DOI:10.20033/j.1003-7241.(2025)06-0046-05

基于时空混沌模型的电力芯片DNA序列双重动态混淆加密技术

祝健杨，辛明勇，徐长宝，王 宇
(贵州电网有限责任公司电力科学研究院,贵州 贵阳 550002)

摘 要: 针对电力芯片图像信息数据加密技术存在数据遗失的安全性不足的问题,提出一种基于时空混沌模型的电力芯片DNA序列双重动态混淆加密技术。选用二维混沌系统进行加密运算,构建混沌时空模型;通过DNA编码和解码规则对混沌系统时空分布图像的像素值进行识别处理,实现双重动态加密数据处理;构建电力芯片序列双重动态混淆架构,进行混淆动态加密计算,得到电力芯片DNA序列双重动态混淆加密和解密矩阵序列。由实验数据表明,利用所提方法的加密总时长为0.489 s,图像还原度高,能够有效提高电力芯片数据传输和图像识别的安全性,应用效果良好。

关键词: 时空混沌模型;电力芯片;DNA序列;动态混淆加密
中图分类号:TP309 文献标识码:A 文章编号:1003-7241(2025)06-0046-05

Double Dynamic Confusion Encryption of DNA Sequences in Power Chips Based on Spatiotemporal Chaos Model

ZHU Jian-yang, XIN Ming-yong, XU Chang-bao, WANG Yu
(Electric Power Research Institute of Guizhou Power Grid Co., Ltd., Guiyang 550002, China)

Abstract: Aiming at the problem of insufficient security due to data loss in power chip image information encryption technology, a dual dynamic confusion encryption technology for power chip DNA sequences based on spatiotemporal chaos model is proposed. It selects a two-dimensional chaotic system for encryption operations to construct a chaotic spatiotemporal model. Through DNA encoding and decoding rules, the pixel values of spatiotemporal distribution images of chaotic systems are recognized and processed to achieve dual dynamic encrypted data processing. It constructs a dual dynamic obfuscation architecture for power chip sequences, performs obfuscation dynamic encryption calculations, and obtains dual dynamic obfuscation encryption and decryption matrix sequences for power chip DNA sequences. Experimental data show that the total encryption time using the proposed method is 0.489 seconds, and the image restoration degree is high. It can effectively improve the security of power chip data transmission and image recognition, with good application results.

Keywords: spatiotemporal chaos model; power chip; DNA sequence; dynamic obfuscation encryption

0 引言

目前,网络安全问题频发,电子芯片和图像数据信息泄露影响信息传输安全。因此,针对芯片数据加密技术的研究逐渐成为网络安全领域研究的重点方向。

文献[1]以多点控制单元(multipoint control unit, MCU)输入网端为安全加密通信基础,选用IPESC加密芯片,与通信安全装置之间进行同步数据连接,并加强对电力芯片配电终端的安全防护。但数据连接过程中动态性较差,数据安全监测工作效率较低。文献[2]基于网格编码调制(trellis-coded modulation,TCM)加密芯片对系统内部信息数据进行搜集整理,优化数据传输介质加密性能,提升信息储存安全性,能够实现数据与云计算间的协同处理。但在信息搜集过程需要建立跨网络通信支持,操作成本高。文献[3]基于语音加密算法和忆阻器混沌系统生成s盒数据,应用分叉图表示忆阻器系数的混沌范围,数据加密效果良好。但混沌参数的计算量大,计算效率有待提高。

针对传统方法存在的弊端,本文研究一种基于时空混沌模型的电力芯片DNA序列双重动态混淆加密技术。通过构建混沌系统模型,增强电力芯片图像数据识别提取效能,结合DNA序列规则编码解码,利用动态混淆加密运算实现电力芯片的双重动态混淆加密,有效提升信息数据通信的安全性。

1 时空混沌模型

1.1 混沌系统

混沌系统是一种基于混沌动力学的非线性科学理

*基金项目:国家重点研发计划(2020YFB0906000;2020YFB0906001);贵州电网有限公司科技项目(GZKJXM20200720)
收稿日期:2023-12-06

论，具有一定的不确定性和不可预测性。由混沌系统形成的混沌模型对样本数据具有较强的依赖性，且形成的混沌轨迹随机性大[4-5]。混沌系统主要由一维混沌系统、二维混沌系统、三维混沌系统三部分构成，为了研究基于时空混沌模型的电力芯片DNA序列双重动态混淆加密技术，选用了二维混沌系统进行加密运算，二维混沌系统表示为：

$$\begin{cases} x_{n+1}=\sin\left(\pi\left(4\phi x_n\left(1-x_n\right)+(1-\theta)\sin\left(\pi y_n\right)\right)\right) \\ y_{n+1}=\sin\left(\pi\left(4\phi y_n\left(1-y_n\right)+(1-\theta)\sin\left(\pi x_{n+1}\right)\right)\right) \end{cases} \tag{1}$$

式中，x_n和y_n分别是样本数据的时空混沌系统空间横坐标和纵坐标；x_{n+1}、y_{n+1}分别表示加密运算后时空混沌系统空间的横坐标和纵坐标；ϕ是混沌系统的控制参数，且满足$\phi\in(0,1)$；θ为混沌系统干扰因数。系统将样本数据映射到二维混沌模型中，将映射后的数据进行耦合，通过正弦变换把输入的一维映射数据转换为二维映射数据[6-7]。输入的样本数据得到的数据映射结果在混沌系统中形成的混沌模型如图1所示。

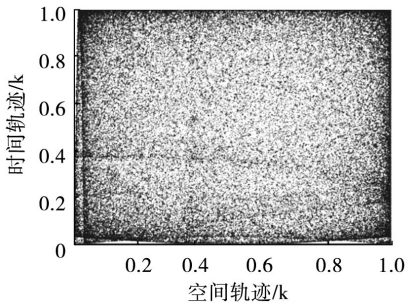


图1 混沌系统轨迹时空分布图

如图1所示，构建的电力芯片混沌模型空间轨迹分布比较均匀，说明该混沌系统的随机性输出效果良好。利用李雅普诺夫指数对混沌系统样本数据的初始状态进行动态描述，得到的混沌轨迹具有两个正向的李雅普诺夫指数，说明该混沌系统的轨迹方向更为发散，混沌属性复杂[8]。利用柯尔莫哥洛夫熵检验该混沌系统的应用性能，判定该混沌系统只具有一个熵值为正数，证明该系统的混沌轨迹具有不可预测性。

1.2 DNA编码和解码

基于混沌系统时空分布图像，选用DNA编码对图像的像素值进行识别处理。首先，提取图像关键像素点作为DNA编码样本数据，识别其灰度值，进行二进制序列转换，将混沌图像转化为DNA编码序列。设A表示腺嘌呤，T为胸腺嘧啶，二者为互补关系；G为鸟嘌呤，C为胞嘧啶，二者同样为互补关系。四个数据组之间能够形成24种编码方案，由于需要对混沌图像进行二进制转换，选择满足碱基互补的规则配对组进行解码，最终得到的规则配对结果如表1所示。

表1 DNA编码解码规则

DNA编码	00	01	10	11
规则1	A	C	G	T
规则2	A	G	C	T
规则3	T	C	G	A
规则4	T	G	C	A
规则5	C	A	T	G
规则6	C	T	A	G
规则7	G	A	T	C
规则8	G	T	A	C

表1中，根据上述规则对DNA编码序列进行反向解码，经过二进制转换将序列数据还原为像素灰度值数据。由于图像像素数据量较大，无法控制编码和解码过程中产生的随机轨迹[9-10]。因此运用混沌系统记录对应的随机序列变化编码和解码，实现时空混沌条件下DNA序列的双重动态混淆加密数据处理。

2 电力芯片DNA序列双重动态混淆加密

2.1 双重动态混淆架构

电力芯片DNA序列双重动态混淆架构主要包括控制模块、扫描模块、更新模块。控制模块操作数据输入，将数据上传到更新模块，通过更新编码转化的输出数据为编码序列[11]。序列数据进入扫描链，扫描链中设定DNA编码规则为逻辑器，数据根据不同特征触发对应的逻辑器，经过逻辑动态混淆后再次输入到更新模块，进行逻辑序列自动更新转换，最后输出数据序列为样本数据的动态混淆策略形态。双重动态混淆架构如图2所示。

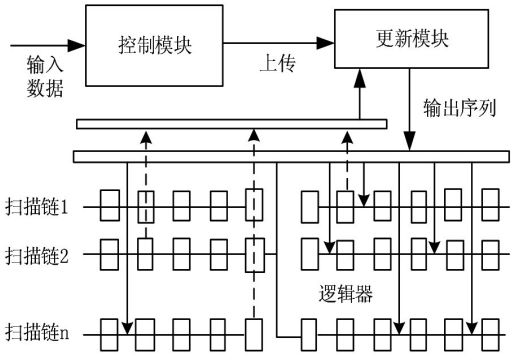


图2 双重动态混淆架构

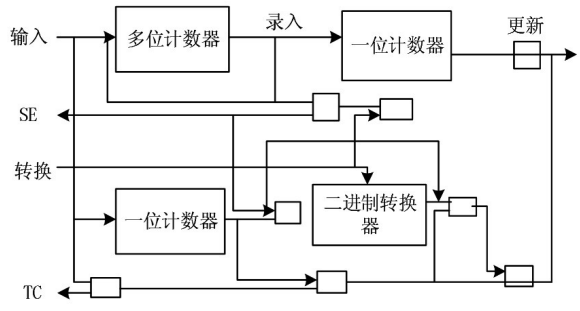


图3 控制模块的电路结构

图2中，控制模块主要负责控制样本图像数据，将其输入到双重动态混淆系统中。控制模块中工作单位为多位计数器和逻辑门，输入数据通过计数器扫描检测输入信号数据位数和更新进制，并控制信号数据输入与输出的时间，为更新模块提供符合检测标准的数据样本。控制模块的电路结构如图3所示。

更新模块和扫描模块相连接，主要功能为利用更新规则转换输入数据，形成适用于双重动态混淆形态的数据样本。再将数据样本输出到扫描链，通过逻辑触发器对输入数据进行序列编码。同时，更新模块中设置有选择器，输入序列能够在选择器中进行选择，选择任意门为输入信号插入逻辑器[12]。由于模块具有双重动态，因此在输入和输出数据时存在低电平和高电平两种状态。当数据处理时处于低电平信号会按照原有序列进行输出，当信号处理为高电平时，会通过高电扫描器混淆输出端数据序列，迭代进行更新扫描后再次输出动态混淆扫描链数据。扫描链的动态混淆算法步骤如下：

$$S_C = \text{function}(m), m \le M \tag{2}$$

式中，S_C表示扫描链输出数据，m为更新模块的变量系数，M表示更新模块进行更新迭代的位数。

$$f(j) \le L - i, f(i) = 1 \tag{3}$$

式中，$f(j)$表示数据序列的更新函数，L表示混淆策略的权重参数，$f(i)$为样本数据序列初始函数，引入扫描逻辑器的编码规则后得到动态加密扫描链数据为：

$$O_C = S_C \oplus K_m \tag{4}$$

式中，O_C表示经过扫描逻辑器的编码规则后得到动态加密扫描链数据；i为样本数据序列；K_m为动态加密系数。

最终输出数据满足双重动态混淆攻击模式自动切换后，则可以输出为实验数据。若无法满足，则需要重新进行动态混淆策略运算，直到输出结果为有效数据为止。

2.2 混淆动态加密

基于上述动态混淆策略运算结果进行加密计算，结合图像灰度值数据和DNA编码序列进行加密，混淆动态加密计算流程如图4所示。

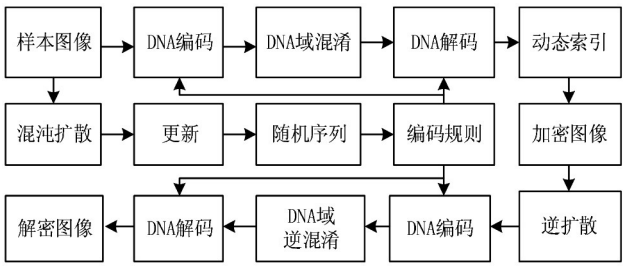


图4 动态混淆加密策略运算流程

假设电子芯片样本图像为P，在时空混沌系统的初始坐标值为x_0, y_0，代入到DNA编码规则运算得到的量化序列的主要运算步骤如下：

$$H = mod\left(\text{floor}\left(\left(x_{n+1} + y_{n+1}\right) \times 10^5\right), 8O_C\right) \tag{5}$$

式中，H表示DNA编码规则，mod表示对样本数据的取舍函数，floor表示样本数据空间坐标的最小实数，经过扩散后得到动态数据变化参数：

$$\alpha = \text{mod}\left(\text{mod}\left(\text{sum}(H) + \left(\text{floor}px_0 \times 10^5\right), 256\right)\right. \tag{6}$$

式中，α为扩散动态数据变化参数，sum(H)表示编码规则数据的累积序列。取样本图像数据范围极值代入公式得到随机序列A作为加密运算的密钥矩阵：

$$A = \text{mod}\left(\text{floor}\left(\theta(1:xy) \times 10^{14}\right), 256H\right) \tag{7}$$

式中，x，y为样本图像的数据范围极坐标。计算后输出的加密矩阵为：

$$\begin{cases} M = \text{mod}\left[\text{floor}\left(\theta(A:a) \times 10^5\right), 4f(j)\right] \\ C = \text{mod}\left[\text{floor}\left(\theta(A:4a) \times 10^5, f(i)\right)\right] \end{cases} \tag{8}$$

式中，C代表密钥解码矩阵。

通过计算能够得到电力芯片DNA序列双重动态混淆加密和解密矩阵序列。

3 实验研究

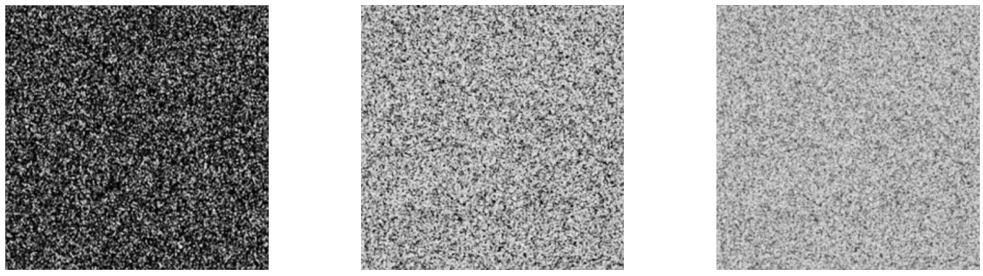
为了验证文章所提技术的加密效果，选用处理器芯片为Intel i5，操作系统为Windows 10的计算机作为实验主机，并与传统的IPSEC安全加密芯片和TCM芯片加密方法进行对比，对图5样本图像进行加密与解密，检验各加密方法的应用效果。

图5 待加密样本图像

3.1 加密与解密效果分析

如图6所示，能够看出文章所提方法对电力芯片图像进行双重动态混淆加密后的结果严密，而传统方法的加密结果存在模糊问题，表明由于其加密层数不够，密保程度不高，导致图像加密效果不良，信息保护安全性较差。再对加密图像进行解密，得到三种方法的解密图像结果如图7所示。

根据图7所示的图像解密结果，可以看出利用文章方法解密后的图像还原效果更好，与原图像高度重合。而传统方法的图像解密结果均存在一定程度的失真现象，



(a) 文章加密方法 (b) IPSEC 加密方法 (c) TCM 加密方法

图6 电力芯片图像加密结果对比

(a) 文章加密方法 (b) IPSEC 加密方法 (c) TCM 加密方法

图7 电力芯片图像解密效果对比

利用互联网络层安全协议(internet protocol security,IPSEC)加密方法解密后的图像光感较差,明暗度失衡;利用TCM加密方法解密后的图像曝光率较高,像素相对降低,饱和度不平衡,还原效果不理想。由此可见文章研究的方法在电力芯片图像加密和解密方面的效果良好,比传统方法更具优势。

3.2 实验结果与性能分析

由表2可知,选用文章方法对电力芯片进行加密,其图像像素平均变化率较低,均保持在0.22%左右,且变化比较稳定,说明对原图像像素的影响较小,加密过程更安全稳定。而传统方法的变化率普遍高于0.35%,TCM加密方法在混沌模型中的像素平均变化率高达0.62%,极差达到了0.25%,说明传统方法在图像加密过程中会对图像本身像素造成不同程度的影响,进而导致解密后图像失真等问题。

表2 像素平均变化率

加密算法	动态混淆加密/%	IPSEC 加密/%	TCM 加密/%
混沌轨迹	0.21	0.35	0.37
DNA序列	0.23	0.38	0.49
混沌模型	0.22	0.36	0.62

表3 时间复杂度分析

加密时间/s	动态混淆加密	IPSEC 加密	TCM 加密
DNA 加密	0.129	0.214	0.335
DNA 解密	0.243	0.246	0.407
动态混淆	0.117	0.227	0.230
总时长	0.489	0.687	0.972

由表3可知,文章方法对样本图像的总加密时长为0.489 s,可见该方法所需加密时间较短,加密效率更高。IPSEC 加密方法的加密总时间为0.687 s,TCM加密方法的加密时间最长,总时长为0.972 s。由此可见,所提方法的加密时间最短,在工作效率方法比传统方法更具优势。

综上所述,所提基于时空混沌模型的电力芯片DNA序列双重动态混淆加密技术能够有效保障图像加密和解密工作的安全性,在处理后能够保持良好的像素变化率,在加密时间和效率上也明显优于传统方法,说明该方法具有良好的应用效果,能够满足当前电力芯片加密工作的需求。

4 结束语

研究了一种基于时空混沌模型的电力芯片DNA序列双重动态混淆加密技术,得到以下结论:(1)选用二维混沌系统构建时空混沌模型,通过混沌轨迹判断混沌系统时空分布图像特征属性,为DNA序列编码解码提供具有稳定随机性的样本数据。(2)通过DNA规则对输入数据序列进行编码和解码,在满足双重动态碱基互补规则的条件下进行序列匹配,有利于快速实现混沌条件下DNA序列的双重动态加密数据处理。(3)构建电力芯片序列双层动态混淆架构,通过扫描链对输入数据进行逻辑控制,将扫描输出数据代入到DNA编码规则运算中得到双重动态混淆加密和解码矩阵,提高数据传输通信的安全性。综上所述,文章所研究的方法通过时空混沌系统和DNA

序列对电力芯片信息安全进行了双重动态加密，具有良好的应用效果，但该方法仍存在一些不足，该方法需要将混沌系统图像识别处理和数据多位数运算相结合，操作难度较大，对设备的智能化网络化要求较高。未来研究应着重于芯片安全系统保密过程的一体化和精简化，进一步提高安全保护效率。

参考文献：

[1] 简淦杨，蔡田田，习伟，等.基于异步传输的IPSEC安全加密芯片应用[J].电子器件，2020，43(2)：239-244.

[2] 刘强，李巧，鲍晓.基于国产TCM芯片加密的边云协同数据采集架构[J].计算机与现代化，2022，(8)：94-98，113.

[3] ELSAFTY，ABDULAZIZ H.，TOLBA，MOHAMMED F.，et al.Hardware realization of a secure and enhanced s-box based speech encryption engine[J].Analog Integrated Circuits and Signal Processing，2021，106(2)：385-397.

[4] 李蓝航，丘森辉，肖丁维，等.基于DNA序列和动态索引扩散的图像加密算法[J].广西师范大学学报：自然科学版，2021，39(3)：40-53.

[5] 张淑霞，李珊珊，白牡丹，等.基于混沌系统的数字彩色图像加密技术[J].科学技术与工程，2022，(13)：5291-5298.

[6] 郝晋，王伟，李庆宇，等.基于混沌序列与DNA突变原理的彩色图像加密方案[J].大连工业大学学报，2021，40(3)：214-221.

[7] 王洋，马剑，姚程，等.基于区块链技术的能源隐私大数据能源共享方法[J].自动化技术与应用，2023，42(6)：119-122，173.

[8] 陈虹，赵菊芳，郭鹏飞，等.基于混沌映射的分块循环DNA图像加密算法[J].计算机应用研究，2022，39(6)：1865-1871.

[9] 钟巍峰，杨庆胜，宁艳，等.基于硬件加密的移动终端安全通信系统设计[J].自动化技术与应用，2023，42(4)：96-100，162.

[10] 方阳，赵婷，刘期烈，等.基于图交互与场景感知融合的轨迹预测方法[J].计算机科学，2022，49(10)：258-264.

[11] 蔡雨岐，郭卫斌.基于多级语义信息融合编码的序列标注方法[J].计算机工程与科学，2022，44(12)：2266-2272.

[12] 黄海生，党成，李鑫，等.一种SDRAM控制器的设计电路[J].现代电子技术，2022，45(4)：35-38.

作者简介：祝健杨(1991—)，男，硕士，工程师，研究方向：电网安全稳定控制技术及智能电网。

(上接第10页)

[9] Dorin Comaniciu，Visvanathan Ramesh，and Alessio Del Bue.2002.Multivariate Saddle Point Detection for Statistical Clustering[C].In Proceedings of the 7th European Conference on Computer Vision-Part III(ECCV'02).Springer-Verlag，Berlin，Heidelberg，561-576.

[10] Xiang-Ru L I，Fu-Chao W U，Zhan-Yi H U.Convergence of a mean shift algorithm[J].Journal of Software 2005，16(3)：365-374.

[11] Q.Guo，X.Chang and H.Chu，Clustering Analysis Based on the Mean Shift[C]//2007 International Confere nce on Mechatronics and Automation，Harbin，China，2007：309-313.

[12] P.W M，C.J M.Kernel Smoothing[M].London：Chapman and Hall/CRC，1995：91-108.

[13] Wang J，Thiesson B，Xu Y，et al.Image and Video Segmentation by Anisotropic Kernel Mean Shift[C]//European Conference on Computer Vision.Berlin，Heidelberg：Springer，2004.

[14] N S A.Mixture Density Mercer Kernels A Method to Learn Kernels Directly from Data[C].Proceedings of the Fourth SIAM International Conference on Data Mining，2004：369-378.

[15] Xianda Z.Matrix Analysis and Application[M].Bei Jing：TsingHua University Press，2004.

[16] F.S G A.A Matrix Handbook for Statisticians[M].NewYork：Wiley-Interscience，2008：220-221.

[17] Wand M X X，Jones M X X.Comparison of Smoothing Parameterizations in Bivariate Kernel Density Estimation[J].JASA：Journal of the American Statistical Association，1993.

[18] Mathews John H.F K D.Numerical methods using MATLAB[M].Bei Jing：Publishing House of Electronics Industry，2004：42.

[19] Duong T.ks：Kernel Density Estima tion and Kernel Discriminant Analysis for Multivariate Data in R[J].Journal of Statistical Software，2007：21.

[20] Xianliang G.Application of functional analysis[M].Hangzhou：Zhejiang University press，1996.

[21] Senlin X，Chunhua X.Mathematical analysis[M].Beijing：Tsinghua Univer sity press，2005：225.

[22] Ge X.Application of functional analysis[M].Hangzhou：Zhejiang Univer sity press，1996.

[23] Chang K J.Common inequality[M].3rd ed.Jinan：Shandong Science and Technology Press，2004：1.

[24] D M.Higher mathematics[M].BeiJing：Higher Education Press，1996：55-58.

作者简介：朱晓光(1983—)，男，讲师，研究方向：机器学习。

通信作者：乔立永(1982—)，男，讲师，研究方向：模式识别。