence T can be generated only by n times of exchange. When $n = 512 \times 512$, it takes 0.0150 seconds. While generating a sequence of same length by using chaotic sequence sorting algorithm, it takes 0.0230 seconds. Compared with the chaotic sequence sorting algorithm, the computational complexity of the proposed solution is greatly reduced.

2) FOR GENERATING GAUSS MEASUREMENT MATRIX ϕ

By using the method introduced in sub-Section B, a gauss measurement matrix ϕ can be generated. When the size of ϕ is 512×512, it takes 0.0310 seconds.

3) FOR GENERATING PSEUDO-RANDOM BINARY SEQUENCE S

By using the method introduced in sub-Section C, a chaotic pseudo-random binary sequence S can be generated. When the length of S is 1000000 bits, it takes 0.0470 seconds.

V. CONCLUSION

This paper has constructed a class of quadratic polynomial chaotic maps which are topologically conjugate with Tent maps. a method of generating uniform random numbers by chaotic mapping has been provided and the applications of random variables obeying uniform distribution in generating position scrambling sequences, observation matrices in compressed sensing and random number generator are discussed. It has been demonstrated that the uniform random number generated by the method in this paper has good randomness. It has passed Chi-Square test and NIST SP 800-22 test and TestU01. In addition, the method of constructing Gauss measurement matrix using the uniform random number generated by the method in this paper overcomes the shortcomings of the previous Gaussian matrix which requires large storage space and high computational complexity. Random number generators are crucial ingredients for a whole range of computer usages, such as statistical experiments, simulation of stochastic systems, numerical analysis, probabilistic algorithms, cryptology, secure communications, computer games, and gambling machines, to name a few. Therefore, the proposed approach has a wide range of industrial significance in the field of computer application.

REFERENCES

[1] B. B. Gupta, *Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives*. Boca Raton, FL, USA: CRC Press, 2017.
[2] B. B. Gupta, D. P. Agrawal, and S. Yamaguchi, "*Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*. Philadelphia, PA, USA: IGI Global, 2016.
[3] Q. Zheng, X. Wang, M. K. Khan, W. Zhang, B. B. Gupta, and W. Guo, "A lightweight authenticated encryption scheme based on chaotic SCML for railway cloud service," *IEEE Access*, vol. 6, pp. 711–722, 2018.
[4] C. Yu, J. Li, X. Li, X. Ren, and B. B. Gupta, "Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram," *Multimedia Tools Appl.*, vol. 77, no. 4, pp. 4585–4608, Feb. 2017.
[5] A. Tewari and B. B. Gupta, "A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices," *Int. J. Adv. Intell. Paradigms*, vol. 9, nos. 2–3, pp. 111–121, Jan. 2017.
[6] J. Li, C. Yu, B. B. Gupta, and X. Ren, "Color image watermarking scheme based on quaternion Hadamard transform and Schur decomposition," *Multimedia Tools Appl.*, vol. 77, no. 4, pp. 4545–4561, Feb. 2017.

[7] Q. Zhang, Q. Liu, and G. Wang, "PRMS: A personalized mobile search over encrypted outsourced data," *IEEE Access*, vol. 6, pp. 31541–31552, 2018.

[8] C. E. Shannon, "Communication theory of security systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.

[9] B. B. Gupta, S. Gupta, and P. Chaudhary, "Enhancing the browser-side context-aware sanitization of suspicious HTML5 code for halting the DOM-based XSS vulnerabilities in cloud," *Int. J. Cloud Appl. Comput.*, vol. 7, no. 1, pp. 1–31, Jan. 2017.

[10] X. Deng, J. Luo, L. He, Q. Liu, X. Li, and L. Cai, "Cooperative channel allocation and scheduling in multi-interface wireless mesh networks," *Peer-to-Peer Netw. Appl.*, vol. 12, no. 1, pp. 1–12, Jan. 2019.

[11] P. Guan, X. Deng, Y. Liu, and H. Zhang, "Analysis of multiple clients' behaviors in edge computing environment," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 9052–9055, Sep. 2018.

[12] C. Zhu, "A novel image encryption scheme based on improved hyper-chaotic sequences," *Opt. Commun.*, vol. 285, no. 1, pp. 29–37, 2012.

[13] H. Zhu, X. Zhang, H. Yu, C. Zhao, and Z. Zhu, "An image encryption algorithm based on compound homogeneous hyper-chaotic system," *Nonlinear Dyn.*, vol. 89, no. 1, pp. 61–79, Jul. 2017.

[14] Y. Zhang, D. Xiao, Y. Shu, and J. Li, "A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations," *Signal Process., Image Commun.*, vol. 28, no. 3, pp. 292–300, 2013.

[15] J.-X. Chen, Z.-L. Zhu, C. Fu, and H. Yu, "Optical image encryption scheme using 3-D chaotic map based joint image scrambling and random encoding in gyrator domains," *Opt. Commun.*, vol. 341, pp. 263–270, Apr. 2015.

[16] S. Zhu and C. Zhu, "Image encryption algorithm with an avalanche effect based on a six-dimensional discrete chaotic system," *Multimedia Tools Appl.*, vol. 77, no. 21, pp. 29119–29142, Nov. 2018.

[17] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18759–18770, 2018.

[18] C. Li, D. Lin, B. Feng, J. Lü, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018.

[19] C. Li, D. Lin, J. Lü, and F. Hao, "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography," *IEEE Multimedia*, vol. 25, no. 4, pp. 46–56, Oct./Dec. 2018.

[20] Z. Hua, B. Zhou, and Y. Zhou, "Sine chaotification model for enhancing chaos and its hardware implementation," *IEEE Trans. Ind. Electron.*, vol. 66, no. 2, pp. 1273–1284, Feb. 2019.

[21] C. Li, B. Feng, S. Li, J. Kurths, and G. Chen, "Dynamic analysis of digital chaotic maps via state-mapping networks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, to be published. doi: 10.1109/TCSI.2018.2888688.

[22] X. Huang, Y. Zhang, Y. Jin, and H. Lu, "An improved decomposition method in probabilistic analysis using Chebyshev approximations," *Structural Multidisciplinary Optim.*, vol. 43, no. 6, pp. 785–797, Jun. 2011.

[23] P. Góra and A. Boyarsky, "On the significance of the tent map," *Int. J. Bifurcation Chaos*, vol. 13, no. 5, pp. 1299–1301, May 2003.

[24] F.-G. Li, "Effects of noise on periodic orbits of the logistic map," *Central Eur. J. Phys.*, vol. 6, no. 3, pp. 539–545, Sep. 2008.

[25] H. Broer and F. Takens, "Dynamical systems and chaos," in *Applied Mathematical Sciences*, vol. 172. New York, NY, USA: Springer, 2011.

[26] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[27] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, 2011.

[28] C. Zhu, G. Wang, and K. Sun, "Improved cryptanalysis and enhancements of an image encryption scheme using combined 1D chaotic maps," *Entropy*, vol. 20, no. 11, Nov. 2018, Art. no. 843.

[29] F.-Y. Sun, S.-T. Liu, and Z.-W. Lü, "Image encryption using high-dimension chaotic system," *Chin. Phys.*, vol. 16, no. 12, pp. 3616–3623, Dec. 2007.

[30] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," *Pattern Recognit. Lett.*, vol. 31, no. 5, pp. 347–354, 2010.

[31] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[32] E. J. Candès and M. B. Wakin, "An introduction to compressive sampling," *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 21–30, Mar. 2008.

[33] Y. Zhang, L. Y. Zhang, J. Zhou, L. Liu, F. Chen, and X. He, "A review of compressive sensing in information security field," *IEEE Access*, vol. 4, pp. 2507–2519, 2016.

[34] S. Zhu, C. Zhu, and W. Wang, "A novel image compression-encryption scheme based on chaos and compression sensing," *IEEE Access*, vol. 6, pp. 67095–67107, 2018.

[35] Y.-M. Ren, Y.-N. Zhang, and Y. Li, "Advances and perspective on compressed sensing and application on image processing," *Acta Automatica Sinica*, vol. 40, no. 8, pp. 1563–1575, 2014.

[36] R. Baraniuk, M. Davenport, R. DeVore, and M. Wakin, "A simple proof of the restricted isometry property for random matrices," *Constructive Approximation*, vol. 28, no. 3, pp. 253–263, Dec. 2008.

[37] E. J. Candès and T. Tao, "Near-optimal signal recovery from random projections: Universal encoding strategies?" *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5406–5425, Dec. 2006.

[38] E. J. Candès, "The restricted isometry property and its implications for compressed sensing," *Comp. Rendus Mathematique*, vol. 346, nos. 9–10, pp. 589–592, May 2008.

[39] J. Bobin, J.-L. Starck, and R. Ottensamer, "Compressed sensing in astronomy," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 5, pp. 718–726, Oct. 2008.

[40] N. Zhou, J. Yang, C. Tan, S. Pan, and Z. Zhou, "Double-image encryption scheme combining DWT-based compressive sensing with discrete fractional random transform," *Opt. Commun.*, vol. 354, pp. 112–121, Nov. 2015.

[41] E. Au-Yeung, "Sparse signal recovery using a new class of random matrices," *Adv. Pure Appl. Math.*, vol. 8, no. 2, pp. 79–89, Apr. 2017.

[42] E. J. Candès, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489–509, Feb. 2006.

[43] G. E. P. Box and M. E. Müller, "A note on the generation of random normal deviates," *Ann. Math. Statist.*, vol. 29, no. 2, pp. 610–611, 1958.

[44] Y. Zhang, Y. Xiang, and L. Y. Zhang, "Compressive Sensing," in *Secure Compressive Sensing in Multimedia Data, Cloud Computing and IoT*. Singapore: Springer, 2019.

[45] X. Deng, D. Zeng, and H. Shen, "Causation analysis model: Based on AHP and hybrid Apriori-Genetic algorithm," *J. Intell. Fuzzy Syst.*, vol. 35, no. 1, pp. 767–778, 2018.

[46] Y. Wang, Z. Liu, J. Ma, and H. He, "A pseudorandom number generator based on piecewise logistic map," *Nonlinear Dyn.*, vol. 83, no. 4, pp. 2373–2391, Mar. 2016.

[47] M. Garcia-Martinez and E. Campos-Canton, "Pseudo-random bit generator based on multi-modal maps," *Nonlinear Dyn.*, vol. 82, no. 4, pp. 2119–2131, Dec. 2015.

[48] M. A. Murillo-Escobar, C. Cruz-Hernández, L. Cardoza-Avendaño, and R. Méndez-Ramírez, "A novel pseudorandom number generator based on pseudorandomly enhanced logistic map," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 407–425, Jan. 2017.

[49] M. François, T. Grosges, D. Barchiesi, and R. Erra, "Pseudo-random number generator based on mixing of three chaotic maps," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 4, pp. 887–895, Apr. 2014.

[50] S. F. Raza and V. R. Satpute, "PRaCto: Pseudo random bit generator for cryptographic application," *Ksii Trans. Internet Inf. Syst.*, vol. 12, no. 12, pp. 6161–6176, Dec. 2018.

[51] Y. Liu, J. Wang, J. Fan, and L. Gong, "Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences," *Multimedia Tools Appl.*, vol. 75, no. 8, pp. 4363–4382, Apr. 2016.

[52] J. M. Bahi, X. Fang, C. Guyeux, and L. Larger, "FPGA design for pseudo-random number generator based on chaotic iteration used in information hiding application," *Appl. Math. Inf. Sci.*, vol. 7, no. 6, pp. 2175–2188, Nov. 2013.

[53] M. A. Dastgheib and M. Farhang, "A digital pseudo-random number generator based on sawtooth chaotic map with a guaranteed enhanced period," *Nonlinear Dyn.*, vol. 89, no. 4, pp. 2957–2966, Sep. 2017.

[54] C. Zhu, G. Wang, and K. Sun, "Cryptanalysis and improvement on an image encryption algorithm design using a novel chaos based S-box," *Symmetry*, vol. 10, no. 9, 2018, Art. no. 399.

[55] S. Zhu, C. Zhu, and W. Wang, "A new image encryption algorithm based on chaos and secure hash SHA-256," *Entropy*, vol. 20, no. 9, Sep. 2018, Art. no. 716.

[56] A. L. Ruhkin, "Testing randomness: A suite of statistical procedures," *Theory Probab. Appl.*, vol. 45, no. 1, pp. 111–132, Jul. 2000.

[57] K.-H. Sun, S.-B. He, Y. He, and L.-Z. Yin, "Complexity analysis of chaotic pseudo-random sequences based on spectral entropy algorithm," *Acta Phys. Sin.*, vol. 62, no. 1, Jan. 2013, Art. no. 010501.

[58] S.-B. He, K.-H. Sun, and C.-X. Zhu, "Complexity analyses of multi-wing chaotic systems," *Chin. Phys. B*, vol. 22, no. 5, May 2013, Art. no. 050506.

SHUQIN ZHU received the master's degree in mathematics from the University of Science and Technology Beijing, China. She joined Liaocheng University, where she is currently an Associate Professor in mathematics. Her research interests include mathematical model, the applications of chaos-based cryptography in multimedia information security, and image processing.

CONGXU ZHU received the Ph.D. degree in computer science and technology from Central South University, Changsha, Hunan, China, in 2006, where he is currently a Professor. His research interests include chaos theory and its applications in multimedia information security, chaos-based cryptography, and image processing.

HUANQING CUI received the Ph.D. degree in computer software and theory from the Shandong University of Science and Technology, China, in 2011. He is currently an Associate Professor with the Shandong University of Science and Technology. His research interests include wireless sensor networks, algorithm design and analysis, and graph computing. He is a Senior Member of the China Computer Federation.

WENHONG WANG received the B.S. degree in computer software from Shandong University, Jinan, China, in 1995, the M.S. degree in computer application technology from the Beijing University of Chemical Technology, Beijing, China, in 2003, and the Ph.D. degree in computer science and technology from Zhejiang University, Hangzhou, China, in 2016. He is currently an Associate Professor with the College of Computer Science, Liaocheng University, Liaocheng, China. His main research interests include image processing, pattern recognition, and machine learning.