Designing Hyperchaotic Cat Maps With Any Desired Number of Positive Lyapunov Exponents

Zhongyun Hua, *Member, IEEE*, Shuang Yi, *Student Member, IEEE*, Yicong Zhou, *Senior Member, IEEE*, Chengqing Li, *Senior Member, IEEE*, and Yue Wu, *Member, IEEE*

***Abstract*—Generating chaotic maps with expected dynamics of users is a challenging topic. Utilizing the inherent relation between the Lyapunov exponents (LEs) of the Cat map and its associated Cat matrix, this paper proposes a simple but efficient method to construct an n-dimensional (n-D) hyperchaotic Cat map (HCM) with any desired number of positive LEs. The method first generates two basic n-D Cat matrices iteratively and then constructs the final n-D Cat matrix by performing similarity transformation on one basic n-D Cat matrix by the other. Given any number of positive LEs, it can generate an n-D HCM with desired hyperchaotic complexity. Two illustrative examples of n-D HCMs were constructed to show the effectiveness of the proposed method, and to verify the inherent relation between the LEs and Cat matrix. Theoretical analysis proves that the parameter space of the generated HCM is very large. Performance evaluations show that, compared with existing methods, the proposed method can construct n-D HCMs with lower computation complexity and their outputs demonstrate strong randomness and complex ergodicity.**

***Index Terms*—Cat map, Cat matrix, chaotification, hyperchaotic behavior, Lyapunov exponent (LE).**

I. Introduction

CHAOTIC behaviors can be observed in all kinds of natural and non-natural phenomena, such as weather forecasting in meteorology [1] and population growth in sociology [2]. Dynamic systems are mathematical concepts describing chaotic behaviors, and attract intensive attentions [3], [4]. A dynamic system demonstrating chaotic behavior has properties of ergodicity, unpredictability, and sensitivity to change of initial condition and/or control parameter. So, strong chaotic behavior is very desired in many real applications [5] and Lyapunov exponent (LE) is a widely used indicator to quantitatively measure it [6]–[8]. If a dynamic system owns one positive LE, it is considered chaotic. Furthermore, if a high-dimensional (HD) dynamic system has at least two positive LEs, it can demonstrate hyperchaotic behavior, and its attractors irregularly distribute in several dimensions [9]. Thus, its behavior is usually much more complex and it has much unpredictable topological structure than that owning only one positive LE [10], [11], making hyperchaotic systems are more attractive, especially in the field of chaos-based cryptography [12]–[14].

Existing hyperchaotic systems can be classified into two categories: 1) discrete-time system and 2) continuous-time system. A discrete-time system is commonly defined by a difference equation and it can be implemented through an iterative procedure. In contrast, a continuous-time system is usually represented by a partial and/or ordinary differential equation. In the past decades, a wide body of research has been devoted to developing continuous-time hyperchaotic systems using various strategies: state feedback control [15], [16], linear or nonlinear coupling [17], [18], and other techniques [19]–[23]. It deserves noting that Shen *et al.* [20], [21] proposed a systematic methodology for constructing hyperchaotic systems with multiple positive LEs and further developed a simple model to design hyperchaotic systems with any desired number of positive LEs. Using the methods given in [20] and [21], one can construct a continuous-time hyperchaotic system with multiple positive LEs, and thus can customize it with the expected complex behavior. Compared with continuous-time systems, the occurrence of chaotic behaviors of discrete-time systems can be directly observed. Thus, the latter has many advantages in performance analysis and hardware/software implementation, making designing discrete-time hyperchaotic systems with multiple positive LEs very attractive [24].

As a special discrete-time chaotic system, Arnold's Cat map not only has common properties of discrete-time chaotic systems, but also possesses many exclusive characteristics, including adaptability to arbitrary finite precision [25], reversibility [26], area preserving [25], Anosov diffeomorphism and structural stability [27]. Such nice properties let Cat map receive many researchers' attentions [28]–[30]. It has been used in many applications, such as the cryptographic applications [31]–[33] and steganography [34]. Besides, Cat

Manuscript received May 20, 2016; revised October 9, 2016; accepted December 8, 2016. Date of publication January 4, 2017; date of current version January 15, 2018. This work was supported in part by the Macau Science and Technology Development Fund under Grant FDCT/016/2015/A1, and in part by the Research Committee at University of Macau under Grant MYRG2014-00003-FST and Grant MYRG2016-00123-FST. This paper was recommended by Associate Editor M. Forti. *(Corresponding author: Yicong Zhou.)*

Z. Hua is with the School of Computer Science and Technology, Harbin Institute of Technology Shenzhen Graduate School, Shenzhen 518055, China, and also with the Department of Computer and Information Science, University of Macau, Macau 999078, China (e-mail: huazyum@gmail.com).

S. Yi and Y. Zhou are with the Department of Computer and Information Science, University of Macau, Macau 999078, China (e-mail: yishuang0227@gmail.com; yicongzhou@umac.mo).

C. Li is with the College of Information Engineering, Xiangtan University, Xiangtan 411105, China (e-mail: drchengqingli@gmail.com).

Y. Wu is with the Information Sciences Institute, University of Southern California, CA 90292 USA (e-mail: yue_wu@isi.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCYB.2016.2642166

map also has potential for some hot applications, such as real-time secure communication system [35] and networked system [36]. To achieve high randomness and a large parameter space, some construction methods of generating Cat map were proposed. Among them, a typical generation method is to construct n-dimensional (n-D) Cat matrices, i.e., transformation matrices of n-D Cat maps. These methods can be further classified into two classes: 1) fixed dimensional Cat map generation methods [25], [37], [38] and 2) variable dimensional Cat map generation methods [39]–[41]. As for the former, the parameter spaces are commonly too small to satisfy the security requirement of cryptographic applications [31]. As for the latter, the number of independent parameters is quite small even when the dimension is very large, due to all kinds of linear operations involved in constructing the Cat matrices, e.g., matrix multiplication and addition.

To construct Cat maps with more independent parameters, higher randomness and desired complexity, this paper first discloses some inherent relation between LEs of the Cat map and its associated Cat matrix, and then proposes a simple model to construct n-D hyperchaotic Cat map (HCM) with any desired number of positive LEs, where $n \geq 3$. In the process of constructing an n-D Cat matrix, two basic n-D Cat matrices are iteratively constructed using a parametric 2-D Cat matrix. The final n-D Cat matrix can be obtained by performing similarity transformation on a basic n-D Cat matrix with another. Additional spatial location parameters are introduced to expand the parameter space of Cat matrices. It was proved that the obtained n-D Cat maps have $\lfloor n/2 \rfloor$ positive LEs. Thus, one can customize a new n-D HCM owning any given number of positive LEs. To verify the effectiveness of the proposed method and the found relation between LEs and the Cat matrix, we construct two concrete examples of n-D HCMs: 1) a 5-D HCM with two positive LEs and 2) a 10-D HCM with five positive LEs. Theoretical analysis shows that the proposed method can generate an n-D Cat matrix with $\lfloor n^2/2 \rfloor$ independent elements. Compared with existing methods proposed in [25] and [37]–[42], the proposed method can generate n-D HCMs owning any desired number of positive LEs with a lower computation complexity. Meanwhile, ergodicity property of the obtained HCM is more complex.

The rest of this paper is organized as follows. Section II briefly reviews n-D Cat map and explores its properties. Section III presents the proposed method of constructing n-D Cat maps, and Section IV provides two representative examples of them. Section V further evaluates performance of the proposed method and the last section concludes this paper.

II. n-D Cat Map and Its Dynamic Property

The n-D discrete Cat map can be defined as

$$\mathbf{x}(t+1) = (\mathbf{C} \cdot \mathbf{x}(t)) \mod N \tag{1}$$

TABLE I
Descriptions of Important Notations

Notation	Description
n	the Cat map dimension
N	the number of finite states
$\mathbf{C}$	an n-D Cat matrix
$c_{i,j}$	an element of $\mathbf{C}$
$\mathbf{x}(t)$	the observation state of Cat map in time t
LE_j	the j-th Lyapunv exponent of Cat map
λ_j	the j-th eigenvalue of $\mathbf{C}$
$\mathbf{J}(\mathbf{x}(t))$	the Jacobian matrix of chaotic system with $\mathbf{x}(t)$
$\mathbf{I}$	an identity matrix
$\mathbf{C}'$	the parametric 2-D Cat matrix
p, q	two parameters of $\mathbf{C}'$
$\mathbf{a}$	a pseudo-random binary sequence
$\mathbf{b}$	a pseudo-random binary sequence
$\mathbf{h}$	a pseudo-random integer sequence
$\mathbf{g}$	a pseudo-random integer sequence
K	the number of positive LEs
$\#_{SLCs}$	the total number of spatial location configuration
P_{SLCs}	the parameter space of spatial location configuration
$\#_{MECs}$	the total number of matrix entity configuration
P_{MECs}	the parameter space of matrix entity configuration
$P_{\mathbf{C}}$	the whole parameter space of constructing $\mathbf{C}$

where $\mathbf{x}(t) = \{x_1(t), x_2(t), \ldots, x_n(t)\}^T \in \mathbb{N}^{n\times 1}$, N is the finite number of states in the range spanned by the components of $\mathbf{x}(t)$, and

$$\mathbf{C} = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix} \tag{2}$$

is the corresponding *Cat matrix*, which satisfies $c_{i,j} \in \mathbb{N}$ and $\det(\mathbf{C}) = 1$ [25], [29], [32]. When the elements of $\mathbf{x}(t)$ are real numbers, (1) is an n-D general Cat map. In the rest of this paper, we use the discrete Cat map to demonstrate the properties of the Cat map. These properties also hold for the general Cat map. To facilitate description of this paper, some important notations are defined in Table I.

As shown in Propositions 1 and 2, there is simple mapping relation between LEs of n-D Cat map (1) and eigenvalues of the corresponding Cat matrix. In addition, summation of the n LEs is equal to zero. Proposition 3 describes a property of two eigenvalues of a special type of 2-D Cat matrix.

Proposition 1: Let $\mathrm{LE}_1, \mathrm{LE}_2, \ldots, \mathrm{LE}_n$ denote the n LEs of the n-D Cat map given in (1), one has

$$\mathrm{LE}_j = \ln(\lambda_j) \text{ for } 1 \leq j \leq n \tag{3}$$

where $\lambda_1, \lambda_2, \ldots, \lambda_n$ represent the n eigenvalues of the corresponding Cat matrix, respectively.

Proof: For an n-D discrete-time chaotic system, $\mathbf{x}(t+1) = F(\mathbf{x}(t))$, it has n LEs because its orbits have n independent initial displacement directions. Suppose $\mathbf{J}(\mathbf{x}(t))$ is the Jacobian matrix of $F(\mathbf{x})$ with the observation state $\mathbf{x}(t)$ and $\lambda_1^{\mathbf{x}(t)} \sim \lambda_n^{\mathbf{x}(t)}$ are the n eigenvalues of $\mathbf{J}(\mathbf{x}(t))$. From definition of LE (e.g., [43, eq. (1)]) and its calculation method

(e.g., [6, eq. (8)]), one can obtain the n LEs of the system

$$\mathrm{LE}_j = \lim_{t\to\infty} \frac{1}{t}\sum_{i=0}^{t-1} \ln\left(\lambda_j^{\mathbf{x}(t)}\right)$$

where $j = 1, \ldots, n$. As for the n-D Cat map (1), its Jacobian matrix is not related to the observation state $\mathbf{x}(t)$, which means that $\mathbf{J}(\mathbf{x}(0)) = \mathbf{J}(\mathbf{x}(1)) = \cdots = \mathbf{J}(\mathbf{x}(t-1)) = \mathbf{C}$. So, one has $\lambda_j^{\mathbf{x}(0)} = \lambda_j^{\mathbf{x}(1)} = \cdots = \lambda_j^{\mathbf{x}(t-1)} = \lambda_j$ for any j. Then, one can get

$$\mathrm{LE}_j = \lim_{t\to\infty} \frac{1}{t}\sum_{i=0}^{t-1} \ln(\lambda_j) = \ln(\lambda_j).$$

■

Proposition 2: The n LEs of n-D Cat map (1) satisfy

$$\sum_{j=1}^{n} \exp(\mathrm{LE}_j) = \sum_{j=1}^{n} c_{jj} \tag{4}$$

and

$$\sum_{j=1}^{n} \mathrm{LE}_j = 0 \tag{5}$$

where c_{jj} is the diagonal element of the Cat matrix (2).

Proof: The characteristic equation of the n-D Cat matrix $\mathbf{C}$ is

$$\begin{aligned}\det(\lambda\mathbf{I}-\mathbf{C}) &= \begin{vmatrix} \lambda - c_{11} & -c_{12} & \cdots & -c_{1n} \\ -c_{21} & \lambda - c_{22} & \cdots & -c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -c_{n1} & -c_{n2} & \cdots & \lambda - c_{nn} \end{vmatrix} \\ &= \lambda^n + d_{n-1}\lambda^{n-1} + \cdots + d_1\lambda + d_0 \\ &= 0\end{aligned} \tag{6}$$

where d_i is the ith order polynomial coefficient of $\det(\lambda\mathbf{I}-\mathbf{C})$. According to definition of determinant, the right part of (6) can be represented as addition of determinant of 2^n matrices, whose every entry is composed by one element in set $\{\lambda\}\bigcup\{-c_{i,j}\}_{i=1,j=1}^{n,n}$. Among them, there are n ones containing item λ^{n-1}

$$\begin{vmatrix} -c_{11} & 0 & \cdots & 0 \\ -c_{21} & \lambda & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -c_{n1} & 0 & \cdots & \lambda \end{vmatrix}, \ldots, \begin{vmatrix} \lambda & 0 & \cdots & -c_{1n} \\ 0 & \lambda & \cdots & -c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -c_{nn} \end{vmatrix}.$$

Summation of the above n determinants is

$$(-c_{11} - c_{22} - \cdots - c_{nn})\lambda^{n-1} = -\sum_{j=1}^{n} c_{jj}\lambda^{n-1}.$$

So, $d_{n-1} = -\sum_{j=1}^{n} c_{jj}$. The constant item of the determinant (6) is

$$\begin{aligned}\begin{vmatrix} -c_{11} & -c_{12} & \cdots & -c_{1n} \\ -c_{21} & -c_{22} & \cdots & -c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -c_{n1} & -c_{n2} & \cdots & -c_{nn} \end{vmatrix} &= (-1)^n \det(\mathbf{C}) \\ &= (-1)^n.\end{aligned}$$

Then, $d_0 = (-1)^n$. Using Vieta's formulas shown in [44], one has

$$\sum_{j=1}^{n} \lambda_j = -d_{n-1} = \sum_{j=1}^{n} c_{jj} \tag{7}$$

and

$$\prod_{j=1}^{n} \lambda_j = (-1)^n d_0 = 1 \tag{8}$$

where $\lambda_1, \lambda_2, \ldots, \lambda_n$ are n roots of (6), namely the n eigenvalues of Cat matrix $\mathbf{C}$.

From Proposition 1, one can get $\lambda_j = \exp(\mathrm{LE}_j)$ for $j = 1 \sim n$. Substituting the above equation into (7) and (8), one can obtain

$$\sum_{j=1}^{n} \exp(\mathrm{LE}_j) = \sum_{j=1}^{n} c_{jj}$$

and

$$\prod_{j=1}^{n} \exp(\mathrm{LE}_i) = \exp\left(\sum_{j=1}^{n} \mathrm{LE}_j\right) = 1$$

respectively. Then, one has $\sum_{j=1}^{n} \mathrm{LE}_j = 0$, which completes proof of this proposition. ■

Proposition 3: Two eigenvalues of parametric 2-D Cat matrix

$$\mathbf{C}' = \begin{pmatrix} p\cdot q + 1 & p \\ q & 1 \end{pmatrix} \tag{9}$$

λ_1 and λ_2, satisfy

$$\ln(|\lambda_1|)\cdot\ln(|\lambda_2|) < 0$$

if

$$(p\cdot q) \notin \{0, -4\}. \tag{10}$$

Proof: The characteristic equation of $\mathbf{C}'$ is

$$\begin{aligned}\det(\lambda\mathbf{I}-\mathbf{C}') &= \begin{vmatrix} \lambda - (p\cdot q + 1) & -p \\ -q & \lambda - 1 \end{vmatrix} \\ &= \lambda^2 - (p\cdot q + 2)\lambda + 1 = 0.\end{aligned} \tag{11}$$

The root discriminant of (11) is $\Delta = (p\cdot q+2)^2 - 4$. If $(p\cdot q) \notin \{0, -4\}$, $\Delta \neq 0$. This means that (11) has two different roots, namely, $\lambda_1 \neq \lambda_2$. From (8), one has $\lambda_1 \cdot \lambda_2 = 1$. Thus, one can get $|\lambda_1| < 1$, $|\lambda_2| > 1$ or $|\lambda_2| < 1$, $|\lambda_1| > 1$, i.e., $\ln(|\lambda_1|)\cdot\ln(|\lambda_2|) < 0$, which completes proof of this proposition. ■

III. Methodology

This section introduces the proposed method of constructing n-D HCMs with a desired number of positive LEs. First, two basic n-D Cat matrices are constructed from the parametric 2-D Cat matrix. Then, the final n-D Cat matrix is generated by doing similarity transformation on one basic Cat matrix with the other.

A. Constructing Basic n-D Cat Matrix From $(n-2)$-D One

First, we introduce Proposition 4 that constructs a Cat matrix from two Cat matrices with lower dimensions.

Proposition 4: Let the $\mathbf{C}_1$ and $\mathbf{C}_2$ denote i-D Cat matrix and $(n-i)$-D Cat matrix, respectively. If at least one of $\mathbf{M}_1$ and $\mathbf{M}_2$ is zero matrix, block matrix

$$\mathbf{C} = \begin{pmatrix} \mathbf{C}_1 & \mathbf{M}_1 \\ \mathbf{M}_2 & \mathbf{C}_2 \end{pmatrix} \tag{12}$$

is an n-D Cat matrix and its eigenvalues are composed by that of $\mathbf{C}_1$ and $\mathbf{C}_2$, where $n > i$, $\mathbf{M}_1$ and $\mathbf{M}_2$ are $i \times (n-i)$ matrix and $(n-i) \times i$ matrix, respectively.

Proof: Since $\mathbf{C}_1$ and $\mathbf{C}_2$ are two Cat matrices, one has $\det(\mathbf{C}_1) = 1$ and $\det(\mathbf{C}_2) = 1$. As at least one of $\mathbf{M}_1$ and $\mathbf{M}_2$ is zero matrix, then $|\mathbf{M}_1||\mathbf{M}_2| = 0$, and $\det(\mathbf{C}) = |\mathbf{C}_1||\mathbf{C}_2| - |\mathbf{M}_1||\mathbf{M}_2| = 1$. Thus, $\mathbf{C}$ is an n-D Cat matrix, and its eigenvalues are the eigenvalues of its submatrices in the main diagonal line, $\mathbf{C}_1$ and $\mathbf{C}_2$. ■

Referring to Proposition 4, one can construct an n-D Cat matrix (12) from an $(n-2)$-D Cat matrix by one of the following two types of setting.

1) $\mathbf{C}_1 = \mathbf{C}'$, where p and q are random integers in (9), $\mathbf{C}_2$ is the $(n-2)$-D Cat matrix.
2) $\mathbf{C}_2 = \mathbf{C}'$, where p and q are random integers in (9), $\mathbf{C}_1$ is the $(n-2)$-D Cat matrix.

In both cases, at least one of $\mathbf{M}_1$ and $\mathbf{M}_2$ in Proposition 4 is zero matrix.

As shown in Proposition 3, $\mathbf{C}'$ in (9) has one eigenvalue of absolute value larger than 1 if $(p \cdot q) \notin \{0, -4\}$. So, one can assure that the obtained n-D Cat matrix has one more eigenvalue of absolute value larger than 1 than the $(n-2)$-D Cat matrix.

B. Constructing n-D Cat Map With $\lfloor n/2 \rfloor$ Positive LEs

Using Proposition 4, one can construct basic n-D Cat matrix by iteratively expanding an initial matrix with a 2×2 matrix. The construction procedure is described as follows.

1) *Step 1:* Set the initial matrix as a 1×1 special matrix if n is odd, otherwise set it as the parametric 2-D Cat matrix given in Proposition 3.
2) *Step 2:* Place the initial matrix and another parametric 2-D Cat matrix in the main diagonal of a 2×2 block matrix (12). To increase the parameter space of the obtained Cat matrix, the locations of the two matrices are assigned randomly.
3) *Step 3:* As for the other two matrix blocks in the antidiagonal direction, randomly select one and set it of fixed value zero. Then, elements of the other matrix block are assigned with any integer randomly.
4) *Step 4:* Set the current composite matrix as the initial matrix.
5) *Step 5:* Repeat *step* 2 through *step* 4 $\lfloor (n-1)/2 \rfloor - 1$ times.

Algorithm 1 presents the pseudocode of the function operating the above procedure, HCMF($\mathbf{a}$, $\mathbf{b}$, $\mathbf{h}$, $\mathbf{g}$, n), where $\mathbf{a} = \{a_i\}_{i=1}^{\lfloor (n-1)/2 \rfloor}$ and $\mathbf{b} = \{b_i\}_{i=1}^{\lfloor (n-1)/2 \rfloor}$ are pseudo-random binary sequences, $\mathbf{h} = \{h_i\}_{i=1}^{\lfloor n/2 \rfloor \cdot 2}$ and $\mathbf{g} = \{g_i\}_{i=1}^{\lfloor n^2/2 \rfloor - \lfloor n/2 \rfloor \cdot 2}$ are pseudo-random integer sequences. To obey the requirement (10), the elements of $\mathbf{h}$ satisfy $(h_{2i-1} \cdot h_{2i}) \notin \{0, -4\}$ for $i = 1 \sim \lfloor n/2 \rfloor$.

Algorithm 1 Algorithm for Generating a Basic n-D Cat Matrix

function HCMF($\mathbf{a}$, $\mathbf{b}$, $\mathbf{h}$, $\mathbf{g}$, n)
  $c = ((n+1) \mod 2) + 1$;
  if $c = 1$ **then**
    $\mathbf{C} = [1]$
  else
    $\mathbf{C} = \mathbf{C}'$, where p, q are selected from $\mathbf{h}$.
  end if
  for $i = 1$ to $\lfloor (n-1)/2 \rfloor$ **do**
    Initialize a $\mathbf{C}'$, where p, q are fetched from $\mathbf{h}$.
    if $a_i = 1$ **then**
      $\mathbf{C}_1 = \mathbf{C}$, $\mathbf{C}_2 = \mathbf{C}'$,
      $\mathbf{M}_1 \in \mathbb{N}^{(2(i-1)+c) \times 2}$, $\mathbf{M}_2 \in \mathbb{N}^{2 \times (2(i-1)+c)}$.
    else
      $\mathbf{C}_1 = \mathbf{C}'$, $\mathbf{C}_2 = \mathbf{C}$,
      $\mathbf{M}_1 \in \mathbb{N}^{2 \times (2(i-1)+c)}$, $\mathbf{M}_2 \in \mathbb{N}^{(2(i-1)+c) \times 2}$.
    end if
    if $b_i = 1$ **then**
      $\mathbf{M}_1 = \mathbf{0}$, elements of $\mathbf{M}_2$ are fetched from $\mathbf{g}$.
    else
      $\mathbf{M}_2 = \mathbf{0}$, elements of $\mathbf{M}_1$ are fetched from $\mathbf{g}$.
    end if
    $\mathbf{C} = \begin{pmatrix} \mathbf{C}_1 & \mathbf{M}_1 \\ \mathbf{M}_2 & \mathbf{C}_2 \end{pmatrix}$.
  end for
  return $\mathbf{C}$.
end function

Fig. 1 shows an example of generating a basic 5-D Cat matrix using Algorithm 1. The parameters are set as follows: $\mathbf{a} = \{1, 0\}$, $\mathbf{b} = \{0, 1\}$, $\mathbf{h} = \{h_i\}_{i=1}^{4}$, and $\mathbf{g} = \{g_i\}_{i=1}^{8}$. The detailed procedures can be described as follows.

1) As $c = 1$, set the initial matrix $\mathbf{C} = [1]$, which is shown in Fig. 1(a).
2) The following four steps are performed to generate the 3-D Cat matrix shown in Fig. 1(b): a) initialize a 2-D Cat matrix $\mathbf{C}'$ in (9) with $p = h_1$ and $q = h_2$; b) set $\mathbf{C}_1 = \mathbf{C}$ and $\mathbf{C}_2 = \mathbf{C}'$ as $a_1 = 1$; c) set $\mathbf{M}_2 = \mathbf{0}$ and use the elements of $\mathbf{g}$ to initialize $\mathbf{M}_1$ as $b_1 = 0$; and d) construct the 3-D Cat matrix using (12).
3) The following four steps are performed to generate the basic 5-D Cat matrix shown in Fig. 1(c): a) initialize a 2-D Cat matrix $\mathbf{C}'$ in (9) with $p = h_3$ and $q = h_4$; b) set $\mathbf{C}_1 = \mathbf{C}'$ and $\mathbf{C}_2 = \mathbf{C}$ as $a_2 = 0$; c) set $\mathbf{M}_1 = \mathbf{0}$ and use the elements of $\mathbf{g}$ to initialize $\mathbf{M}_2$ as $b_2 = 1$; and d) generate the basic 5-D Cat matrix using (12).

As zero matrices are used in the generation procedure, the obtained Cat matrix using Algorithm 1 has blocks of fixed value zero, which can be observed from Fig. 1(c). To further enhance dynamics of the constructed n-D Cat map, we use the following two steps to construct the final n-D Cat matrix: 1) construct two basic n-D Cat matrices, $\dot{\mathbf{C}}$ and $\ddot{\mathbf{C}}$, by running Algorithm 1 twice with different inputs and 2) generate the final n-D Cat matrix $\mathbf{C}$ by operating similarity transformation

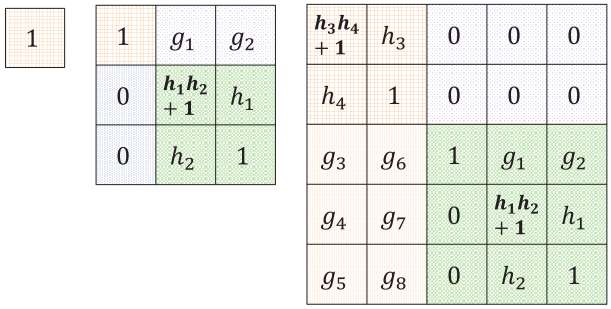


Fig. 1. Example of generating a basic 5-D Cat matrix using Algorithm 1. (a) 1-D Cat matrix. (b) 3-D Cat matrix. (c) Obtained basic 5-D Cat matrix.

on $\dot{\mathbf{C}}$ with $\ddot{\mathbf{C}}$, namely

$$\mathbf{C} = \ddot{\mathbf{C}} \cdot \dot{\mathbf{C}} \cdot \ddot{\mathbf{C}}^{-1}. \tag{13}$$

As the proposed method can construct n-D Cat map with $\lfloor n/2 \rfloor$ positive LEs, one can get the number of positive LEs

$$K = \begin{cases} n/2, & \text{if} \quad n \mod 2 = 0 \\ (n-1)/2, & \text{if} \quad n \mod 2 = 1. \end{cases} \tag{14}$$

From Proposition 2, one can assure that the summation of all the n LEs of the obtained n-D Cat map is equal to zero. As its LEs are dependent on the eigenvalues of the used parametric 2-D Cat matrix $\mathbf{C}'$ in (9), the number of positive LEs can be deduced via Proposition 3, but their magnitude cannot be set a priori.

C. Parameter Space of the Obtained HCM

The proposed method has two kinds of parameters in constructing an n-D Cat matrix: 1) spatial location configuration (SLC) and 2) matrix entity configuration (MEC). The elements in **a** and **b** are SLCs while those in **h** and **g** are MECs. A binary element in **a** controls the position of a newly added parametric 2-D Cat matrix $\mathbf{C}'$ while that in **b** indicates the position of a newly added nonzero submatrix in (12). There are total $\lfloor (n-1)/2 \rfloor$ iterations in constructing a basic n-D Cat matrix, thus **a** and **b** both has $\lfloor (n-1)/2 \rfloor$ binary elements. Then the total number of SLCs to construct two basic n-D Cat matrices is $\#_{\text{SLCs}} = 4\lfloor (n-1)/2 \rfloor$. As each SLC has two possible values, the parameter space of SLCs is

$$P_{\text{SLCs}} = 2^{\#_{\text{SLCs}}} = 2^{4\lfloor (n-1)/2 \rfloor}.$$

Sequences **h** and **g** contain the matrix entities of each newly added $\mathbf{C}'$ and nonzero submatrix, respectively. As shown in Algorithm 1, constructing a basic n-D Cat matrix needs $\lfloor n/2 \rfloor$ $\mathbf{C}'$s, and every one has 2 MECs. So, **h** has $2\lfloor n/2 \rfloor$ elements. In every expansion, the same number of determined entities and MECs are used. Constructing a basic n-D Cat matrix needs $\lfloor n^2/2 \rfloor$ MECs. Thus, the number of elements in **g** is $\lfloor n^2/2 \rfloor - 2\lfloor n/2 \rfloor$, and the total number of MECs in constructing two basic n-D Cat matrices is $\#_{\text{MECs}} = 2\lfloor n^2/2 \rfloor$. For simplicity of calculation, we assume that all MECs are randomly selected from M possible values. Then the parameter space of MECs is $P_{\text{MECs}} = M^{\#_{\text{MECs}}} = M^{2\lfloor n^2/2 \rfloor}$.

TABLE II
PARAMETER SPACES OF CONSTRUCTING AN n-D CAT MATRIX **C** WITH DIFFERENT DIMENSIONS

Dimension	P_{SLCs}	P_{MECs}	$P_{\mathbf{C}}$
3	16	M^8	$16M^8$
4	16	M^{16}	$16M^{16}$
5	256	M^{24}	$256M^{24}$
6	256	M^{36}	$256M^{36}$
⋮	⋮	⋮	⋮
n	$2^{4\lfloor (n-1)/2 \rfloor}$	$M^{2\lfloor n^2/2 \rfloor}$	$2^{4\lfloor (n-1)/2 \rfloor} M^{2\lfloor n^2/2 \rfloor}$

Because SLC and MEC are independent, the whole parameter space of constructing an n-D Cat matrix **C** is the multiplication of the parameter spaces of SLCs and MECs, namely

$$\begin{aligned} P_{\mathbf{C}} &= P_{\text{SLCs}} \times P_{\text{MECs}} \\ &= 2^{4\lfloor (n-1)/2 \rfloor} M^{2\lfloor n^2/2 \rfloor}. \end{aligned}$$

Table II lists the parameter spaces of constructing an n-D Cat matrix with different dimensions n.

IV. TWO ILLUSTRATIVE EXAMPLES

This section provides two n-D HCMs with desired number of positive LEs using the proposed method: 1) a 5-D HCM with two positive LEs and 2) a 10-D HCM with five positive LEs.

A. 5-D HCM With Two Positive LEs

In this example of generating the 5-D HCM, a typical setting was used to generate the first basic 5-D Cat matrix: $\mathbf{a} = \{1, 0\}$, $\mathbf{b} = \{0, 1\}$, $\mathbf{h} = \{2, 1, 1, 1\}$, and $\mathbf{g} = \{2, 1, 1, 1, 1, 2, 1, 2\}$. Starting with 1-D Cat matrix $\mathbf{C} = [1]$, run Algorithm 1 and get

$$\dot{\mathbf{C}} = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 2 & 1 \\ 1 & 1 & 0 & 3 & 2 \\ 1 & 2 & 0 & 1 & 1 \end{pmatrix}.$$

To get the second basic 5-D Cat matrix, we set $\mathbf{a} = \{1, 1\}$, $\mathbf{b} = \{0, 1\}$, $\mathbf{h} = \{2, 2, 2, 1\}$, and $\mathbf{g} = \{2, 1, 2, 2, 2, 1, 1, 1\}$. Starting with 1-D Cat matrix $\mathbf{C} = [1]$ also, we obtain

$$\ddot{\mathbf{C}} = \begin{pmatrix} 1 & 2 & 1 & 0 & 0 \\ 0 & 5 & 2 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 2 & 2 & 1 & 3 & 2 \\ 2 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

The final 5-D Cat matrix **C** can be generated by (13)

$$\mathbf{C} = \begin{pmatrix} 5 & 2 & -8 & 1 & -1 \\ 7 & 3 & -11 & 2 & -2 \\ 3 & 1 & -4 & 1 & -1 \\ 2 & 12 & -30 & 4 & 1 \\ 4 & 6 & -17 & 2 & 0 \end{pmatrix}.$$

The five LEs of the constructed 5-D HCM composed with the above Cat matrix are $\mathrm{LE}_1 = 1.3170$, $\mathrm{LE}_2 = 0.9624$, $\mathrm{LE}_3 = 0$, $\mathrm{LE}_4 = -0.9624$, and $\mathrm{LE}_5 = -1.3170$. There are two positive LEs, and it is easy to verify that

$$\sum_{j=1}^{5} \exp(\mathrm{LE}_j) = 8 = \sum_{j=1}^{5} \mathbf{C}_{jj}^{5}$$

and $\sum_{j=1}^{5} \mathrm{LE}_j = 0$, which agree with the theoretical expectations.

B. 10-D HCM With Five Positive LEs

When $n = 10$, the input parameters for generating the first basic 10-D Cat matrix are set as follows: $\mathbf{a} = \{1, 0, 0, 1\}$, $\mathbf{b} = \{0, 1, 1, 0\}$, elements in $\mathbf{h} = \{h_i\}_{i=1}^{10}$ and $\mathbf{g} = \{g_i\}_{i=1}^{40}$ are randomly selected from the set $\{1, 2\}$. Run Algorithm 1 and get

$$\dot{\mathbf{C}} = \begin{pmatrix} 3 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 \\ 2 & 2 & 5 & 2 & 0 & 0 & 0 & 0 & 2 & 1 \\ 2 & 1 & 2 & 1 & 0 & 0 & 0 & 0 & 1 & 2 \\ 2 & 2 & 1 & 1 & 3 & 2 & 1 & 1 & 2 & 2 \\ 2 & 1 & 2 & 1 & 1 & 1 & 2 & 1 & 1 & 1 \\ 2 & 1 & 1 & 1 & 0 & 0 & 5 & 2 & 2 & 2 \\ 2 & 1 & 1 & 2 & 0 & 0 & 2 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

As for the second basic 10-D Cat matrix, the input parameters are set as follows: $\mathbf{a} = \{1, 0, 1, 0\}$, $\mathbf{b} = \{1, 1, 1, 0\}$, elements of $\mathbf{h} = \{h_i\}_{i=1}^{10}$ and $\mathbf{g} = \{g_i\}_{i=1}^{40}$ are also randomly selected from the set $\{1, 2\}$. Then, we obtain

$$\ddot{\mathbf{C}} = \begin{pmatrix} 3 & 2 & 1 & 1 & 1 & 2 & 1 & 2 & 2 & 1 \\ 1 & 1 & 1 & 2 & 2 & 1 & 1 & 2 & 2 & 2 \\ 0 & 0 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 3 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 & 2 & 1 & 3 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 & 1 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 & 3 & 2 \\ 0 & 0 & 2 & 1 & 1 & 2 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

The final 10-D Cat matrix is obtained by performing (13) and get

$$\mathbf{C} = \begin{pmatrix} 9 & 0 & -104 & 192 & 41 & -75 & 34 & -60 & -8 & 31 \\ 7 & 1 & -68 & 133 & 30 & -57 & 31 & -54 & -6 & 26 \\ 1 & 5 & 150 & -219 & -38 & 51 & 13 & -19 & 1 & -8 \\ 1 & 3 & 82 & -117 & -20 & 26 & 9 & -14 & 0 & -3 \\ 2 & 8 & 178 & -265 & -43 & 59 & 19 & -28 & -1 & -5 \\ 3 & 5 & 81 & -111 & -16 & 19 & 17 & -28 & -3 & 4 \\ 7 & 1 & -79 & 148 & 31 & -58 & 27 & -42 & -7 & 23 \\ 5 & 1 & -28 & 63 & 14 & -30 & 20 & -30 & -4 & 13 \\ 7 & -1 & -99 & 182 & 39 & -70 & 30 & -52 & -5 & 28 \\ 5 & 1 & -8 & 34 & 10 & -24 & 22 & -35 & -3 & 13 \end{pmatrix}.$$

The 10 LEs of this 10-D HCM are $\mathrm{LE}_1 = 1.7627$, $\mathrm{LE}_2 = 1.7627$, $\mathrm{LE}_3 = 1.3170$, $\mathrm{LE}_4 = 1.3170$, $\mathrm{LE}_5 = 1.3169$, $\mathrm{LE}_6 = -1.7628$, $\mathrm{LE}_7 = -1.7627$, $\mathrm{LE}_8 = -1.3173$, $\mathrm{LE}_9 = -1.3168 + 0.0003i$, and $\mathrm{LE}_{10} = -1.3168 - 0.0003i$. As expected, the number of positive LEs is five. It is easy to calculate that

$$\sum_{j=1}^{10} \exp(\mathrm{LE}_j) = 24 = \sum_{j=1}^{10} \mathbf{C}_{jj}$$

and

$$\sum_{j=1}^{10} \mathrm{LE}_j = 3.8177 \times e^{-11} \approx 0.$$

The above approximation is caused by finite precision of digital computer. So, the 10-D HCM still agrees with the expectations.

To verify the randomness of the obtained 10-D HCM, we set the number of finite states $N = 512$ and initial value $\mathbf{x}(0) = \mathbf{1}_{10\times 1}$ in (1). Fig. 2 plots the distributions of the generated outputs projected in different 3-D phase planes. As can be seen in Fig. 2, the generated trajectory is randomly distributed in the entire 3-D phase planes, which demonstrates the outputs of the 10-D HCM have good randomness.

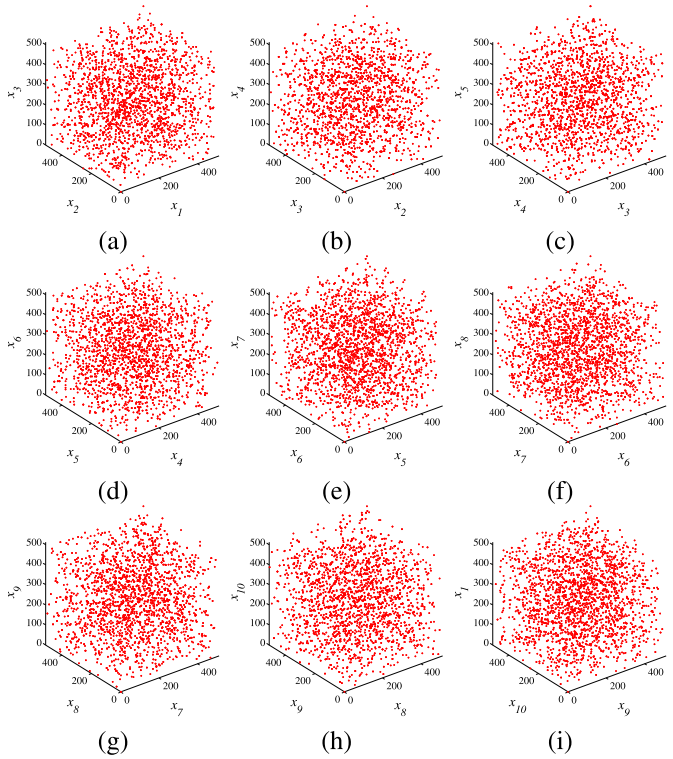


Fig. 2. Trajectory projections of the constructed 10-D HCM with five positive LEs. (a) $x_1 - x_2 - x_3$ plane. (b) $x_2 - x_3 - x_4$ plane. (c) $x_3 - x_4 - x_5$ plane. (d) $x_4 - x_5 - x_6$ plane. (e) $x_5 - x_6 - x_7$ plane. (f) $x_6 - x_7 - x_8$ plane. (g) $x_7 - x_8 - x_9$ plane. (h) $x_8 - x_9 - x_{10}$ plane. (i) $x_9 - x_{10} - x_1$ plane.

V. Performance Evaluation

This section evaluates the performance of the proposed method from four aspects: 1) LE; 2) time complexity; 3) information entropy; and 4) correlation dimension. Some typical

TABLE III
AVERAGE NUMBER OF POSITIVE LEs OF n-D CAT MAPS GENERATED BY DIFFERENT METHODS

Dimension	n-D Cat map generation methods				
n	Tang's	Falcioni's	Nance's	Wu's	Proposed
3	1.025	1	1	0.75	1
4	1.275	1.1375	1	1.15	2
5	2	1.1625	1	1.975	2
6	2.4125	1.3344	1	2.7344	3
7	2.9063	1.4921	-	3.6078	3
8	3.5781	1.5789	-	4.6070	4
9	4.2285	1.8445	-	5.6512	4
10	4.6594	2.0002	-	6.6377	5
11	5.1815	2.2209	-	7.5915	5
12	5.7666	2.4559	-	8.4290	6
13	6.3348	2.6714	-	-	6
14	6.7812	2.8990	-	-	7
15	7.2893	3.1344	-	-	7
16	7.9066	3.3548	-	-	8

Cat map generation methods are used as comparison methods: Lian *et al.*'s method [42], Chen *et al.*'s method [25], Liu *et al.*'s method [37], Pan and Li's method [38], Tang and Tang's method [45], Falcioni *et al.*'s method [39], Nance's method [40], and Wu *et al.*'s method [41]. The former four ones are fixed dimensional Cat map generation methods while the latter four ones are generation methods of variable dimensional Cat map. For Wu *et al.*'s method [41], we set the spatial configuration parameters in **I** and **J** as 2, and randomly determine the matrix entries parameters in **P** and **Q**.

A. Lyapunov Exponent

The number of positive LEs is a key factor to measure dynamics complexity of a dynamic system. Based on this point, we did a large number of experiments to compare the proposed method with Tang's, Falcioni's, Nance's and Wu's methods in terms of the number of positive LEs. We found the proposed method owns obvious superiority in this aspect. Here, we list a typical example: $M = 2$ (MECs are restricted to $\{1, 2\}$) and dimension n is selected in the scope $\{3, 4, \ldots, 16\}$. Table III lists the average number of positive LEs for different generation methods under different dimensions n. As can be seen, the proposed method can generate n-D Cat maps with $\lfloor n/2 \rfloor$ positive LEs. It allows users to generate n-D Cat maps with a specified and desired number of positive LEs. Although Tang's and Wu's methods can also generate a large number of positive LEs, their quantities cannot be controlled. In contract, Falcioni's and Nance's methods can only generate few positive LEs.

Furthermore, Nance's and Wu's methods require a large number of multiplications and additions in generating n-D Cat matrix. When dimension $n \geq 7$ in Nance's method and $n \geq 13$ in Wu's method, some entities of the generated Cat matrix are too large to be correctly represented by commonly used data formats, which lead to inaccurate experimental results. Thus, we only display the experimental results for dimension $n \leq 6$ in Nance's method and $n \leq 12$ in Wu's method.

TABLE IV
TIME COMPLEXITY OF DIFFERENT n-D CAT MAP GENERATION METHODS

	n-D Cat map generation methods				
	Tang's	Falcioni's	Nance's	Wu's	Proposed
5	1135	22	746	232	129
10	44045	150	22300	3042	1010
50	$50^{4.8174}$	$50^{2.4785}$	$50^{4.5948}$	$50^{3.6558}$	$50^{3.001}$
100	$100^{4.8473}$	$100^{2.5528}$	$100^{4.6532}$	$100^{3.7033}$	$100^{3.000}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
n	$O(n^5)$	$O(n^3)$	$O(n^5)$	$O(n^4)$	$O(n^3)$

B. Time Complexity

The previous methods of generating n-D Cat maps require complicate operations and the costed time complexity is very high. This becomes a bottleneck when Cat maps are used in real applications, especially in real-time scenarios. In Tang's, Falcioni's, Nance's, Wu's methods and the proposed method, there are four kinds of involved operations: matrix entity addition, matrix entity multiplication, matrix multiplication, and matrix determinant. The computation complexity of matrix multiplication for two $k \times k$ matrices is of order $O(k^{2.373})$ [46] and that of matrix determinant of size $k \times k$ is of order $O(k^{2.376})$ [47]. We consider them as $O(k^3)$ for simplicity. In Tang's, Falcioni's, Nance's, and Wu's methods, the numbers of matrix entity additions are $n(n-1)/2$, $(n/2)^2$, 0, and $2(n-1)$, respectively. Their computation complexities caused by matrix multiplication and matrix determinant are $(n(n-1)/2 - 1)O(n^3)$, $O((n/2)^3)$, $\sum_{k=3}^{n}(k-1)O(k^3)$ and $\sum_{k=2}^{n} O(k^3)$, respectively. Thus, the total time complexity of the four generation methods are

$$\begin{aligned} T_{\text{Tang's}} &= n(n-1)/2 + (n(n-1)/2 - 1)O\left(n^3\right) \\ T_{\text{Falcioni's}} &= (n/2)^2 + O\left((n/2)^3\right) \\ T_{\text{Nance's}} &= \sum_{k=3}^{n}(k-1)O\left(k^3\right) \\ T_{\text{Wu's}} &= 2(n-1) + \sum_{k=2}^{n} O\left(k^3\right) \end{aligned}$$

respectively. As for the proposed method, the time complexities of matrix entity addition, matrix entity multiplication, and matrix multiplication are $\lfloor n/2 \rfloor$, $\lfloor n/2 \rfloor$, and $O(n^3)$, respectively. So, its time complexity is

$$T_{\text{Proposed}} = 2\lfloor n/2 \rfloor + O\left(n^3\right).$$

Table IV compares the time complexity of different methods. As can be seen, the proposed method has the time complexity of order $O(n^3)$, which has the same order of magnitude as Falcioni's method and is less than Wu's method by one order of magnitude, and is less than Tang's and Nance's methods by two orders of magnitude.

TABLE V
MAXIMUM INFORMATION ENTROPY VALUES OF 3-D CAT MAPS GENERATED BY DIFFERENT METHODS WITH VARIOUS NUMBER OF FINITE STATES

	The number of finite states N												
	3	4	5	6	7	8	9	10	11	12	13	14	15
Lian's	3.6972	3.8069	4.9540	6.5072	5.8328	4.8073	5.2854	7.7615	7.0553	7.5078	7.5157	8.6402	8.6546
Chen's	3.6972	3.8069	4.9540	6.5072	5.8328	4.8073	5.2854	7.7615	7.0553	7.5078	7.5157	8.6402	8.6546
Liu's	3.5819	3.5846	4.9067	5.1699	5.8073	4.5850	5.1699	5.9069	7.0444	6.1699	7.5078	7.3923	7.4919
Pan's	3.6972	3.5846	4.9540	6.2848	5.8328	4.5850	5.2854	7.5391	7.0553	7.2854	7.5157	7.8329	8.6546
Tang's	3.6972	3.8069	4.9540	6.5072	5.8328	4.8073	5.2854	7.7615	7.0553	7.5078	7.5157	8.6402	8.6546
Falcioni's	3.5819	3.5846	4.9067	5.1699	5.8073	4.5850	5.1699	5.9069	7.0444	6.1699	7.5078	7.3923	7.4919
Nance's	3.6972	3.5846	4.9540	5.7004	5.8328	4.5850	5.2854	6.9542	7.0553	7.2854	7.5157	7.8329	8.6546
Wu's	3.6972	5.7704	6.7604	7.6051	8.2817	8.8732	9.3931	9.8513	10.3036	10.6556	11.0092	11.3338	11.6377
Proposed	4.6267	5.8621	6.8455	7.6563	8.3295	8.9173	9.4358	9.8978	10.3147	10.6978	11.0477	11.3722	11.6738
$H_{\max}$	4.7549	6.0000	6.9658	7.7549	8.4221	9.0000	9.5098	9.9658	10.3783	10.7549	11.1013	11.4221	11.7207

C. Information Entropy

Information entropy is a widely used measure to test randomness of a sequence of data, which is defined as

$$H = -\sum_{i=1}^{L} \Pr(i) \log_2 \Pr(i)$$

where L is the number of possible values and $\Pr(i)$ is the probability of the ith possible value. For the n-D Cat map defined in (1), its observation state $\mathbf{x}(t+1) = \{x_1(t+1), x_2(t+1), \ldots, x_n(t+1)\}^T$ has n dimensions and N finite states. Therefore, each dimension has N channels and the number of possible values is $L = N^n$. A larger value of information entropy indicates better randomness. The theoretical maximum information entropy $H_{\max} = \log_2(N^n) = n \log_2 N$ when $\Pr(i) = 1/N^n$ for $\forall\ i \in [1, N^n]$.

We designed two groups of experiments to test the randomness of outputs of n-D Cat maps. The first group fixes the dimension $n = 3$ and investigates the information entropy value against the number of finite states in interval $[3, 15]$. For each generation method of HCM, we randomly generate $5N^3$ n-D Cat maps with $M = N$ (MECs are restricted to $\{1, 2, \ldots, N\}$), and then calculate their information entropy values with the initial value $\mathbf{x}(0) = \mathbf{1}_{3\times 1}$ and iteration number N^4. Fig. 3(a) shows the average information entropy values of 3-D Cat maps generated by different methods with different values of N. It displays that the proposed method can generate 3-D Cat maps with much larger average information entropy values than other eight existing methods. Table V lists the maximum information entropy values of these 3-D Cat maps generated by different methods. For different numbers of finite states N, the 3-D Cat maps generated by the proposed method can achieve the maximum values larger than that of other methods, which means that they have better randomness.

The second group of experiments investigates the information entropy values against different dimensions n by fixing $M = N = 3$ (all MECs are restricted to $\{1, 2, 3\}$). For each n-D Cat map generation method with $n \in \{3, 4, \ldots, 10\}$, we randomly generate $5n^3$ n-D Cat maps, and then calculate their information entropy values with the initial value $\mathbf{x}(0) = \mathbf{1}_{n\times 1}$ and iteration number 3^{n+1}. Fig. 3(b) shows the average information entropy values of n-D Cat maps generated by those methods with different dimensions n. As can be seen from the figure, when dimension $n \leq 6$, the proposed method can generate n-D Cat maps with bigger average information entropy values; when dimension $n \geq 7$, both Wu's method and the proposed method can achieve bigger average information entropy values than other methods. Table VI lists the maximum information entropy values of n-D Cat maps achieved by different methods and that can be obtained theoretically. The Wu's method and the proposed method can both approach theoretical optimal performance very much and demonstrate much better than other methods in the aspect. These further verify that the proposed method can generate n-D Cat maps with extremely good randomness.

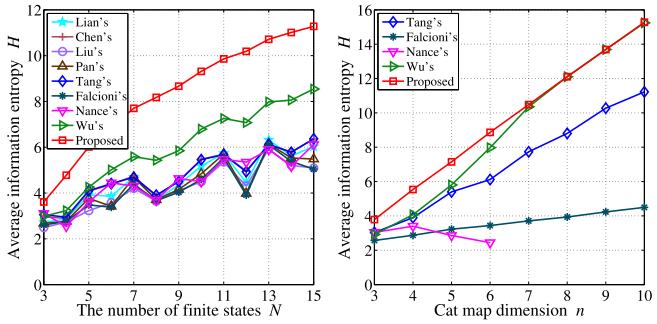


Fig. 3. Average information entropy values of n-D Cat maps generated by different methods. (a) Dimension $n = 3$ and the number of finite states $N \in \{3, 4, \ldots, 15\}$. (b) Number of finite states $N = 3$ and dimension $n \in \{3, 4, \ldots, 10\}$.

D. Correlation Dimension

Correlation dimension describes the space dimensionality of a set of points as a type of fractal dimension [48]. For a dynamic system, its attractor strangeness or degrees of freedom can be measured by correlation dimension. For a set of points $S = \{s_i \mid i = 1, 2, \ldots, M\}$ with a given embedding dimension e, a new point set $\overline{S} = \{\overline{s_t} \mid t = 1, 2, \ldots\}$ can be obtained, where $\overline{s_t} = (s_t, s_{t+\xi}, s_{t+2\xi}, \ldots, s_{t+(e-1)\xi})$ and $t \in \{1, 2, \ldots, M - (e-1)\xi\}$, ξ is the time delay (It is usually

TABLE VI
MAXIMUM INFORMATION ENTROPY VALUES OF n-D CAT MAPS GENERATED BY DIFFERENT METHODS WITH THE NUMBER OF FINITE STATES $N = 3$ AND DIMENSION $n \in \{3, 4, \ldots, 10\}$

Dimension	n-D Cat map generation methods					
n	Tang's	Falcioni's	Nance's	Wu's	Proposed	$H_{\max}$
3	3.6972	3.5819	3.6972	3.6972	4.5619	4.7549
4	5.3206	4.1689	5.2822	6.0505	6.0394	6.3399
5	6.9184	5.1696	4.1698	7.5783	7.6088	7.9248
6	8.5076	5.1699	3.4926	9.2116	9.1259	9.5098
7	10.0940	6.4918	-	10.7792	10.6707	11.0947
8	11.6795	6.4918	-	12.2388	12.2239	12.6797
9	13.2646	7.9773	-	13.7932	13.9718	14.2647
10	14.8496	7.9773	-	15.5143	15.5521	15.8496

set as 1). The correlation dimension d can be calculated as

$$d = \lim_{r \to 0} \lim_{M \to \infty} \frac{\log C_e(r)}{\log r}$$

where $\log C_e(r)$ is called the correlation integral defined by

$$C_e(r) = \lim_{M \to \infty} \frac{1}{[M - (e-1)\zeta][M - (e-1)\zeta - 1]} \times \sum_{i=1}^{M-(e-1)\zeta} \sum_{j=i+1}^{M-(e-1)\zeta} \theta\left(r - |\bar{s}_i - \bar{s}_j|\right)$$

where $\theta(\omega)$ is a step function

$$\theta(\omega) = \begin{cases} 0, & \text{if } \omega \le 0 \\ 1, & \text{if } \omega > 0. \end{cases}$$

If it exists, the correlation dimension d can be regarded as the slope of $\log C_e(r)$ with respect to $\log r$, defined by

$$d = \lim_{r \to 0} \lim_{M \to \infty} \frac{d(\log C_e(r))/dr}{d(\log r)/dr}.$$

With a bigger correlation dimension value, the trajectory of a dynamic system can occupy space of a larger dimensionality and its attractors can achieve more complex strangeness.

In the experiment, we set the embedding dimension $e = 2$ and designed two groups of experiments. The first group fixes $n = 3$ and investigates the correlation dimension values of n-D Cat maps against the number of finite states N in (1). For each generation method with $N \in \{3, 4, \ldots, 15\}$, $5N^2$ n-D Cat maps are randomly generated with $M = N$ (all MECs are restricted to $\{1, 2, \ldots, N\}$). The initial value is set as $\mathbf{x}(0) = \mathbf{1}_{3\times 1}$ and the observation state $\mathbf{x}(t+1) = \{x_1(t+1), x_2(t+1), \ldots, x_n(t+1)\}^T$ in every iteration is scaled

$$x_{t+1} = \left(\sum_{i=1}^{n} x_i(t+1) N^{i-1}\right) / N^n.$$

Fig. 4(a) shows the average correlation dimension values of 3-D Cat maps generated by different methods. As can be seen from the figure, the 3-D Cat maps generated by the proposed method have trajectories with higher correlation dimension values than the other eight methods.

The second group of experiments is to investigate the correlation dimension values of n-D Cat maps against the dimension

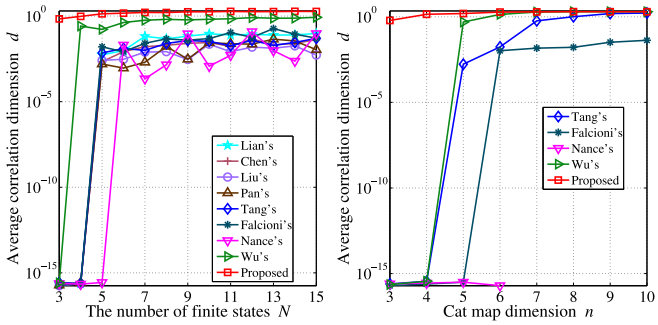


Fig. 4. Average correlation dimension values of n-D Cat maps generated by different methods. (a) Dimension $n = 3$ and the number of finite states $N \in \{3, 4, \ldots, 15\}$. (b) Number of finite states $N = 3$ and dimension $n \in \{3, 4, \ldots, 10\}$.

$n \in \{3, 4, \ldots, 10\}$. For each generation method, $5n^2$ n-D Cat maps are randomly generated by fixing $N = 3$ and $M = 3$ (all MECs are restricted to $\{1, 2, 3\}$). The correlation dimension values of these Cat maps are then calculated with initial value $\mathbf{x}(0) = \mathbf{1}_{n\times 1}$. Fig. 4(b) depicts their average values. The results further prove that the proposed method can generate n-D Cat maps with bigger correlation dimensions and better ergodicity.

VI. CONCLUSION

This paper has studied the inherent relation between the LEs of the Cat map and its associated Cat matrix, and proposed a simple but efficient model of constructing n-D HCMs with $\lfloor n/2 \rfloor$ positive LEs. For an arbitrarily desired number of positive LEs, the proposed method allows users to produce a new n-D HCM with expected complexity. To verify the effectiveness of the proposed method and the inherent relation, two numerical examples of HCMs, a 5-D HCM with two positive LEs and a 10-D HCM with five positive LEs, were constructed. Performance evaluations were performed in terms of LE, time complexity, information entropy and correlation dimension. Compared with existing HD Cat map generation methods, the proposed method can generate n-D HCMs with a desired number of positive LEs and lower computation time complexity, and the corresponding n-D Cat maps have better randomness and ergodicity. This research will promote practical application of digital Cat maps.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions that greatly contribute to improving the quality of this paper.

REFERENCES

[1] E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, no. 2, pp. 130–141, 1963.
[2] R. Law, D. J. Murrell, and U. Dieckmann, "Population growth in space and time: Spatial logistic equations," *Ecology*, vol. 84, no. 1, pp. 252–262, 2003.
[3] Z. Hua and Y. Zhou, "Dynamic parameter-control chaotic system," *IEEE Trans. Cybern.*, vol. 46, no. 12, pp. 3330–3341, Dec. 2016.

[4] M. Shen, W.-N. Chen, J. Zhang, H. S.-H. Chung, and O. Kaynak, "Optimal selection of parameters for nonuniform embedding of chaotic time series using ant colony optimization," *IEEE Trans. Cybern.*, vol. 43, no. 2, pp. 790–802, Apr. 2013.

[5] Y. Zhou, Z. Hua, C.-M. Pun, and C. L. P. Chen, "Cascade chaotic system with applications," *IEEE Trans. Cybern.*, vol. 45, no. 9, pp. 2001–2012, Sep. 2015.

[6] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, "Determining Lyapunov exponents from a time series," *Phys. D Nonlin. Phenom.*, vol. 16, no. 3, pp. 285–317, 1985.

[7] J. M. Amigo, L. Kocarev, and J. Szczepanski, "Discrete Lyapunov exponent and resistance to differential cryptanalysis," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 54, no. 10, pp. 882–886, Oct. 2007.

[8] Z.-P. Wang and H.-N. Wu, "On fuzzy sampled-data control of chaotic systems via a time-dependent Lyapunov functional approach," *IEEE Trans. Cybern.*, vol. 45, no. 4, pp. 819–829, Apr. 2015.

[9] G. Grassi and D. A. Miller, "Theory and experimental realization of observer-based discrete-time hyperchaos synchronization," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 49, no. 3, pp. 373–378, Mar. 2002.

[10] C. Li, J. C. Sprott, W. Thio, and H. Zhu, "A new piecewise linear hyperchaotic circuit," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 61, no. 12, pp. 977–981, Dec. 2014.

[11] S. Yu, J. Lü, X. Yu, and G. Chen, "Design and implementation of grid multiwing hyperchaotic Lorenz system family via switching control and constructing super-heteroclinic loops," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 59, no. 5, pp. 1015–1028, May 2012.

[12] Z. Hua and Y. Zhou, "Image encryption using 2D logistic-adjusted-Sine map," *Inf. Sci.*, vol. 339, pp. 237–253, Apr. 2016.

[13] C. Li, Y. Liu, T. Xie, and M. Z. Q. Chen, "Breaking a novel image encryption scheme based on improved hyperchaotic sequences," *Nonlin. Dyn.*, vol. 73, no. 3, pp. 2083–2089, 2013.

[14] H.-P. Ren, M. S. Baptista, and C. Grebogi, "Wireless communication with chaos," *Phys. Rev. Lett.*, vol. 110, no. 18, 2013, Art. no. 184101.

[15] Y. Li, W. K. S. Tang, and G. Chen, "Generating hyperchaos via state feedback control," *Int. J. Bifurcation Chaos*, vol. 15, no. 10, pp. 3367–3375, 2005.

[16] G. Hu, "Generating hyperchaotic attractors with three positive Lyapunov exponents via state feedback control," *Int. J. Bifurcation Chaos*, vol. 19, no. 2, pp. 651–660, 2009.

[17] B. Cannas and S. Cincotti, "Hyperchaotic behaviour of two bi-directionally coupled Chua's circuits," *Int. J. Circuit Theory Appl.*, vol. 30, no. 6, pp. 625–637, 2002.

[18] D. Cafagna and G. Grassi, "Hyperchaotic coupled Chua circuits: An approach for generating new $n \times m$-scroll attractors," *Int. J. Bifurcation Chaos*, vol. 13, no. 9, pp. 2537–2550, 2003.

[19] Y. Li, G. Chen, and W. K. S. Tang, "Controlling a unified chaotic system to hyperchaotic," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 52, no. 4, pp. 204–207, Apr. 2005.

[20] C. Shen, S. Yu, J. Lü, and G. Chen, "A systematic methodology for constructing hyperchaotic systems with multiple positive Lyapunov exponents and circuit implementation," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 3, pp. 854–864, Mar. 2014.

[21] C. Shen, S. Yu, J. Lü, and G. Chen, "Designing hyperchaotic systems with any desired number of positive Lyapunov exponents via a simple model," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 8, pp. 2380–2389, Aug. 2014.

[22] Q. Wang *et al.*, "Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 3, pp. 401–412, Mar. 2016.

[23] Q. Hong, Q. Xie, Y. Shen, and X. Wang, "Generating multi-double-scroll attractors via nonautonomous approach," *Chaos*, vol. 26, no. 8, 2016, Art. no. 083110.

[24] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D Sine logistic modulation map for image encryption," *Inf. Sci.*, vol. 297, pp. 80–94, Mar. 2015.

[25] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic Cat maps," *Chaos Solitons Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[26] F. Chen, K.-W. Wong, X. Liao, and T. Xiang, "Period distribution of the generalized discrete Arnold Cat map for $N = 2^e$," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 3249–3255, May 2013.

[27] J. Ford, G. Mantica, and G. H. Ristow, "The Arnol'd Cat: Failure of the correspondence principle," *Phys. D Nonlin. Phenom.*, vol. 50, no. 3, pp. 493–520, 1991.

[28] I. Antoniou, B. Qiao, and Z. Suchanecki, "Generalized spectral decomposition and intrinsic irreversibility of the Arnold Cat map," *Chaos Solitons Fractals*, vol. 8, no. 1, pp. 77–90, 1997.

[29] F. Chen, K.-W. Wong, X. Liao, and T. Xiang, "Period distribution of generalized discrete Arnold Cat map for $N = p^e$," *IEEE Trans. Inf. Theory*, vol. 58, no. 1, pp. 445–452, Jan. 2012.

[30] B. J. Saha, K. K. Kabi, and C. Pradhan, "A new approach on color image encryption using Arnold 4D Cat map," in *Computational Intelligence in Data Mining*. New Delhi, India: Springer, 2016, pp. 131–138.

[31] C. Li, "Cracking a hierarchical chaotic image encryption algorithm based on permutation," *Signal Process.*, vol. 118, pp. 203–210, Jan. 2016.

[32] A. Kanso and M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map," *Commun. Nonlin. Sci. Numer. Simulat.*, vol. 17, no. 7, pp. 2943–2959, 2012.

[33] M. Brindha and N. A. Gounden, "A chaos based image encryption and lossless compression algorithm using hash table and Chinese remainder theorem," *Appl. Soft Comput.*, vol. 40, pp. 379–390, Mar. 2016.

[34] D.-C. Lou and C.-H. Sung, "A steganographic scheme for secure communications based on the chaos and Euler theorem," *IEEE Trans. Multimedia*, vol. 6, no. 3, pp. 501–509, Jun. 2004.

[35] Z. Lin, S. Yu, J. Lü, S. Cai, and G. Chen, "Design and ARM-embedded implementation of a chaotic map-based real-time secure video communication system," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 25, no. 7, pp. 1203–1216, Jul. 2015.

[36] H. Liu, H. Wan, C. K. Tse, and J. Lü, "An encryption scheme based on synchronization of two-layered complex dynamical networks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 11, pp. 2010–2021, Nov. 2016.

[37] H. Liu, Z. Zhu, H. Jiang, and B. Wang, "A novel image encryption algorithm based on improved 3D chaotic Cat map," in *Proc. IEEE 9th Int. Conf. Young Comput. Sci.*, 2008, pp. 3016–3021.

[38] T. G. Pan and D. Y. Li, "A new algorithm of image encryption based on 3D Arnold Cat," *Adv. Eng. Forum*, vol. 1, pp. 183–187, Sep. 2011.

[39] M. Falcioni, L. Palatella, S. Pigolotti, and A. Vulpiani, "Properties making a chaotic system a good pseudo random number generator," *Phys. Rev. E*, vol. 72, no. 1, 2005, Art. no. 016220.

[40] J. Nance, "Periods of the discretized Arnold Cat map and its extension to n dimensions," 2011. [Online]. Available: http://arxiv.org/pdf/1111.2984v1.pdf

[41] Y. Wu, Z. Hua, and Y. Zhou, "n-dimensional discrete Cat map generation using Laplace expansions," *IEEE Trans. Cybern.*, vol. 46, no. 11, pp. 2622–2633, Nov. 2016.

[42] S. Lian, Y. Mao, and Z. Wang, "3D extensions of some 2D chaotic maps and their usage in data encryption," in *Proc. IEEE 4th Int. Conf. Control Autom.*, Montreal, QC, Canada, 2003, pp. 819–823.

[43] U. Schwengelbeck and F. H. M. Faisal, "Definition of Lyapunov exponents and KS entropy in quantum dynamics," *Phys. Lett. A*, vol. 199, nos. 5–6, pp. 281–286, 1995.

[44] E. W. Weisstein. (2002). *Vieta's Formulas*. Accessed on Dec. 12, 2016. [Online]. Available: http://mathworld.wolfram.com/VietasFormulas.html

[45] K. W. Tang and W. K. S. Tang, "A chaos-based secure voice communication system," in *Proc. IEEE Int. Conf. Ind. Technol.*, Hong Kong, 2005, pp. 571–576.

[46] A. M. Davie and A. J. Stothers, "Improved bound for complexity of matrix multiplication," *Proc. Roy. Soc. Edinburgh Section A Math.*, vol. 143, no. 2, pp. 351–369, 2013.

[47] J. A. Storer, *An Introduction to Data Structures and Algorithms*. Basel, Switzerland: Springer, 2001.

[48] A. M. Albano, J. Muench, C. Schwartz, A. I. Mees, and P. E. Rapp, "Singular-value decomposition and the Grassberger–Procaccia algorithm," *Phys. Rev. A*, vol. 38, no. 6, pp. 3017–3026, 1988.

Zhongyun Hua (S'14–M'16) received the B.S. degree from Chongqing University, Chongqing, China, in 2011, and the M.S. and Ph.D. degrees from the University of Macau, Macau, China, in 2013 and 2016, respectively, all in software engineering.

He is currently an Assistant Professor with the School of Computer Science and Technology, Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, China. His current research interests include chaotic system, chaos-based applications, and multimedia security.

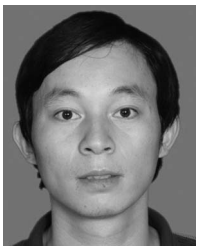
Shuang Yi (S'14) received the B.S. degree in software engineering from Chongqing University, Chongqing, China, in 2011. She is currently pursuing the Ph.D. degree with the Department of Computer and Information Science, University of Macau, Macau, China.

Her current research interests include multimedia security, data hiding, and signal/image processing.

Yicong Zhou (M'07–SM'14) received the B.S. degree from Hunan University, Changsha, China, and the M.S. and Ph.D. degrees from Tufts University, Medford, MA, USA, all in electrical engineering.

He is currently an Associate Professor and the Director of the Vision and Image Processing Laboratory with the Department of Computer and Information Science, University of Macau, Macau, China. His current research interests include chaotic systems, multimedia security, image processing and understanding, and machine learning.

Dr. Zhou was a recipient of the Third Prize of Macau Natural Science Award in 2014. He is an Associate Editor of the *Journal of Visual Communication and Image Representation*, an Editorial Board Member of *Neurocomputing*, and a Leading Co-Chair of Technical Committee on Cognitive Computing in the IEEE Systems, Man, and Cybernetics Society.



Chengqing Li (M'07–SM'13) received the bachelor's degree in mathematics from Xiangtan University, Xiangtan, China, the M.Sc. degree in applied mathematics from Zhejiang University, Hangzhou, China, in 2005, and the Ph.D. degree in electronic engineering from the City University of Hong Kong, Hong Kong, in 2008.

He was a Post-Doctoral Fellow with the Hong Kong Polytechnic University, Hong Kong, until 2010. Then, he joined the College of Information Engineering, Xiangtan University, Xiangtan, China, as an Associate Professor. From 2013 to 2014, he was with the University of Konstanz, Konstanz, Germany, under the support of the Alexander von Humboldt Foundation. He has published about 40 papers on the subject in the past ten years, receiving over 1500 citations with an H-index of 21. His current research interest includes security analysis of image and chaos-based encryption schemes.

Dr. Li is serving as an Associate Editor for the *International Journal of Bifurcation and Chaos*.

Yue Wu (S'08–M'12) received the Bachelor of Engineering degree with the Huazhong University of Science and Technology, Wuhan, China, in 2005, the Master of Science degree with the University of Toledo, Toledo, OH, USA, in 2008, and the Ph.D. degree in electrical engineering from Tufts University, Medford, MA, USA, in 2012. In his thesis work, he pioneered the data security techniques using Sudoku arrays.

Since 2014, he has been a Research Scientist with the Information Sciences Institute (ISI), University of South California, Los Angeles, CA, USA, where he continued his research in handwritten character recognition, but also started new research in face recognition and media forensics. He was a summer intern with Raytheon BBN Technologies, Cambridge, MA, USA, before graduation, and later joined as a Research Scientist. He developed and used algorithms for handwritten character recognition. His current research interests include automatic line segmentation, image denoising, and document binarization.