基于 Logistic 映射的通信网络信息安全加密方法

吴 倩[1] 杜柱石[1] 王立岩[1]
WU Qian DU Zhushi WANG Liyan

摘 要 传统加密算法加密模式和密钥管理相对固定，无法适应不同类型的数据和通信网络环境，导致明文信息加密不全面，安全性降低。为此，文章提出一种基于 Logistic 映射的通信网络信息安全加密方法。通过运用网络分析技术，识别通信网络中的关键节点，建立一个包含这些节点的覆盖集合，以实现节点间的最优连接和路径规划，确保信息在传输过程中的高效与稳定。结合 Logistic 映射算法，将转换明文信息的数字序列，并生成复杂的通信网络信息密文，进一步增强节点间信息传输的加密强度。为了确保通信过程中信息的机密性、完整性和认证性，采用 TLS/SSL 协议来进行通信网络节点的密钥交换和加密通信传输。实验结果表明，该方法能够成功地将待传输的明文信息转换为复杂的密文信息，且加密传输信息的丢失率为 0，有效提升通信网络信息安全性，这一结果充分验证了本方法在保障信息安全传输方面的卓越性能与可靠性。

关键词 Logistic 映射；通信节点；密文；加密方法；安全；通信网络信息

doi：10.3969/j.issn.1672-9528.2024.12.013

0 引言

数字化时代，通信网络信息安全成为不容忽视的关键问题。信息传输量的急剧增加，使网络攻击手段日益复杂多变，对信息安全提出了严峻挑战。目前的加密方法，尽管在一定程度上保障了信息安全，但在面对高级持续性威胁（APT）等新型攻击时，其局限性逐渐显现。因此，探索更为高效、安全的信息加密技术成为当前研究的热点。

当前研究中，石小兵 [1] 通过时域分析提取通信数据的特征向量，利用 AES 算法对通信数据的明文进行加密，再用 ECC 算法对 AES 密钥进行加密，从而生成密钥密文，实现双重加密保护。虽然 AES 和 ECC 算法本身也具有较高的安全性，但密钥在加密过程中相对固定，尤其是在密钥管理不善的情况下，存在被破解的风险，同时，密钥管理和分发机制仍需进一步优化，以确保密钥的安全性和高效性。张雷 [2] 结合身份认证、数据加密、安全审计与灾备机制，设计了一套全面的安全防御体系。通过对系统通信过程的数据进行加密处理，有效防止了敏感信息在传输过程中的泄露风险，提高了系统的整体安全性。在实际应用中，该方法需要管理多种密钥，包括身份认证密钥和数据加密密钥等，增加了密钥管理的复杂度。随着网络安全威胁的不断演变，该方法的安全性逐渐减弱，面临着被破解的风险。

1. 中国人民解放军 91202 部队 辽宁葫芦岛 125000

为实现对研究成果的深化，提高网络信息的安全性，本文提出一种基于Logistic映射的通信网络信息安全加密方法。通过引入 Logistic 映射算法进行信息加密，克服了传统加密方法的不足，提高了加密强度、灵活性和安全性，能够更好地满足现代通信网络对信息安全的需求。

1 建立通信网络信息路径节点覆盖集合

在通信网络信息安全加密过程中，本文旨在构建一个高效的节点覆盖集合，以识别并加固通信网络中的关键节点。通过这种方式，让信息在传输时精准经过已实施安全加固举措的节点，大幅降低信息在传输途中被非法截获或恶意篡改的风险，确保信息传输的安全性与完整性。通过设计的节点覆盖策略，能够在网络中建立起一个坚固的安全传输通道，有效保护信息在传输过程中的完整性和机密性 [3]。

选择通信网络中关键节点作为信息路径的起点和终点，设计从起点到终点的信息路径，确保路径上的节点能够连续覆盖。所选的节点覆盖度计算公式为：

$$C=\frac{\left|U_p \in P\left\{n\middle|n \in p\right\}\right|}{N} \tag{1}$$

式中：C 表示节点覆盖度；U 表示所有通信路径中不同节点的总数；p 表示节点覆盖的第 p 条路径；P 表示节点覆盖路径集合；n 表示通信网络中的节点 n；N 表示通信网络中的节点集合。在确保所选节点满足通信需求的前提下，将通信路径长度最小化作为主要目标，构建了一个目标函数，旨在寻

找覆盖所有关键节点的最短路径[4]。该目标函数表达式为：

$$L_{\min}=\sum_{p\in P}L(p)\cdot C \tag{2}$$

式中：$L_{\min}$ 表示最小化路径长度；L 表示所有路径的总长度。在建立目标函数的基础上，建立最小生成树，生成树中应包含图中所有顶点，并且边的总权重最小。根据生成树的节点分布，建立高效通信网络，确保所有节点连通、覆盖[5]。以此为依据，对目标函数进行约束，计算生成树的最小化边的总权重，计算公式为：

$$W=\sum_{M}\frac{w(u)}{L_{\min}} \tag{3}$$

式中：W 表示最小化边的总权重；M 表示最小生成树；w 表示 MST 中的一条边；u 表示 w 的权重。输出总权重最小化边对应的节点，根据通信起点与终点的位置，对节点进行排序，得到通信网络信息路径节点覆盖集合。

2 基于 Logistic 映射生成通信网络信息密文

仅依靠节点覆盖策略无法完全抵御复杂的网络攻击和窃听手段。为了进一步增强节点间信息传输的加密强度，在节点覆盖策略下的安全传输通道中，本文应用 Logistic 映射算法进行节点信息加密。Logistic 映射作为一种混沌映射方法，具有高度的复杂性和不可预测性，使得加密后的密文难以被破解。通过将明文信息转换为数字序列并进行 Logistic 映射加密，可以满足不同场景下的信息安全需求，提高信息的加密强度[6]。

在信息发送方发送通信网络明文信息后，将其在传输通道内转换为密文，确保信息在通信网络中传输的安全性。此过程如图 1 所示。

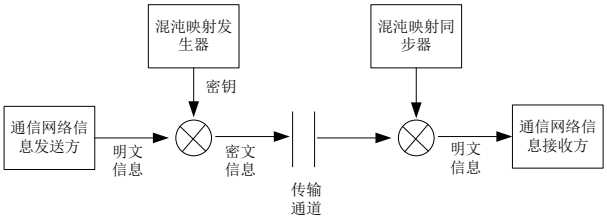


图 1 基于混沌映射生成通信网络信息密文

在此过程中，选择 Logistic 映射作为信息加密中的混沌映射方法，根据通信网络信息路径节点覆盖集合，对节点进行混沌映射[7]。映射过程计算公式为：

$$K(i)=\frac{m(i)\cdot k(i)}{x(W+1)} \tag{4}$$

式中：K 表示节点混沌映射；i 表示第 i 个数据序列；m 表示当前状态，在 [0, 1] 区间内；k 表示控制参数，通常在 [0, 4] 区间内，但混沌行为主要在 [3.57, 4] 内。完成通信路径节点的映射后，选择通信网络明文信息中的初始值和控制参数作为密钥的核心部分[8]。所选信息为文本信息时，将每个字符的 ASCII 码转换为数字；所选的信息为图像信息时，将像素值转换为数字序列。通过这种方式，将明文信息（如文本、图像等）转换为数字序列，以此实现对明文信息的预处理[9]。此过程计算公式为：

$$Z(i)=\left[K(i)\cdot 10^{9}\right]\bmod 256 \tag{5}$$

式中：Z 表示明文信息的数字序列；mod 表示字符的 ASCII 码值。在此基础上，使用混沌序列作为密钥流，通过异或操作，迭代混沌映射生成足够长的数据序列，将密钥流与明文序列进行结合，实现密钥流的生成[10]。在此过程中，将某文本明文信息转换为 0~255 之间的整数，此过程计算公式为：

$$A=\frac{Z(i)}{a(i)\oplus B} \tag{6}$$

式中：A 表示密钥流；a 表示文本明文信息转换系数；$\oplus$ 表示异或操作；B 表示明文信息中的序列值。对于密钥流中的每个文本与数据，使用密钥流中的对应序列值，对其进行加密，以此生成通信网络信息密文[11]。密文生成过程公式为：

$$F=\boldsymbol{S}(\boldsymbol{s}'+1)\cdot A^{t} \tag{7}$$

式中：F 表示通信网络信息密文；$\boldsymbol{S}$ 表示通信网络信息矩阵；$\boldsymbol{s}'$ 表示单元矩阵；t 表示密文生成中的迭代次数。通过上述方式，完成基于 Logistic 映射生成通信网络信息密文。

3 网络信息安全加密通信传输

在节点覆盖策略下的安全传输通道中，尽管 Logistic 映射加密为数据内容提供了高强度的保密性和完整性保护，但通信网络的整体安全性还要求确保通信双方身份的真实性、通信过程的保密性以及密钥交换的安全性。为此，本文采用了 TLS/SSL 协议来实现通信网络节点的密钥交换和加密通信传输，从而确保信息在传输过程中不会被窃听、篡改或伪造。通过这种方式能够全方位地保护信息的安全，确保其在复杂的网络环境中依然能够安全无虞地传输。

在完成密文的生成后，利用 TLS/SSL 协议进行通信网络节点的密钥交换[12]。TLS/SSL 协议在通信中主要起到节点与数据的握手作用，握手过程中，使用通信网络的公钥，交换对称加密密钥，实现对通信节点覆盖的公钥加密。此过程计算公式为：

$$f=F^{e}\cdot\bmod d \tag{8}$$

式中：f 表示公钥加密；e 表示公钥中的指数；d 表示公钥和私钥的模。完成节点握手加密后，利用集成在节点的私钥，在传输终端进行密文的解密，解密过程计算公式为：

$$D=E_{\text{key}}(f,\boldsymbol{V}) \tag{9}$$

式中：D 表示接收终端解密；E 表示握手次数；key 表示对称密钥；$\boldsymbol{V}$ 表示初始化向量，用于增加加密的随机性。为确

保通信网络信息在传输后的完整性与真实性，TLS/SSL 将使用 HMAC 消息认证码，验证消息在传输过程中是否被篡改。其中 HMAC 消息认证码的表达式为：

$$MAC = HMAC_{key}(D) \quad (10)$$

式中：MAC 表示 HMAC 消息认证码；HMAC 表示认证信息。确保信息未被篡改的条件下，对输出的数据进行循环冗余校验，在接收终端的物理层或数据链路层，进行数据循环验证 [14]。此过程计算公式为：

$$Y = I(\Sigma h(i)\text{-}2^{n}\cdot MAC) \quad (11)$$

式中：Y 表示冗余验证；I 表示循环次数；h 表示校验和。输出通过校验的数据集合，完成网络信息安全加密通信传输，实现加密方法的设计。

4 对比实验

4.1 实验准备

完成上述设计后，为实现对该方法的检验，选择某大型通信服务中心作为研究试点，该服务中心日均处理通信数据量高达 10 TB，覆盖用户群体超过 500 万。其网络架构采用先进的 5G 与光纤混合技术，确保了数据传输速率平均达到 500 Mbit/s 以上。用户满意度调查中，网络速度满意度高达 92%。此外，该中心还部署了智能路由与负载均衡系统，有效降低了网络拥堵率至不足 1%，保障了高峰时段的通信稳定性。为确保实验结果的真实性，对此通信网络服务中心的网络建设进行分析，如表 1 所示。

表 1 通信网络建设情况

序号	项目	参数
1	接入网接入方式	光纤接入、无线接入、混合接入
2	光纤接入用户数	截至 2023 年底，光纤接入 (FTTH/O) 端口达到 10.94 亿个，同比增长显著
3	传输介质	光纤光缆为主
4	光缆线路总长度	全国光缆线路总长度达 6432 万公里，其中长途光缆线路 114 万公里
5	算力规模	对外提供的公共基础算力规模超 26E Flops

在深入试点单位的研究中发现，尽管加密技术在保护通信数据方面发挥着关键作用，但仍存在的不足，一方面，现有加密算法的安全性随时间和技术进步而减弱，另一方面，加密系统的实现和维护存在漏洞，未能及时更新或修补已知的安全缺陷。

4.2 实验步骤

在上述内容的基础上，设计对比实验，对本文方法展开测试。选择支持所需编程语言的 Python 3.x 系统，通过命令行运行 pip install cryptography 指令进行数据加密库的安装。搭建测试环境，技术参数如表 2 所示。

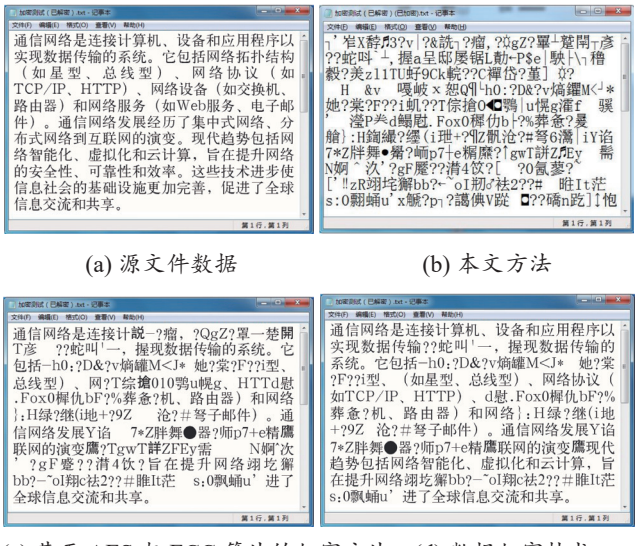
表 2 测试环境技术参数

序号	项目	参数
1	密钥长度	256 位
2	密钥管理标准	FIPS 140-2 Level 3 标准
3	数据传输速率	1 Gbit/s
4	带宽要求	＞ 100 Mbit/s
5	防火墙性能	吞吐量≥ 1 Gbit/s 并发连接数≥ 100 000
6	安全审计系统	支持日志存储时间≥ 90 天， 支持多种日志格式
7	VPN 性能	加密速度≥ 500 Mbit/s
8	安全协议支持	SSL/TLS 1.2 及以上，IPsec、SSH 等

完成测试环境的部署后，在试点单位历史库中调用部分数据，将其作为本次实验中的样本数据。并引入文献 [1] 中提出的基于 AES 与 ECC 算法的加密方法和文献 [2] 中提出的数据加密技术作为对比方法，与本文方法展开加密效果对比分析。旨在全面对比不同加密方法在保障通信网络信息安全性方面的性能与效果。

4.3 实验结果与分析

为了验证加密传输过程中通信网络信息的安全性。本次实验收集了加密传输过程中的相关数据，分别利用本文方法、基于 AES 与 ECC 算法的加密方法和数据加密技术对所收集的加密传输数据进行加密处理。各方法的加密处理结果如图 2 所示。



(a) 源文件数据　(b) 本文方法

(c) 基于 AES 与 ECC 算法的加密方法　(d) 数据加密技术

图 2 网络信息安全加密效果

从图 2 结果可以看出，本文方法能够成功地在信息通信传输阶段将明文信息（源文件数据）转换为复杂的密文信息；而采用基于 AES 与 ECC 算法的加密方法和数据加密技术对明文信息进行加密处理，处理后的结果存在明显的明文信息内容，加密全面性较差，导致在面对攻击时，易发生信息泄露，

安全性低。由此，经上述分析表明，所提方法能够完整的对明文信息进行加密，加密效果较好，在保障通信网络信息安全方面具有卓越的性能。

为进一步验证所提方法的加密强度，在上述各方法所得密文信息的基础上，设置传输时间为 8 s，在传输的第 3 s、第 4 s 和第 6 s 引入攻击，利用信息的丢失率来衡量加密传输数据的完整性。其丢失率越低，说明方法的加密强度越强，可有效抵抗攻击，确保通信网络信息的安全性。则在本文方法、基于 AES 与 ECC 算法的加密方法和数据加密技术加密下，信息丢失率结果如图 3 所示。

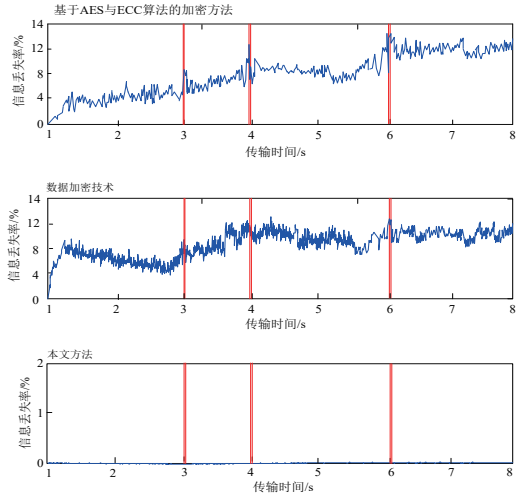


图 3 各加密方法下的信息丢失率结果

根据图 3 结果可知，采用本文方法进行加密处理后得到的密文信息，在存在攻击的环境下进行传输，其信息丢失率为 0，可有效抵抗攻击。而在基于 AES 与 ECC 算法的加密方法和数据加密技术加密下，其传输的密文信息易受到攻击影响，使得信息泄漏的风险增加，其丢失率随传输时间以及攻击次数的增加，呈现阶段性的上升趋势。由此，经上述分析表明，本文方法具有较强的加密强度，可抵抗攻击，防止信息泄漏，保障通信网络信息传输的安全性。

5 结语

Logistic 映射，其输出的复杂且难以预测的序列，极大地增强了加密算法的复杂性和安全性，使得基于 Logistic 映射的加密方法能够超越传统加密技术的局限性。本实验验证的结果表明，本文方法能够成功将待传输的明文信息转换为复杂的密文信息，具有较好的加密效果，且加密传输信息的丢失率为 0，确保了通信网络的信息安全性。这一创新成果不仅丰富了信息安全领域的研究内容，也为应对日益复杂多变的信息安全威胁提供了一种更为高效、可靠的解决方案。

参考文献：

[1] 石小兵 . 基于 AES 与 ECC 混合算法的计算机网络通信数据安全加密方法 [J]. 常州工学院学报 , 2024, 37 (3): 6-10.

[2] 张雷 . 基于数据加密技术的医院信息管理系统通信安全防御方法 [J]. 电脑编程技巧与维护 , 2024(6): 158-161.

[3] 郎加云 , 丁晓梅 . 基于可搜索加密技术的分布式数据库安全访问多级控制算法 [J]. 吉林大学学报 (信息科学版), 2024, 42 (3): 531-536.

[4] 王宝永 . 基于多因素认证与动态加密的物联网安全与隐私保护协议研究 [J]. 信息与电脑 , 2024, 36 (9): 196-198.

[5] 董汉霞 , 吕东锋 , 商乙山 . 多种技术支持下数字化档案数据加密信息安全系统的设计与实现 [J]. 网络安全技术与应用 , 2024(4): 33-35.

[6] 林雨康 , 刘云皓 , 王文丽 . 基于神经网络与全同态加密的多生物特征融合安全认证方案 [J]. 电子制作 , 2024, 32 (7): 68-71.

[7] 柏松 , 王晓勇 , 胡胜利 . 基于区块链和代理重加密的医疗物联网数据安全管理系统 [J]. 中国计量大学学报 , 2024, 35 (1): 80-88.

[8] 高丽萍 , 季仕承 , 郝玉忠 . 基于云端辅助的国土资源数字化档案信息自动加密方法 [J]. 自动化技术与应用 , 2024, 43 (2): 85-88.

[9] 蔡茗静 . 基于混沌理论的供电企业数字化全面预算信息安全加密算法 [J]. 信息与电脑 , 2023, 35 (24): 67-69.

[10] 蒲亮 , 姚树智 , 敖继威 . 基于方差特征选择与 3DES 加密算法的医院信息数据安全防御系统设计 [J]. 计算机测量与控制 , 2024, 32 (5): 253-259.

[11] 邹易奇 . 基于计算机属性加密的 Linux 安全模块访问控制实现及系统测试 [J]. 科技与创新 , 2023(21): 140-141+146-147.

[12] 郑伟 , 张迪 , 原昊 , 等 . 基于轨道角动量全息和频移的大容量光学信息加密技术 [J]. 红外与激光工程 , 2023, 52 (7): 332-341.

[13] 田如意 , 顾风军 , 彭坤 , 等 . 基于一维 Logistic 映射和二维 Tent 映射双混沌思路的网络信息加密 [J]. 计算机测量与控制 , 2023, 31 (6): 280-286.

[14] 漆明欣 . 基于多特征信息融合的医院统战档案信息存储加密系统设计 [J]. 无线互联科技 , 2022, 19 (21): 92-94.

【作者简介】

吴倩（1989—），女，河北秦皇岛人，本科，助理工程师，研究方向：信息安全技术和信息与通信工程。

杜柱石（1979—），男，辽宁朝阳人，本科，高级工程师，研究方向：舰艇装备管理和水面靶标应用研究。

王立岩（1985—），男，辽宁锦州人，本科，中职工程师，研究方向：通信工程、雷达工程。

（收稿日期：2024-09-18）