Yuanyuan LI, Xiaoqing YOU, Jianquan LU, Jungang LOU, 2023. A joint image compression and encryption scheme based on a novel coupled map lattice system and DNA operations. *Frontiers of Information Technology & Electronic Engineering,* 24(6):813-827. https://doi.org/10.1631/FITEE.2200645

A joint image compression and encryption scheme based on a novel coupled map lattice system and DNA operations

Key words: Compressive sensing; Coupled map lattice (CML); DNA operations; Semi-tensor product

Corresponding author: Jianquan LU
E-mail: jqluma@seu.edu.cn
ORCID: https://orcid.org/0000-0003-4423-6034

Motivation

1. How to design a secure and efficient image encryption scheme has always been a challenging issue. Image encryption based on compressive sensing (CS) faces the following challenges:

(1) An extremely large measurement matrix is needed when encrypting large-size images, and it will cost a lot of storage resources;

(2) CS cannot resist known-plaintext attacks (NPAs) or chosen-plaintext attacks (CPAs);

(3) The CS decryption process generally takes a long time.

Motivation (Cont’d)

2. Although the spatiotemporal chaotic system has been studied, the range of logistic map parameters is still not large enough and the randomness is unstable. Therefore, it is necessary to optimize the existing spatiotemporal chaotic system.

The proposed spatiotemporal chaotic system in this paper can not only applied in our encryption scheme, but also adapt to general encryption algorithms based on chaotic sequence.

Main idea

1. The central thought in this paper is that the scheme of using the spatiotemporal chaotic system with good performance to generate a CS measurement matrix, combined with semi-tensor product compressive sensing (STP-CS) and DNA encryption, can improve the encryption security and reduce the encryption speed of CS.

Method

1. Introducing a random parameter of linear and nonlinear neighbors can greatly improve the randomness of mixed linear–nonlinear coupled map lattice (MLNCML) system.

2. Plaintext-related scrambling and DNA encryption can resist NPAs and CPAs. Therefore, the security can be improved.

3. Using semi-tensor product (STP) of matrices in compressive sensing can reduce the decryption time.

Major results

1. The proposed chaotic system

A novel mixed linear–nonlinear coupled map lattice (NMLNCML) system with L lattices is defined as

$$x_{n+1}(i) = \mathrm{mod}(f[x_n(i)] + (1-\eta)\cdot\{f[x_n(i+1)] + f[x_n(i-1)]\} + \eta\cdot\{f[x_n(j)] + f[x_n(k)]\}, 1),$$

where i, j, k are different lattices ($2 \le i \le L-1$, $1 \le j, k \le L$), η is the coupling parameter ($0 \le \eta \le 1$), n is the time sequence ($n=1, 2, \ldots$), and $x_{n+1}(i)$ is the state of lattice i at time $n+1$. Logistic map $f(x)=\mu x(1-x)$, and $\mu \in [3.56, 4]$. The neighbor relationship among j, k, and i obeys the Arnold transform.

Major results (Cont’d)

Simulation results show that, compared with the MLNCML system,

(1) the Kolmogorov–Sinai entropy of our NMLNCML system is larger;

(2) the range of optional parameter μ in NMLNCML has been enlarged from [3.56, 4] to [2.28, 4];

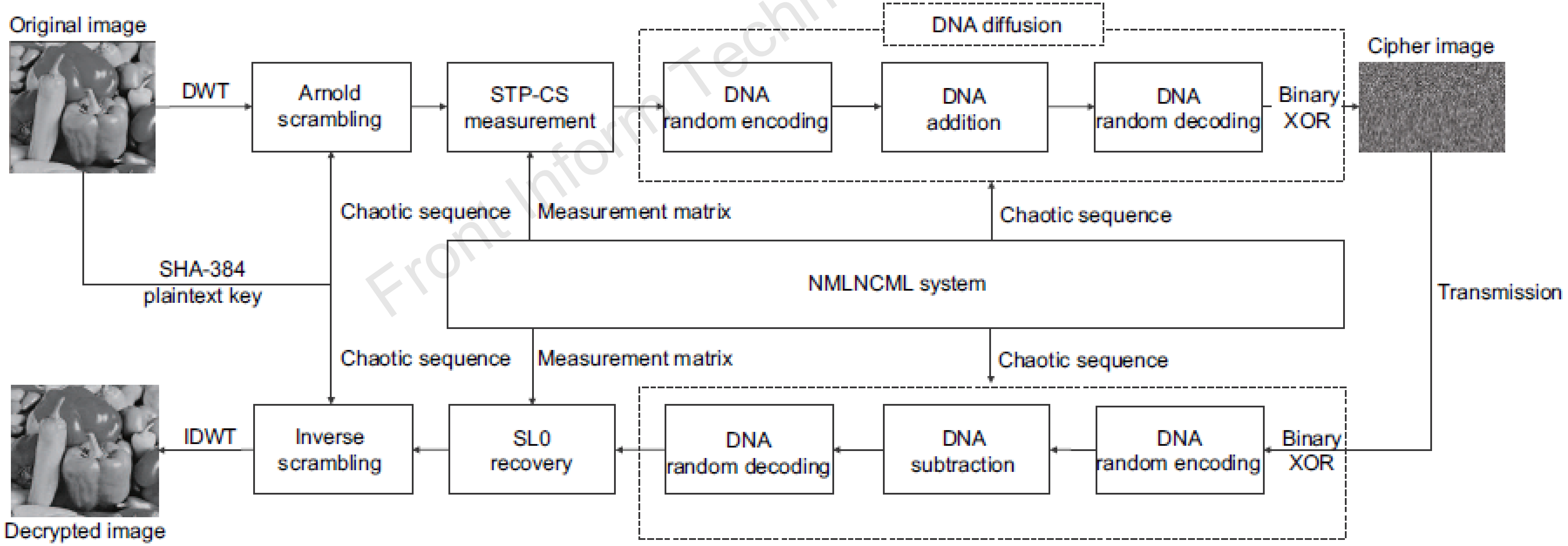
(3) the number of periodic windows in bifurcation diagrams has decreased.

Thus, the chaotic property is stronger and ergodicity of the system has been significantly improved.

Major results (Cont’d)

2. Image encryption scheme

The encryption algorithm consists of scrambling, STP-CS measurement, and DNA diffusion. The process is shown as follows:



Major results (Cont’d)

Simulation results and security analysis indicated that our cryptosystem has significant key space, high sensitivity to secret keys, great resistance to chosen-plaintext, statistical, and differential attacks, and good robustness to noise and data loss.

In addition, the outstanding compression and encryption performance can promote secure image compression and transmission on public channels and networks.

Conclusions

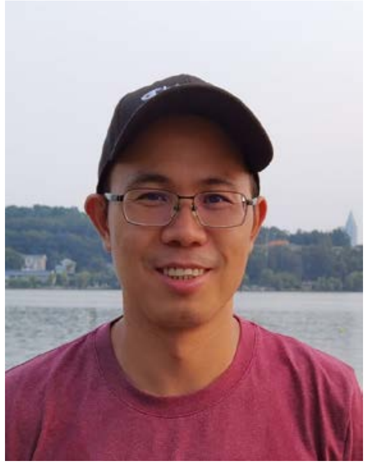
In this paper, we presented a scheme for image encryption that takes advantages of a spatiotemporal chaotic system and DNA operations in CS.

A new chaotic system was proposed and applied to generate the CS measurement matrix. STP-CS and DNA encryption were used to reduce the decryption speed and enhance security.

Simulation results show the effectiveness and superiority of the proposed image encryption scheme.

Yuanyuan LI received the B.S. degree in Mathematics from Nanjing Normal University, Nanjing, China in 2004, and the Ph.D. degree in Mathematics from Nanjing University, Nanjing, China in 2009. Now she is an associate professor in Department of Applied Mathematics, Nanjing Forestry University, Nanjing, China. Her current research interests include algebraic number theory, Boolean networks, and hybrid systems.

Xiaoqing YOU received the B.S. degree in Computer Science and Technology from Nanjing University of Finance and Economics, Nanjing, China in 2018, and the M.S. degree in Cyber Science and Engineering from Southeast University, Nanjing, China, in 2021. Now she is a software development engineer in Shanghai, China. Her research interests include logical networks and complex networks.



Jianquan LU received the B.S. degree in Mathematics from Zhejiang Normal University, Jinhua, China, in 2003, the M.S. degree in Mathematics from Southeast University, Nanjing, China, in 2006, and the Ph.D. degree in Applied Mathematics from City University of Hong Kong, Hong Kong, China in 2009. From 2010 to 2012, he was an Alexander von Humboldt Research Fellow in PIK, Germany. He is currently a professor with Southeast University, Nanjing, China. His current research interests include collective behavior in complex dynamical networks and multi-agent systems, logical networks, and hybrid systems. He has published over 100 papers in refereed international journals. Dr. LU was named as Highly Cited Researcher by Clarivate Analytics from 2018 for four consecutive years, and he was elected Most Cited Chinese Researchers by Elsevier during 2014–2021. Dr. LU is an associate editor of *Neural Processing Letters*, *Journal of Franklin Institute*, and *Neural Computing and Applications*, and a guest editor of *Science China: Information Sciences* and *IET Control Theory & Applicat*ions.

Jungang LOU received the B.S. degree in Mathematics from Zhejiang Normal University, China, in 2003, and the M.S. degree in Computational Mathematics and the Ph.D. degree in Computer Science and Technology from Tongji University, Shanghai, China, in 2006 and 2010, respectively. He is currently a Professor with the Yangtze Delta Region (Huzhou) Institute of Intelligent Transportation, Huzhou University, Huzhou, China. He also holds a Researcher position at the Zhejiang Province Key Laboratory of Smart Management & Application of Modern Agricultural Resources, Huzhou University, Huzhou, China. He was a Visiting Scholar with the Department of Computer Science at The University of Texas at San Antonio between Nov. 2017 and May 2018 (advisor Professor Qi Tian, IEEE Fellow). His current research interests include dependable computing, reliability engineering, artificial intelligence, machine learning and network stability. He has published over 80 papers in refereed international journals including *IEEE TC*, *IEEE TCAD*, *IEEE TFIS*, *IEEE TNNLS*, *IEEE TR*, and so on.