

基于 CMS 协议和混沌映射的继电保护通信 报文安全防篡改方法

黄翔¹, 徐培栋^{2†}, 俞力珉², 任旭超¹, 宋亮亮³

(1. 国网江苏电力有限公司, 江苏 南京 210024; 2. 国网江苏电力有限公司无锡供电分公司, 江苏 无锡 214200;
3. 国网江苏电力有限公司电力科学研究院, 江苏 南京 210024)

摘要: 由于仅对通信报文关键信息进行单次加密, 导致常规方法的防篡改效果不佳。因此, 设计了基于 CMS 协议和混沌映射的继电保护通信报文安全防篡改方法。首先, 对获取的通信报文信息进行滤波处理, 提取出通信报文的关键信息, 并分析其内部的关联规则; 再根据通信报文关键信息的特点, 生成对应的混沌映射函数, 并利用该函数对通信报文关键信息进行初次加密处理; 然后, 在 CMS 协议的作用下, 对其进行二次加密处理; 最后, 通过对通信报文信息进行解密, 对其完整性进行验证, 实现通信报文安全防篡改。实验结果表明, 该方法在实际应用中的防篡改成功率较高, 防篡改效果较好。

关键词: CMS 协议; 混沌映射; 继电保护; 通信报文; 报文安全; 防篡改方法; 方法设计

中图分类号: G642

文献标识码: A

A Security and Tampering Prevention Method for Relay Protection Communication Messages Based on CMS Protocol and Chaos Mapping

HUANG Xiang¹, XU Peidong^{2†}, YU Limin², REN Xuchao¹, SONG Liangliang³

(1. State Grid Jiangsu Electric Power Co., Ltd., Nanjing, Jiangsu 210024, China;
2. Wuxi Power Supply Branch, State Grid Jiangsu Electric Power Co., Ltd., Wuxi, Jiangsu 214200, China;
3. State Grid Jiangsu Electric Power Co., Ltd., Research Institute, Nanjing, Jiangsu 210024, China)

Abstract: Due to only encrypting the key information of communication messages in a single attempt, the anti tampering effect of conventional methods is poor. Therefore, a secure and tamper proof method for relay protection communication messages based on CMS protocol and chaotic mapping was designed. Firstly, filter and process the obtained communication message information, then extract the key information of the communication message, and analyze its internal association rules. Based on the characteristics of the key information of the communication message, generate the corresponding chaotic mapping function, and use this function to encrypt the key information of the communication message for the first time. Under the action of the CMS protocol, encrypt it for the second time, and decrypt the communication message information, and verify its integrity to achieve secure and tamper proof communication messages. The experimental results show that the method has a high success rate in anti tampering and good anti tampering effect in practical applications.

Key words: CMS protocol; chaos mapping; relay protection; communication message; message security; anti tampering methods; method design

智能电网的快速发展,使得电力系统对继电保护通信报文的可靠性和安全性提出了更高的要求。通信报文包含了控制电力系统的关键信息,如故障定位、设备状态等,是确保电力系统稳定运行的关键信息,一旦被篡改,可能导致严重的电力事故。然而,由于通信通道的开放性,这些报文面临着被篡改的风险。传统的防篡改方法由于过于复杂,加上极为依赖特定的硬件或者软件环境,导致其通用性不强、实时性较差。因此,在上述背景下,不少研究学者针对防篡改方法展开了研究。

文献[1]利用区块链技术的分布式特性,确保数据不会被单一的节点控制,在改进 CP-ABE 算法的作用下,根据数据属性对数据进行加密处理,并将其存储在区块链上,再对数据修改进行验证。该方法根据不同的属性对数据进行加密,具有很高的灵活性,但其依赖于区块链网络的正常运行,方法的安全性和稳定性不高。文献[2]利用信息隐藏技术,将关键信息嵌入到普通数据中,并利用加密算法对隐藏的信息进行加密,并在数据中添加标记,由此来判定数据是否被篡改。该方法根据实际需求调整信息隐藏的策略和加密算法,以满足不同场景下的防篡改需求,但其在处理大量数据时,需要面临较高的计算和存储成本,防篡改成本较高。文献[3]利用 Native Detection 技术对数据进行实时监控,并设计多种防篡改模型,全方位地保护系统的安全,设定实时报警机制,对出现的异常行为进行实时检测,再利用自动修复机制对系统的漏洞进行修复。该方法通过多种防篡改模式的综合运用,可以有效地防止各种形式的篡改行为,但其自动修复机制还不完善,很容易导致系统信息被篡改,方法的安全性不高。文献[4]利用区块链技术构建链路网络,并对网络参数进行设置,使用对称加密和非对称加密对敏感数据进行加密和解密,在智能合约的作用下,对数据访问权限进行限制,避免数据被篡改。该方法由于区块链的不可篡改性和可追溯性,任何对数据的篡改都会被立即检测到,从而降低了数据被篡改的风险,但其无法根据实际需求调整敏感数据的加密方式,导致方法的灵活性较低。

在上述研究的基础上,本文设计了基于 CMS 协议和混沌映射的继电保护通信报文安全防篡改方法。先提取继电保护通信报文关键信息,在 CMS 协议和混沌映射的作用下,构建通信报文加密机制,再对通信报文进行解密处理,验证通信报文的完整性,判断通信报文信息是否被篡改,并对其修复处理^[5-6]。本文设计的方法有助于提高电力系统的安全性和稳定性,降低因通信报文被

篡改而引发的电力事故风险。同时,本文设计的方法将进一步完善混沌映射和 CMS 协议在继电保护通信中的应用,为相关领域的研究提供新的思路和方法,也能为其他需要防篡改的通信系统提供借鉴和参考。

1 继电保护通信报文安全防篡改方法设计

1.1 继电保护通信报文关键信息提取

为了实现继电保护通信报文安全的防篡改,需要对继电保护通信报文的关键信息进行提取。在提取的过程中,需要先对通信报文信息进行滤波处理,消除通信报文信息获取过程中的干扰和噪声^[7]。其滤波处理的具体过程如下所示:

$$y_i = \sum_{i=1}^n x_i \cdot N \tag{1}$$

式中, y_i 表示通信报文信息滤波处理的结果, x_i 表示原始的通信报文信息, N 表示滤波处理的窗口。通过上述公式,完成对通信报文信息的滤波处理。将上述滤波处理结果作为基础,提取出通信报文信息的关键信息^[8]。其具体提取结果如下所示:

$$y'_i = \frac{1}{N} \sum_{v=0}^{N-1} x_v \cdot W_v \cdot k_v \tag{2}$$

式中, y'_i 表示提取的通信报文关键信息, x_v 表示提取的通信报文关键信息, W_v 表示通信报文关键复数单位根, k_v 表示通信报文关键信息的幅值分量。通过上述公式,提取出通信报文的关键信息,将该提取结果作为基础,对不同通信报文之间的关联规则进行分析^[9]。其具体分析过程如下所示:

$$\left\{ \begin{aligned} S(y_A \Rightarrow y_B) &= \frac{S(y_A \cup y_B)}{T} \cdot y'_i \\ C(y_A \Rightarrow y_B) &= \frac{S(y_A \cup y_B)}{S(y_A)} \end{aligned} \right. \tag{3}$$

式中, $S(y_A \Rightarrow y_B)$ 表示不同通信报文信息同时出现的置信度, $S(y_A \cup y_B)$ 表示不同通信报文信息的数量, T 表示不同通信报文的内置项数量, $C(y_A \Rightarrow y_B)$ 表示不同通信报文之间的关联规则, $S(y_A)$ 表示通信报文的关键信息量。通过上述公式,完成对通信报文关键信息的提取和分析,将提取结果作为基础,为后续构建通信报文加密机制奠定基础。至此,继电保护通信报文关键信息提取的设计完成。

1.2 基于 CMS 协议和混沌映射的通信报文加密机制构建

将上述提取的通信报文关键信息作为基础,在

CMS 协议和混沌映射的作用下,构建通信报文加密机制。CMS 协议是国家电网公式标准的通信报文规范,其采用编码规则,能够提供高效的编码能力,有效提高数据的安全性和隐私性。将其应用于通信报文加密机制的构建中,能够将明文数据转换为密文数据,防止数据被非法获取或窃取。混沌映射是一种数学工具,能够将一个系统的状态映射到另一个系统中,具有极高的随机性和非线性特性,且敏感性极强^[10]。将其用于通信报文加密中,能够根据通信报文的变化,实时更换加密结果,进一步保证加密效果。在上述两种方法的作用下,对通信报文加密机制的构建过程具体如图 1 所示。

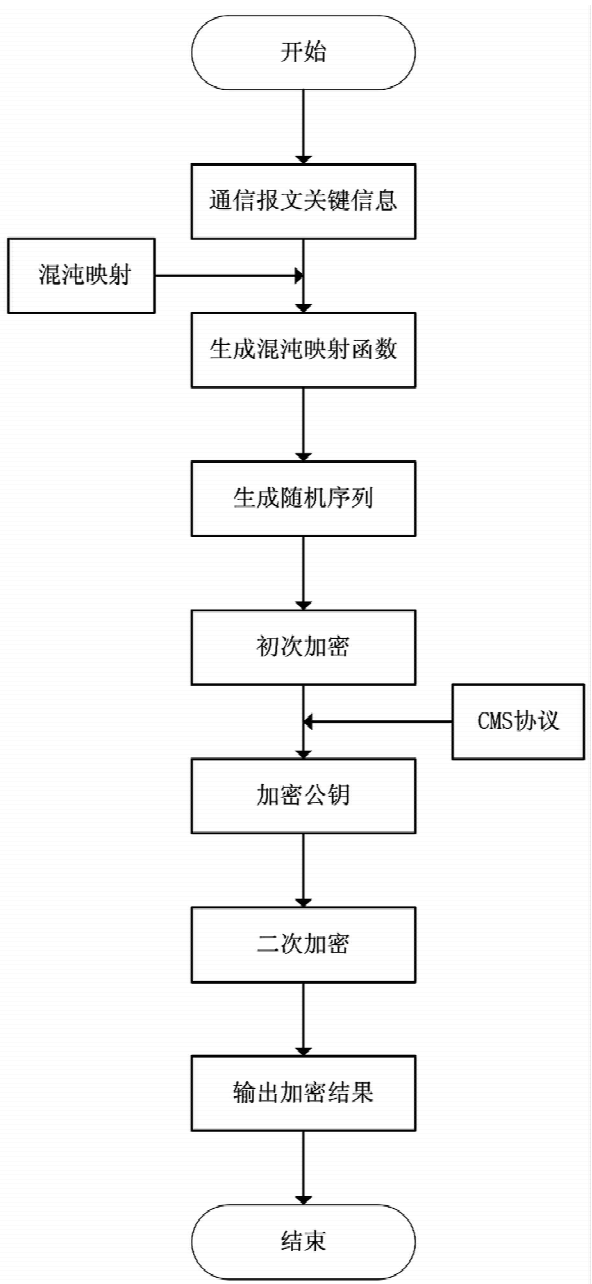


图 1 基于 CMS 协议和混沌映射的通信报文加密机制构建的具体过程

如图 1 所示,将上述提取的通信报文关键信息作为基础,根据通信报文的特性,生成对应的混沌映射函数,通过调整混沌映射的参数,对通信报文关键信息进行编码,生成随机数序列,并将生成的随机数序列作为加密密钥,对通信报文关键信息进行初次加密操作。在上述基础上,利用 CMS 协议,生成对应的公钥,对初次加密后的通信报文关键信息进行二次加密,进一步提高通信报文的加密效果,由此完成对通信报文加密机制的构建^[11]。在上述过程中,生成的混沌映射函数及设定的参数具体如下所示:

$$\begin{cases} M(c) = M_i \times m \\ U = \frac{C}{d_k} \\ D(i) = \frac{\sum_{i=1}^n [c_n - (f_n)_i]^2 \cdot U}{o} \cdot M(c) \end{cases} \quad (4)$$

式中, $D(i)$ 表示生成的混沌映射函数, $M(c)$ 表示混沌映射函数的认证参数, U 表示混沌映射函数的信息形态参数, M_i 表示混沌映射函数的数据差异参数, m 表示混沌映射函数的通信报文信息流总量, C 表示通信报文信息的安全度, d_k 表示通信报文信息的转换量, c_n 表示通信报文信息的维度, f_n 表示不同通信报文信息重置参数, o 表示通信报文的关键信息量化值。通过上述公式,完成对映射函数的生成,利用该映射函数,对通信报文信息进行初次加密^[12]。其初次加密过程如下所示:

$$H_i(c) = g(c) \cdot \sum_{u=0}^k g\left(\frac{k}{u}\right) \cdot D(i) \quad (5)$$

式中, $H_i(c)$ 表示利用混沌映射函数对通信报文信息进行初次加密的结果, $g(c)$ 表示通信报文关键信息的离散值, $g\{\}$ 表示通信报文信息加密的初始函数, k 表示通信报文关键信息的特征值, u 表示通信报文信息重置值。通过上述公式,完成对通信报文的初次加密,以此为基础,利用 CMS 协议对其进行二次加密^[13]。其二次加密的部分代码如图 2 所示。

如图 2 所示,在上述加密过程中,根据通信报文初次加密的结果,先生成对应的密钥对,再根据创建的 CMS 消息,创建对应的加密对象,使用密钥对对加密对象进行加密,并加密的信息进行传输。通过上述初次加密和二次加密的结果,完成对通信报文加密机制的构建^[14]。至此,基于 CMS 协

议和混沌映射的通信报文加密机制构建的设计完成。

```
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.asymmetric import padding
from cryptography.hazmat.primitives import serialization
from cryptography.hazmat.primitives.asymmetric import rsa
from cryptography.hazmat.primitives import cms
from cryptography.hazmat.primitives import constant_time
import base64
import os
private_key = rsa.generate_private_key(public_exponent=65537, key_size=2048)
public_key = private_key.public_key()
message = b"This is a test message"
encryptor = cms.ContentEncryptionAlgorithm("AES-256-CBC")
signer = cms.Signer(private_key, algorithm=hashes.SHA256())
signed_data = signer.sign(message)
encrypted_data = encryptor.encrypt(signed_data)
encrypted_message = encrypted_data + b"\n" +
public_key.public_bytes(encoding=serialization.Encoding.PEM,
format=serialization.PublicFormat.SubjectPublicKeyInfo)
print(base64.b64encode(encrypted_message).decode('utf-8'))
```

图 2 CMS 协议对通信报文信息二次加密的部分代码

1.3 继电保护通信报文信息完整性验证及修复处理

在上述设计的基础上,将设计的通信报文加密机制作为基础,根据加密结果,先对其进行解密处理,再对通信报文信息的完整性进行验证。在上述过程中,通信报文的解密过程如下所示:

$$\varphi(n) = (p-1) \times (q-1) \times H'_i(c) \tag{6}$$

式中, $\varphi(n)$ 表示通信报文信息的解密结果, p 表示混沌映射的解密密钥, q 表示 CMS 协议的解密密钥, $H'_i(c)$ 表示通信报文信息二次加密的结果。通过上述公式,完成对通信报文信息的解密处理,为判断通信报文信息是否被篡改,需要对解密后通信报文信息的完整性进行验证。其具体验证过程如下所示:

$$T_i = \left(\frac{l_1 - l_2}{R} + \frac{F_1 - F_2}{F_c} \right) \cdot \varphi(n) \tag{7}$$

式中, T_i 表示计算的通信报文信息浓度, l_1 、 l_2 分别表示通信报文信息在不同加密过程中的信息量, R 表示加密参数, F_1 、 F_2 分别表示通信报文信息在不同解密过程中的信息量, F_c 表示解密参数。通过上述公式,计算出通信报文的信息浓度,若计算结果与初始的通信报文信息浓度相同,则说明该通信报文信息未被篡改,反之,则通信报文信息已经被篡改。若通信报文信息已经被篡改,则需要对进行修复处理^[15]。其具体修复过程如下所示:

$$G_i = T_i \times MD(X) \tag{8}$$

式中, G_i 表示通信报文信息的修复处理结果, $MD(X)$ 表示修复函数。通过上述公式,完成对通

信报文信息的修复处理,由此实现对通信报文信息的防篡改。

至此,基于 CMS 协议和混沌映射的继电保护通信报文安全防篡改方法的设计完成。

2 实验测试

2.1 实验准备

为验证本文设计的基于 CMS 协议和混沌映射的继电保护通信报文安全防篡改方法在实际应用中的效果,进行实验测试。

以某电力系统为例,以 Windows10 为操作系统,主频为 2.5 GHz 的处理器为 CPU,容量为 2 TB 的为存储器,构建相应的实验环境,进行后续实验测试。其具体的实验环境如图 3 所示。



图 3 实验环境

如图 3 所示,在上述实验环境中,利用相关设备采集继电保护系统的数据,在计算机中进行处理和分析。并将处理结果作为基础,进行后续实验测试。实验中,利用本文设计的方法对上述通信报文信息进行加密和解密处理。其具体的加密和解密处理结果如图 4 所示。

如图 4 所示,在上述处理结果中,利用本文设计的方法进行加密后,加密后的密文呈现出非线性变化,能够更好地隐藏原始信息,可见其加密效果较好。解密后,能够很好地展现晕死的密文信息,解密效果较好。由此能够提高通信报文信息的防篡改能力。此外,实验中还设置了对照实验。其中,本文设计的防篡改方法为方法 1,文献[1]提出的基于区块链与改进 CP-ABE 算法的防篡改方法为方法 2,文献[2]提出的基于信息隐藏的防篡改方法为方法 3。

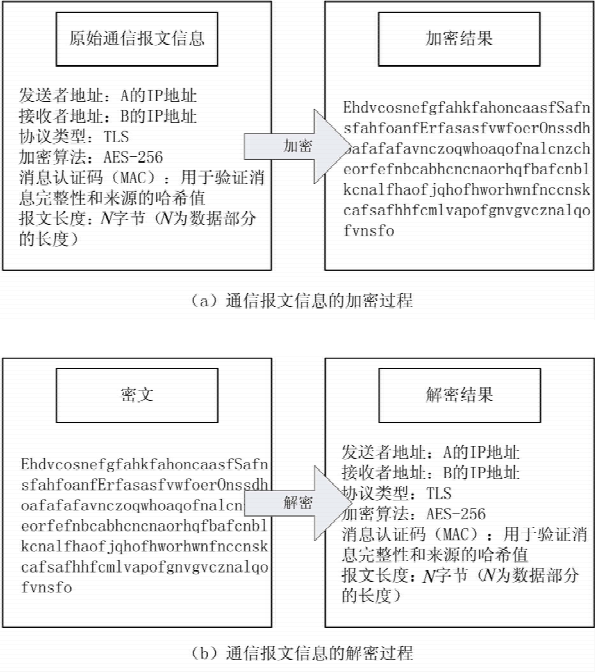


图 4 通信报文信息加密和解密处理结果

2.2 实验结果讨论

为验证上述三种方法在实际应用中的效果,以方法被篡改数据量为评价指标,进行实验测试。实验中,利用三种方法对不同数据体量的通信报文信息进行防篡改处理,统计其处理后的被篡改数据量。其具体统计结果如表 1 所示。

表 1 三种方法的防篡改结果			
数据体量/MB	三种方法的被篡改数据量/MB		
	方法 1	方法 2	方法 3
50	0.23	3.12	10.36
100	0.45	6.98	20.45
200	0.56	10.22	25.36
300	0.64	15.36	30.42
500	0.72	18.24	40.25
1000	0.99	22.54	50.69
2000	1.12	25.69	55.78
3000	1.32	30.12	62.37
5000	1.44	33.65	71.98
10000	1.99	40.28	83.65

如表 1 所示,在上述实验结果中,随着数据体量的增长,三种方法的被篡改数据量也在不断上升。其中,方法 1 的被篡改数据量较少,且上升速度较慢,方法 2 和方法 3 被篡改数据量较大,且上升速度较快。因此,本文设计的方法在实际应用中防篡改效果较好。

为进一步验证上述三种方法的性能,以方法的防篡改成功率作为评价指标,对比三种方法的应用效果。实验中,利用三种方法对不同数据体量的数据进行处理,统计其防篡改成功率。其具体统计结果如图 5 所示。

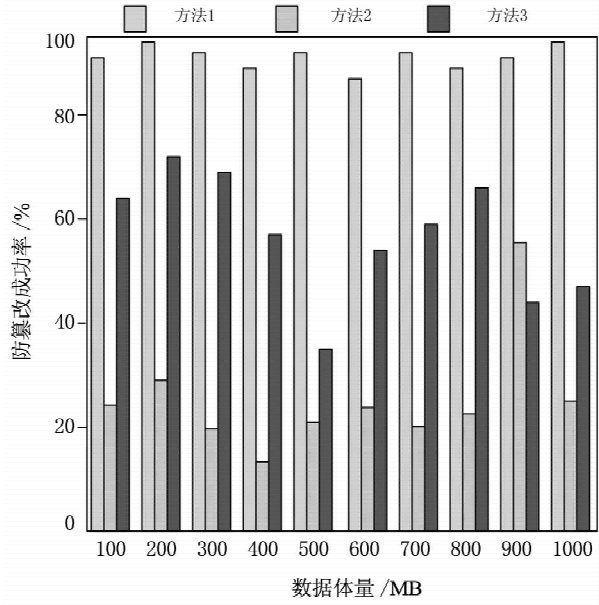


图 5 三种方法的防篡改结果

如图 5 所示,在上述实验结果中,方法 1 的防篡改成功率较高,均在 95% 以上,方法 2 和方法 3 的防篡改成功率较低,远低于方法 1。因此,本文设计的方法在实际应用中防篡改效果较好。

综上所述,本文设计的基于 CMS 协议和混沌映射的继电保护通信报文安全防篡改方法在实际应用中被篡改数据量较低,防篡改成功率较高,防篡改效果较好,能够更好地保证继电保护系统通信报文的信息安全,确保电力系统的稳定运行。

3 结 论

在电力系统的继电保护中,通信报文的准确性和完整性至关重要。由于通信过程中可能存在的安全威胁,报文的安全性需要得到充分保障。基于 CMS 协议和混沌映射的继电保护通信报文安全防篡改方法,旨在提供一种有效的解决方案,确保报文的完整性和真实性。这种方法结合了 CMS 协议的加密技术和混沌映射的随机性,为报文提供强大的保护层。在未来,可以进一步探索该方法的优化和改进,以及与其他安全技术的集成,以构建更为完善的继电保护通信安全体系。此外,随着技术

的不断发展,新的安全威胁和挑战也将不断涌现,因此需要保持对该领域的持续关注和更新。

参考文献

[1] 巫俊洁. 基于区块链与改进 CP-ABE 算法的知识产权数据防篡改方法 [J]. 信息与电脑(理论版), 2023, 35 (13): 40—42.

[2] 刘淑艳,李丽芬. 基于信息隐藏的无线共享网络数据防篡改方法 [J]. 兵器装备工程学报, 2022, 43 (4): 265—270.

[3] MERLO A, RUGGIA A, SCIOLLA L, et al. ARMAND: anti-repackaging through multi-pattern anti-tampering based on native detection[J]. Pervasive and Mobile Computing, 2021, 76(8):101—144.

[4] LI X. An anti-tampering model of sensitive data in link network based on blockchain technology[J]. Web Intelligence and Agent Systems, 2021, 53 (3): 19—38.

[5] 李克楠,邱海彬. 基于 ECC 算法的嵌入式 Linux 系统 ELF 可执行文件防篡改方法 [J]. 信息技术与信息化, 2022, 11 (7): 144—147.

[6] 李金讯,郭娜,林树鸿,等. 基于多重图像隐藏防伪标识公文防篡改的新方法研究 [J]. 电力大数据, 2021, 24 (9):1—8.

[7] 潘伟,李新建,陈飞. 工业互联网中远程通信数据防篡改检测方法 [J]. 电子设计工程, 2022, 30 (19): 84—87+92.

[8] 吉斌,昌力,朱丽叶,等. 区块链系统节点私钥泄露的电力数据防篡改方法与验证机制设计 [J]. 电力自动化设备, 2021, 41 (12): 87—94.

[9] 李克楠,邱海彬. 基于 ECC 算法的嵌入式 Linux 系统 ELF 可执行文件防篡改方法 [J]. 信息技术与信息化, 2022, 11 (7): 144—147.

[10] 郭现峰,李浩华,魏金玉. 基于 Fibonacci 变换和改进 Logistic-Tent 混沌映射的图像加密方案 [J]. 吉林大学学报(工学版), 2023, 53 (7): 2115—2120.

[11] 王艺杭,洪炎,肖志豪. 基于逻辑一无限折叠迭代混沌映射的图像加密 [J]. 佳木斯大学学报(自然科学版), 2023, 41 (4): 34—38.

[12] 熊爱明,李明倩,刘芳. 基于混沌映射的数据库信息隐私加密储存算法 [J]. 吉林大学学报(信息科学版), 2023, 41 (3): 459—464.

[13] 周明伟,阚忠良,蒋东华. 结合压缩感知和新混沌映射的图像加密方案 [J]. 计算机技术与发展, 2023, 33 (3): 63—70.

[14] 赵霞,张君毅,龙倩倩. 基于 Circle 混沌映射的 ISSA-ELM 神经网络室内可见光定位方法 [J]. 光学学报, 2023, 43 (2): 33—42.

[15] 秦秋霞,梁仲月,徐毅. 一种基于分段线性混沌映射的医学图像加密算法 [J]. 大连民族大学学报, 2023, 25 (1): 57—63.

(上接第 183 页)

参考文献

[1] 马记,许伟强,王荣昌,等. 基于改进 GRU-TCN 的磨煤机故障诊断算法[J/OL]. 计算机测量与控制, 1—8[2025—02—22].

[2] AGRAWAL V, PANIGRAHI B, SUBBARAO P. Review of control and fault diagnosis methods applied to coal mills[J]. Journal of Process Control, 2015, 32:138—153.

[3] 鲍晓华,王硕,关博凯,等. 基于 Mel-CNN 和电流频谱的电机轴承外圈故障声纹检测方法[J]. 电机与控制学报, 2024, 28 (11): 68—80.

[4] 胡赵宇,李喆,蒙国勇,等. 基于 Conv-TasNet 的变压器音频降噪识别网络[J]. 电气自动化, 2024, 46(6): 82—85.

[5] 庄小亮,李乾坤,刘紫罡,等. 基于改进 MFCC-OCSVM 和贝叶斯优化 BiGRU 的 GIS 异常工况声纹识别算法[J]. 南方电

网技术, 2025, 19(1): 30—40.

[6] 齐子豪,全杰,张中浩,等. 基于多粒度知识特征和 Transformer 网络的电力变压器故障声纹辨识方法[J/OL]. 中国电机工程学报, 1—13[2025—03—07].

[7] 庄小亮,李乾坤,刘紫罡,等. 基于改进 MFCC-OCSVM 和贝叶斯优化 BiGRU 的 GIS 异常工况声纹识别算法[J/OL]. 南方电网技术, 1—10[2025—02—22].

[8] 崔佳嘉,马宏忠. 基于改进 MFCC 和 3D-CNN 的变压器铁心松动故障声纹识别模型[J]. 电机与控制学报, 2022, 26(12): 150—160.

[9] 欧阳城添,袁瑾. 基于学习矢量量化的空调压缩机声纹诊断方法[J]. 计算机工程与设计, 2021, 42(9): 2634—2641.

[10] 杨婷婷,罗海玉,李浩千,等. 基于 IWOA 优化 TCN 模型的磨煤机故障预警研究[J/OL]. 华北电力大学学报(自然科学版), 1—9[2025—02—22].