

文章编号:1671-5896(2026)04-0776-07

大规模移动网络通信双混沌数据安全加密算法

钟伟华, 黄达辉, 王欣霖, 丘创勋

(梅州市人民医院 数据中心, 广东 梅州 514031)

摘要: 为有效确保网络通信数据的安全性, 以大规模移动网络通信中的图像数据为研究对象, 提出一种双混沌数据安全加密算法。采用新的填充曲线用于大规模移动网络通信图像数据的全局置乱, 通过改进的约瑟夫遍历方法对相邻像素实施比特级置乱, 并引入双向密文反馈实现图像数据的初始加密。将双混沌和 Arnold 变换有效结合, 利用密钥形成初始状态值, 将其用于控制双混沌系统形成一系列混沌矩阵, 并作为辅助对图像像素进行位置变换和数值改变, 再将图像的各个分量分别实施 Arnold 变换, 采用设置的置乱-扩散加密算法对水平连接后的图像进行处理, 最后对图像像素实施异或操作(XOR: exclusive OR), 实现大规模移动网络通信双混沌数据安全加密。实验结果表明, 所提算法可以获取满意的加密效果, 同时还具有良好的明文敏感性。

关键词: 大规模移动网络通信; 双混沌系统; 图像数据; 安全加密; Arnold 变换

中图分类号: TP309.7

文献标志码: A

Security Encryption Algorithm for Dual Chaotic Data in Large-Scale Mobile Network Communication

ZHONG Weihua, HUANG Dahui, WANG Xinlin, QIU Chuangxun

(Data Center, Meizhou People's Hospital, Meizhou 514031, China)

Abstract: In mobile network communication, image data usually needs to be transmitted and shared with multimedia data such as audio and video. Image data often contains personal information, such as photos, videos, etc. In order to ensure the security of network communication data effectively, a double chaotic data encryption algorithm is proposed based on the image data modified in large-scale mobile network communication. A new filling curve is used for global scrambling of image data in large-scale mobile network communication. An improved Joseph ergodic method is used to expand the bit-level scrambling of adjacent pixels, and bidirectional ciphertext feedback is introduced to realize the initial encryption of image data. Double chaos and Arnold transform are effectively combined. The initial state value is formed by using the key, which is used to control the double chaos system to form a series of chaos matrix, the position transformation and value change of image pixels are expanded as an aid, and each component of the image is expanded by Arnold transform. The set scramble-diffusion encryption algorithm is used to process the horizontal connected image, and finally the XOR (exclusive OR) operation is performed on the image pixels to realize the security encryption of double chaos data in large-scale mobile network communication. Experimental results show that the proposed algorithm can obtain satisfactory encryption effect and has good plaintext sensitivity.

Key words: large-scale mobile network communication; double chaotic system; image data; secure encryption; Arnold transformation

收稿日期: 2024-04-26

基金项目: 广东省重点领域研发计划基金资助项目(2020B0706020010)

作者简介: 钟伟华(1988—), 男, 广东梅州人, 梅州市人民医院工程师, 主要从事网络安全研究, (Tel)86-15820354566 (E-mail) zhongweihua566@163.com。

0 引言

图像数据具有二维自相似性、大数据量等特性,其使传统的加密算法在处理图像数据时不能充分发挥其效用。由于传统的加密算法通常将图像数据视为一维数据流进行处理,忽略了其二维结构和自相似性,可能导致加密效果不佳或计算效率低下。而针对图像数据的特殊性质,研究专门的图像加密算法能更有效地保护图像信息的安全。目前,图像数据在网络通信中的传输量日益增大,并且其中可能包含重要的个人信息、商业机密或国家安全信息,一旦泄露或被篡改,将可能造成严重的后果。因此,研究图像数据加密算法对保护这些敏感信息的安全至关重要^[1-2]。

目前人们对图像加密^[3-4]方面的内容进行了大量研究,并且取得了十分显著成果。郑思飞等^[5]将矢量量化和离散小波变换作为基础,利用“明文-明文”的伪装加密方法对图像实施加密处理。虽然该方法可以隐藏数据的真实内容,但伪装后的明文和原始明文在结构上相似,增加了被攻击识别的风险,安全性较低。石金晶等^[6]通过量子细胞神经网络形成的混沌信号控制量子的 Arnold 变换以及交换量子等,将全部操作作用于明文图像中,进而得到密文图像。但其量子加密安全性过于依赖量子密钥的分发以及管理,假设量子密钥在传输或存储过程中存在窃取或篡改的情况,整个加密系统将面临被破解的风险,最终影响加密效果的安全性。曾萍等^[7]采用包围盒分割算法提取体素,通过三线性插值法计算等值面和体素间的交互信息提升重建精度,同时引入基于分数阶 Lorenz 混沌的三维模型加密方案完成加密处理。但其在比较复杂的情况下,安全性比较低,获取的加密效果不理想。Wang 等^[8]主要通过二维正弦嵌入耦合映射完成数据加密处理。但其抗攻击能力比较差,对部分攻击无法有效抵抗,导致加密数据的安全受到威胁。

双混沌系统作为一种新兴的加密技术,在图像数据加密领域具有广阔应用前景。混沌系统具有随机性、对初值敏感性和不可预测性等特点,其使混沌加密算法在图像加密中能提供更高级别的安全性。为保证大规模移动通信网络通信图像数据的安全性,笔者提出一种大规模移动通信双混沌数据安全加密算法。

1 大规模移动通信双混沌数据安全加密算法

1.1 大规模移动通信网络通信图像数据初始加密

为有效实现大规模移动通信网络通信双混沌数据安全加密,对通信图像数据实施2次加密处理,主要通过填充曲线和相邻像素比特置乱的方式完成加密。

空间填充曲线以其出色的扫描效率,在多维索引等研究领域得到了广泛应用,尤其在图像快速置乱方面表现突出。通过该技术,能迅速访问通信图像中的每个像素,并按照线性方式重新排列,使原始像素序列被打乱并重组,从而生成一幅全新的图像。为进一步增强通信图像数据的安全性,将填充曲线与相邻像素比特置乱技术相结合,共同作用于加密处理过程。这种组合技术能确保通信图像在加密过程中得到全方位保护,阻止任何未经授权的访问和破解。具体操作步骤如下。

1) 密钥生成。使用密钥加密是强化加密通信对抗已知明文攻击的关键手段,通过明文图像的哈希值精确设定混沌系统的起始状态。只要图像发生微小变动,其哈希值就会发生改变,进而触发混沌系统初始值的相应变化。通过对自适应密钥的处理,确保其精确地落在混沌系统的有效区间内,从而生成高度安全的密钥。

2) 像素置乱。虽然填充曲线是一种便捷的方法,但现有的部分填充曲线还存在短板。为此,提出一种全新的填充曲线。其以独特的V字型为基础,严格遵循“外围-内部-外围”的扫描顺序,确保每1个像素都能被全方位地访问,不存在任何遗漏。特别是针对连续3个以上像素点的区域,通过采取多方向扫描策略,可以有效防止局部置乱的发生。经过两次V型无线连续扫描后,原始相邻的像素几乎不再相邻,大大增强了置乱效果和安全性。

3) 相邻像素比特置乱。在步骤2)中,虽然通过像素级置乱破坏了通信图像中相邻像素间的相关性,但像素值本身并未发生任何变动,导致加密后的图像在面对统计学攻击时显得相当脆弱。针对上述

问题,笔者提出一种相邻像素比特置乱的创新方法,将约瑟夫遍历和混沌序列两者有效结合。利用

$$\begin{cases} n_{x_i'} = \text{mod}(f_{\text{floor}}(10^{14} \times n_{x_i}), 16 + 1), \\ n_{y_i'} = \text{mod}(f_{\text{floor}}(10^{14} \times n_{y_i}), 8 + 1) \end{cases} \tag{1}$$

对混沌系统形成的伪随机序列 N_X 和 N_Y 中的元素进行处理,设定约瑟夫的起点 $n_{x_i'}$ 和步长 $n_{y_i'}$ 。其中 n_{x_i} 和 n_{y_i} 表示混沌序列。

4) 像素扩散。在完成步骤3)后,微小的明文变动将引发像素的广泛扩散,使整个密文产生显著变化。在加密通信图像时,充分利用混沌序列的独特性质,这不仅依赖于序列本身的值,还需结合图像中前一个像素的信息。即使明文图像只有微小的变化,这种双重调整机制也能确保整个加密后的图像存在显著差异。为进一步增强通信图像的安全性,设计一种方法使密钥序列与明文图像紧密相关,进而大大增加破解难度。在像素扩散过程中,采取正向和反向两种扩散方式,通过有效增强加密的复杂性,使加密效果更加均匀且难以预测。为增强通信图像的安全防护,实施密钥序列与明文图像的高度绑定策略。像素扩散过程被划分为正向和反向两种模式。在设定混沌的初始状态后,启动混沌系统的迭代过程,生成两个特定长度为 $a \times m$ 的序列 n_z 和 n_w 。通过

$$\begin{cases} n_{z_i'} = \text{mod}(f_{\text{floor}}(10^{14} \times n_{z_i}), n_{x_i'}), \\ n_{w_i'} = \text{mod}(f_{\text{floor}}(10^{14} \times n_{w_i}), n_{y_i'}) \end{cases} \tag{2}$$

对序列元素进行处理,获得 $n_{z_i'}$ 和 $n_{w_i'}$ 。其中 n_{z_i} 和 n_{w_i} 表示混沌序列。

在大规模移动网络中,针对给定的通信图像以及序列矩阵,对正向和反向扩散过程分别利用

$$c_{i,j} = \begin{cases} \text{mod}(c_{i,j}n_{w_i'} + R, 256) \oplus N, \\ \text{mod}(c_{i-1,a}n_{w_i'} + R, 256) \oplus N, \\ \text{mod}(c_{i,j-1}n_{w_i'} + R, 256) \oplus N, \end{cases} \tag{3}$$

$$d_{i,j} = \begin{cases} \text{mod}(d_{i,j}n_{z_i'} + S, 256) \oplus N, \\ \text{mod}(d_{i-1,a}n_{z_i'} + S, 256) \oplus N, \\ \text{mod}(d_{i,j-1}n_{z_i'} + S, 256) \oplus N \end{cases} \tag{4}$$

给出。其中 R 表示正向序列矩阵; S 表示反向序列矩阵; N 表示图像矩阵。

通过上述4个步骤实现大规模移动网络通信图像数据的初始加密。

1.2 大规模移动网络通信双混沌数据二次加密

考虑初始加密过程包含了4个步骤,由于步骤较多,攻击可能产生在每个步骤中。因此,为确保大规模移动网络通信数据具有更高的安全性,还需要进一步对通信图像数据^[9]实施加密,采用双混沌和Arnold变换完成二次加密处理。其中通信图像数据二次加密的结构如图1所示。

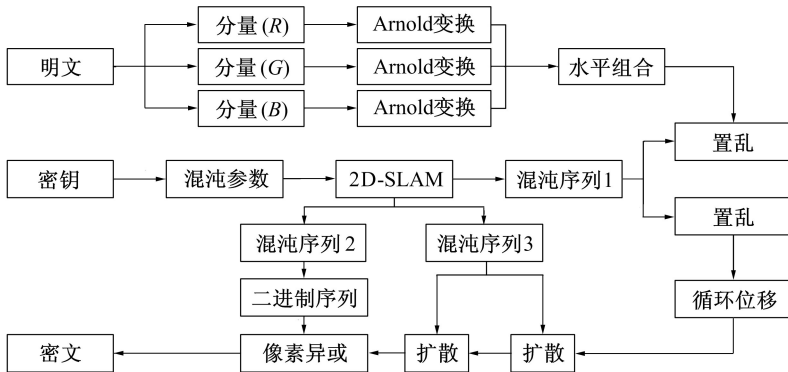


图1 大规模移动网络通信双混沌数据安全加密架构

Fig.1 Architecture diagram of secure encryption for dual chaotic data in large-scale mobile network communication

理论上,只有密钥的长度大于100才可有效抵御穷举攻击。综合考虑,将密钥长度 L 设定为216位,如下:

$$L = \{x_0, y_0, r, c_1, c_2\}, \quad (5)$$

其中 (x_0, y_0) 表示初始状态值; r 表示干扰参数; c_1 和 c_2 表示 r 的扰动参数。设定 x_0 、 y_0 和 r 三者的大小均为52 bit,采用IEEE754浮点数标准的方式将其转换为浮点数。假设 $\{e_1, e_2, \dots, e_{52}\}$ 为一个52位的二进制字符串,通过

$$G = L \sum_{i=1}^{52} e_i 2^{-i} \quad (6)$$

给出详细的转换过程 G 。通过对参数 r 实施扰动后即可获取 $r^{(1)}$ 和 $r^{(2)}$,如下:

$$\begin{cases} r^{(1)} = 0.9 + \text{mod}(rc_{i,j}, 0.1), \\ r^{(2)} = 0.9 + \text{mod}(rd_{i,j}, 0.1). \end{cases} \quad (7)$$

第1轮双混沌系统的初始状态值 $(x_0^{(1)}, y_0^{(1)})$ 是由初始状态 (x_0, y_0) 转换获取的,并将最后一轮迭代获取的数据用于下一轮的初始状态值。在初始值以及参数的控制下,利用双混沌系统可以形成比较复杂的混沌序列,根据置乱-扩散和像素异或等相关操作对通信图像数据进行有效且安全的加密处理^[10]。

分别通过置乱、扩散和加密3个步骤完成加密处理。

1) 步骤1 置乱处理。

① 对混沌序列 T 分别进行列顺序和行顺序排列,获取索引矩阵 $\mathbf{Z}_{(1)}$ 和 $\mathbf{Z}_{(2)}$ 。

② 组建索引坐标矩阵 $\mathbf{U}_{m,1}$ 和 $\mathbf{U}_{m,2}$,通过 $\mathbf{U}_{m,1}$ 和 $\mathbf{U}_{m,2}$ 实现通信图像 P 的位置信息存储。其中横纵坐标的取值分别为由 $\mathbf{Z}_{(1)}$ 和 $\mathbf{Z}_{(2)}$ 组成,如下:

$$\begin{cases} \mathbf{U}_{m,1}(x, y) = \mathbf{U}_{m,1}(\mathbf{Z}_{(1)}(x, y), r^{(1)}), \\ \mathbf{U}_{m,2}(x, y) = \mathbf{U}_{m,2}(\mathbf{Z}_{(2)}(x, y), r^{(2)}). \end{cases} \quad (8)$$

③ 对通信图像进行位置变换,获取密文在 $\mathbf{U}_{m,1}$ 对应的位置,放入通信图像 P 对应的 $\mathbf{U}_{m,2}$ 位置,最终完成置乱处理。

2) 步骤2 扩散处理。

设定 $\mathbf{E}$ 表示混沌矩阵,具体的扩散过程 H_i 如下:

$$H_i = \begin{cases} (\mathbf{U}_{m,1}(x, y) + \mathbf{S} + \lfloor \mathbf{E} \times 2^{32} \rfloor) \bmod G, \\ (\mathbf{U}_{m,2}(x, y) + H_i + \lfloor \mathbf{E} \times 2^{32} \rfloor) \bmod G. \end{cases} \quad (8)$$

。。在置乱结果间进行逐位“异或”操作,将固定位置的数据变换为全新的数据,作为输入再次进行扩散处理。

3) 步骤3 加密处理。

① 为实现通信图像的加密处理,首先将图像的3个分量精确分离,随后分别对它们实施 90° 、 180° 和 270° 的旋转操作,再应用Arnold变换以增强其安全性。最后,将上述图像在水平方向拼接,从而得到通信图像 P_1 。同时,为确保Arnold变换不再遵循单一的规则,通过对混沌序列控制参数 d 和 f 取值,对未变换的数据进行随机变换,有效增强攻击者的破译难度。

② 利用密钥形成所需要的参数 x_0 、 y_0 和 $r^{(1)}$,通过双混沌系统形成随机序列,将混沌序列 $I(i)$ 通过式(9)所示的规则进行转换,获取二进制序列 $B(i)$:

$$B(i) = \begin{cases} 0, & I(i) < 0.5, \\ 1, & I(i) \geq 0.5. \end{cases} \quad (9)$$

③ 对通信图像进行位置交换处理,经过两轮连续操作后可获取通信图像 P_2 。

④ 将 P_2 中的数据进行循环位移处理,获取通信图像 P_3 。

⑤ 对 P_3 进行扩散处理,连续两轮操作后即可获取通信图像 P_4 。

⑥ 通过步骤2)形成的二进制序列 $B(i)$ 对当前情况进行判定,当 $B(i) = 0$ 时不实施任何操作;当 $B(i) = 1$,对 P_4 中当前像素值和右像素值实施异或操作,最终获取加密结果。

2 实验分析

为验证所提大规模移动通信双混沌数据安全加密算法的有效性,进行了实验验证。实验参数设置如表1所示。

表1 实验参数
Tab. 1 Experimental parameters

参数类别	参数名称	具体数值/描述
双混沌系统参数	Logistic 映射初始值	$x_0=0.3$
	Logistic 映射控制参数	$r=3.99$
	Chen 系统初始值	$x_0=0.1, y_0=0.2, z_0=0.3$
	Chen 系统控制参数	$a=35, b=3, c=28$
图像数据参数	图像大小	512×512 像素
	图像格式	彩色 JPG
	填充曲线	Hilbert 曲线
		填充曲线迭代次数: 10
加密步骤参数	全局置乱	置乱后图像分块大小: 64×64
	相邻像素比特级置乱	约瑟夫遍历步长: 17; 比特级置乱轮数: 3; 双向密文反馈轮数: 5
	初始加密	密钥长度: 128 位
		Arnold 变换迭代次数: 4
双混沌与 Arnold 变换结合		混沌矩阵生成轮数: 4
		混沌矩阵大小: 64×64

在实验过程中选取 20 张原始通信图像,部分通信图像如图 2 所示。

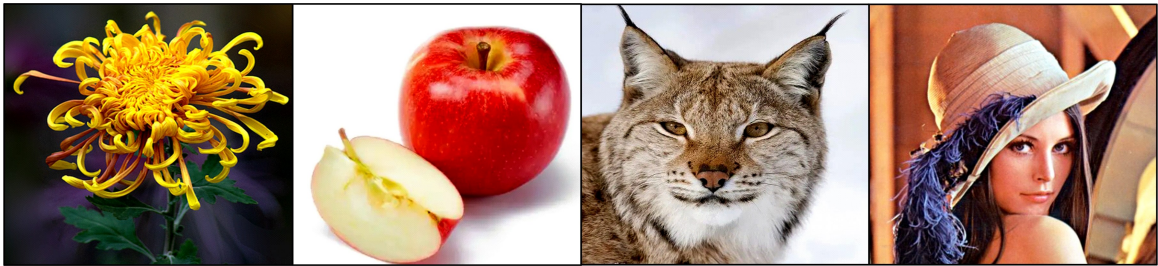


图2 测试样本图像
Fig.2 Test sample image

实验分别采用 3 种加密算法对图 2 所示的测试样本进行加密处理,得到的实验结果如图 3 所示。
通过分析图 3 可知,利用所提算法生成的加密图像,在人眼的视觉感知下与原始图像相比,结果几乎无法辨识出任何相似性联系,展现出了算法出色的隐蔽性和加密效果。而经过另外 2 种算法的加密处理后图像和原始图像差异比较小,无法确保图像的安全性,不能对图像起到保护作用。表明所提算法可以获取满意的加密效果。

实验通常采用像素变化率(NPCR: Number of Pixels Change Rate)和归一化像素值平均改变强度(UACI: Unified Average Changing Intensity)两项指标对明文敏感性进行分析。NPCR 指标若呈现较高的数值,表示加密算法对图像的扰乱程度更为剧烈,从而确保更为卓越的加密效果;而 UACI 值若更高,则凸显出加密算法对像素值的影响更为显著,进而印证其出色的加密效能。这两项指标的高值都表示了加密算法在保护信息安全方面的强大能力。图 4 和图 5 分别给出 3 种算法的 NPCR 值和 UACI 值测试结果。

通过分析图 4 和图 5 可知,在 3 种加密算法中,所提算法的 NPCR 和 UACI 取值均高于另外两种加密算法,主要是因为所提算法实施了 2 次加密,能显著提升通信数据的安全防护能力,有效应对多种攻击手段的威胁,展现出卓越的明文敏感性,从而为用户提供了更加可靠的通信保障。

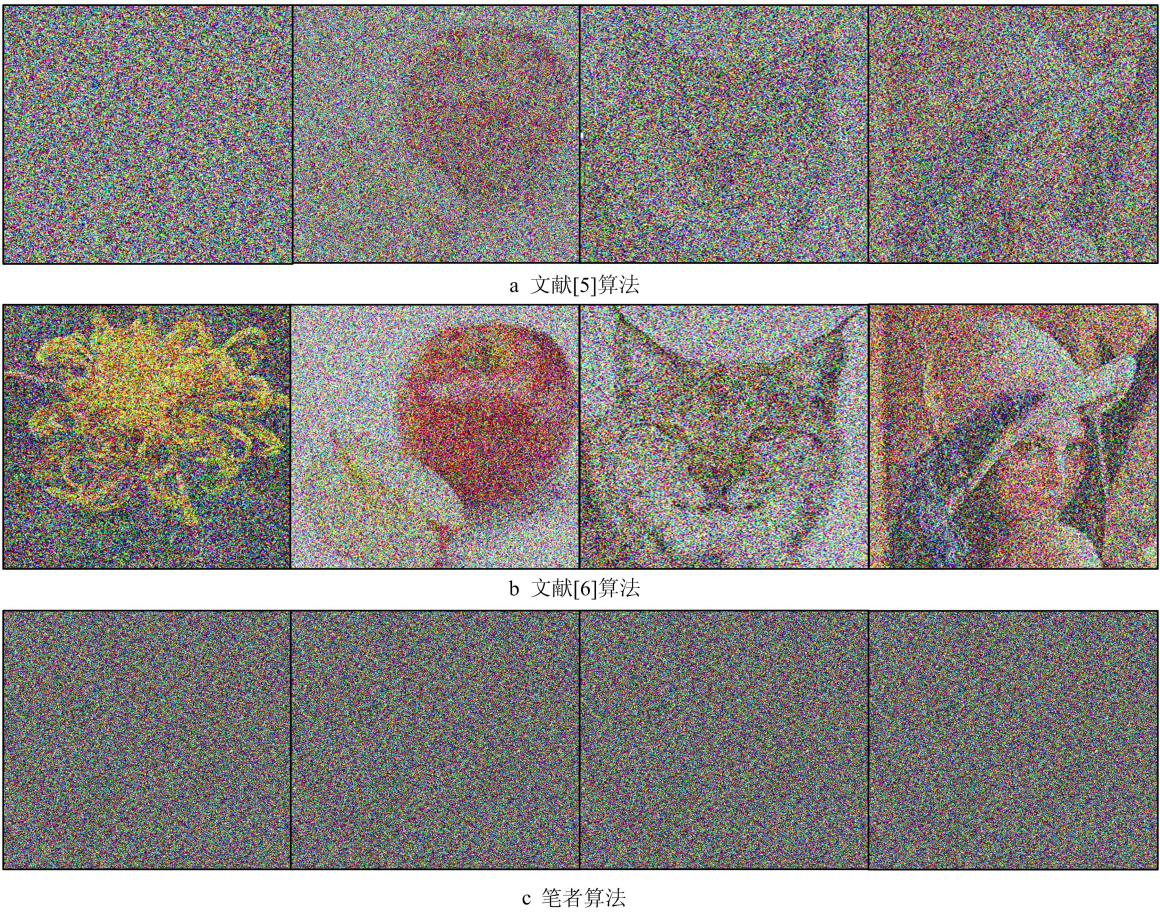


图 3 不同算法的加密效果比较

Fig. 3 Comparison of encryption effects of different algorithms

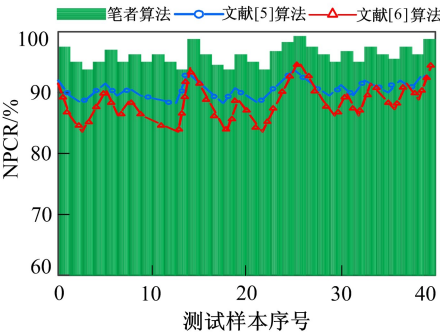


图 4 不同加密算法的 NPCR 实验结果比较

Fig. 4 Comparison of NPCR experimental results of different encryption algorithms

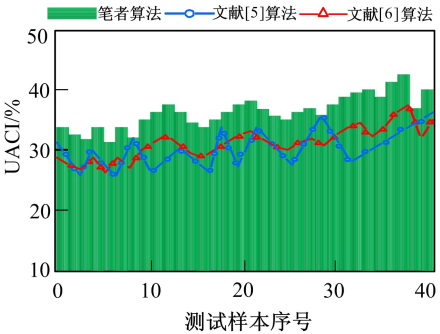


图 5 不同加密算法的 UACI 实验结果比较

Fig. 5 Comparison of UACI experimental results with different encryption algorithms

3 结 语

随着互联网技术的迅猛发展,大规模移动通信的安全性日益显著,已成为业界关注的焦点。笔者提出一种大规模移动通信双混沌数据安全加密算法,并与已有的加密算法进行了对比,结果表明所提算法在安全性以及抗攻击方面表现十分出色,能为用户带来更加安全便捷的通信体验。未来阶段,将持续关注数据安全领域的发展动态,进行更加深入研究,为建立安全且稳定的通信环境提供技术支撑。

参考文献:

- [1] 郑伟, 席思星, 王桂林, 等. 结合计算全息和频移的 JTC 系统多图像光学加密方法 [J]. 红外与激光工程, 2022, 51(5): 440-446.
ZHENG W, XI S X, WANG G L, et al. Multi-Image Optical Encryption Method of JTC System Combining CGH and Frequency Shift [J]. Infrared and Laser Engineering, 2022, 51(5): 440-446.
- [2] 李锦青, 刘泽飞, 满振龙. 基于生成对抗网络的密钥生成方法及其在微光图像加密中的应用 [J]. 兵工学报, 2022, 43(2): 337-344.
LI J Q, LIU Z F, MAN Z L. Key Generation Method Based on Generative Adversarial Network and Its Application in Low-Light-Level Image Encryption [J]. Acta Armamentarii, 2022, 43(2): 337-344.
- [3] 郭媛, 姜津霖, 陈炜, 等. 深度学习压缩重构的通用图像快速加密算法 [J]. 计算机辅助设计与图形学学报, 2022, 34(6): 913-922.
GUO Y, JIANG J L, CHEN W, et al. General Image Fast Encryption Algorithm for Deep Learning Compression and Reconstruction [J]. Journal of Computer-Aided Design & Computer Graphics, 2022, 34(6): 913-922.
- [4] 徐冬冬, 于欣, 杜丽敏, 等. 基于混沌与快速小波变换的多光谱图像压缩加密算法 [J]. 光谱学与光谱分析, 2022, 42(9): 2976-2982.
XU D D, YU X, DU L M, et al. Multispectral Image Compression and Encryption Algorithm Based on Chaos and Fast Wavelet Transform [J]. Spectroscopy and Spectral Analysis, 2022, 42(9): 2976-2982.
- [5] 郑思飞, 冯子婧, 刘成语, 等. 云存储环境中基于矢量量化的图像伪装加密方法 [J]. 计算机工程与科学, 2022, 44(6): 1030-1036.
ZHENG S F, FENG Z J, LIU C Y, et al. An Image Camouflage Encryption Method Based Onvector Quantization in Cloud Storage Environment [J]. Computer Engineering & Science, 2022, 44(6): 1030-1036.
- [6] 石金晶, 陈添, 陈淑慧, 等. 基于 Arnold 变换的量子图像混沌加密方法 [J]. 电子与信息学报, 2022, 44(12): 4284-4293.
SHI J J, CHEN T, CHEN S H, et al. Quantum Image Chaotic Cryptography Scheme Based on Arnold Transforms [J]. Journal of Electronics & Information Technology, 2022, 44(12): 4284-4293.
- [7] 曾萍, 王冰清, 赵耿, 等. 基于改进 MC 算法和分数阶混沌的 CT 图像三维重建和加密方案 [J]. 计算机应用研究, 2023, 40(1): 263-267.
ZENG P, WANG B Q, ZHAO G, et al. 3D Reconstruction and Encryption Scheme of CT Images Based on Improved MC Algorithm and Fractional-Order Chaos [J]. Application Research of Computers, 2023, 40(1): 263-267.
- [8] WANG X, CHEN X. Image Encryption Algorithm Based on Cross-Scrambling and Rapid-Mode Diffusion [J]. The Visual Computer, 2023, 39(10): 5041-5068.
- [9] 任花, 牛少彰, 任如勇, 等. 基于二维压缩感知的有意义图像加密算法研究 [J]. 通信学报, 2022, 43(5): 45-57.
REN H, NIU S Z, REN R Y, et al. Research on Meaningful Image Encryption Algorithm Based on 2-Dimensional Compressive Sensing [J]. Journal on Communications, 2022, 43(5): 45-57.
- [10] 杨璐, 郭文锋. 基于可逆矩阵的多级混沌图像加密算法设计 [J]. 计算机仿真, 2023, 40(7): 239-243, 513.
YANG L, GUO W F. Design of Multi-Level Chaotic Image Encryption Algorithm Based on Reversible Matrix [J]. Computer Simulation, 2023, 40(7): 239-243, 513.

(责任编辑: 刘东亮)