文章编号:1671-4598(2023)06-0280-07 DOI:10.16526/j.cnki.11—4762/tp.2023.06.042 中图分类号:TP309.7 文献标识码:A

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

田如意，顾风军，彭 坤，国 栩
（中国人民解放军总医院 医疗保障中心信息科，北京 100000）

摘要：针对现有网络信息传输过程中加、解密时间长，使得其传输负载超出最佳范围的问题，提出一种基于一维 Logistic 映射和二维 Tent 映射双混沌思路的网络信息加密方法；先采用时间序列分析的方式完成网络稳定性分析，得知每个网络信息特征序列都会随着时间的变化而变化，可依据网络传输时间序列图识别网络的稳定性；然后根据其时间序列的稳定性分析结果，计算网络传输的时间序列偏离度，结合偏离度参数利用双混沌互反馈安全加密方法实现网络数据加密；实验结果表明：与对比方法相比，所提方法加解密时间较短，小于 5 s，且传输负载均在最佳负载范围内，即小于 600 kWh，充分验证了该方法可靠性强、安全性高，具有一定应用价值。

关键词：时间序列；异常数据；双混沌系统加密算法；网络传输；安全加密

Network Information Encryption Based on One-Dimensional Logistic Mapping and Two-Dimensional Tent Mapping

TIAN Ruyi, GU Fengjun, PENG Kun, GUO Xu
(Information Department of Medical Security Center, PLA General Hospital, Beijing 100000, China)

Abstract: Aiming at the problem that the encryption and decryption time in the existing network information transmission process is too long to make its transmission load exceed the optimal range, a network information encryption method based on the dual-chaos idea of one-dimensional Logistic map and two-dimensional Tent map is proposed. Firstly, the network stability analysis is completed by the time series analysis. It is obtained that each network information characteristic sequence will change with time, the network stability can be identified according to the network transmission time series diagram; Then, according to the stability analysis results of the time series, the deviation degree of the time series transmitted by the network is calculated. Finally, combined with the deviation degree parameter, the double chaos mutual feedback security encryption method is used to realize the network data encryption. The experimental results show that compared with the comparison method, the encryption and decryption time of the proposed method is shorter, less than 5 s, and the transmission load is within the optimal load range, that is, less than 600 kWh, which fully verifies that the method has strong reliability and high security, and it has certain application value.

Keywords: time series; abnormal data; double chaotic system; encryption algorithm; network transmission; secure encryption

0 引言

随着企业数据化、信息化的发展，其管理系统中往往需要传输大量数据，因管理不善而出现数据冗余、数据丢失等现象屡见不鲜，制约着企业信息化的发展，企业面临信息传输安全性较差的问题[1-2]。为避免该类问题出现，相关学者对网络信息安全加密方法进行了系统研究。我国学者自本世纪初期就开展相关研究，多年来收效显著。如肖成龙[3]等人提出利用神经网络对网络数据实行第一次加密，再利用混沌系统生成的混沌序列对网络数据实行第二次加密，以此增强了网络通信系统的安全性，有效预防外界攻击。李西明[4]等人优先对网络通信模型实施了抗泄露加密测试，根据测试结果改进了设立的神经网络模型，利用建立的模型更改了网络通信系统中的激活函数，从中取得加密算法模型，通过该模型对网络通信系统加密，以此提高网络通信传输的稳定性及保密性，最终实现加密算法的研究。江健豪[5]等人将加密算法与属性基加密相结合，以此预防外界攻击，提升网络访问的安全性。为避免网络中的密钥出现分发现象，对密钥的结构进行了更改，根据更改密钥结构实现网络数据加密方法，有效防止了系统发生用户撤销、共谋攻击的问题。但是，上述方法在应用过程中仍然难以解决其加解密所用时间较长的问题，且其网络传输信息的安全性也较难把握，故无法大范围应用。针对这

收稿日期:2022-12-23； **修回日期**:2023-02-10。

作者简介:田如意(1982-),男,河北辛集人,硕士,工程师,主要从事医疗信息化、医疗大数据方向的研究。
通讯作者:顾风军(1976-),男,吉林白山人,硕士,工程师,主要从事信息化管理,数据库管理等方向的研究。

引用格式: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.

一问题，部分学者提出将混沌理念融入其中，以此来提升其网络信息传输的高效性和安全性。基于这一理念，部分学者研究出了混沌加密算法及混沌加密系统。目前基于混沌理论所研究的加密系统主要采用一种序列密码体制，即它的加密和解密都是一个互相独立的混沌体系，两者之间没有任何耦合关系。加密端对明文信息进行了加密，然后将其发送到解密端中，解密端可在所有接收到的情况下进行解密，或者使用其他技术进行同步处理后再进行解密。其中，何翠萍[6]所设计方法主要利用混沌序列进行网络信息的加密，来解决了目前网络信息加密中的密码问题。该方法首先给出了相应的混沌序列的特征值，并将其与李雅普诺夫指数相对应，得到了相应的混沌属性，并构造了混沌序列的前馈流，对其进行了初始加密，并对其密码密钥进行随机置乱处理，从而实现了对网络信息的加密。刘银[7]针对现有网络信息安全加密系统安全性不佳的问题，提出了一种双混沌的网络信息安全加密系统，该系统采用 DSP 芯片与 C54x 存储器完成硬件设计，在软件设计过程中，基于网络信息采集模块采集信息，基于双混沌算法完成信息处理，最后设计了一种安全加密数据库，以缩短网络信息查找时间，提升加密效果。龙瑞[8]以超混沌双向认证为基础，提出并设计了一种基于网络信息安全的保密加密方案。该方法主要利用外部密钥来定义密码的粒度，使得超混沌密码可在连续的情况下进行重新谈判，同时利用映射的外密钥获取 TLS 主密钥，从而达到对信息进行加密，通过一次一密、一字一密的方式提升信息传输的安全程度。以上三种方法虽然可在一定程度上改善现有方法存在的不足，提升其加密的安全性，但加密、解密时间过长的问题仍未得到解决，网络传输负载超出最佳范围问题发生显著。

为解决上述方法中存在的问题，提出并设计一种基于一维 Logistic 映射和二维 Tent 映射双混沌思路的网络信息加密方法。本次研究将一维 Logistic 映射和二维 Tent 映射相结合，提出双混沌系统安全加密方法。该方法先将 AR 与 MA 结合建立 ARIMA 预测模型，判断网络中是否存在异常数据，然后计算网络传输的时间序列偏离度，判断其网络传输过程是否存在异常波动。检测完毕后，利用双混沌互反馈安全加密方法实现网络数据加密，最后利用实验证明所提方法的先进性。希望通过所提方法，可为后续网络数据加密传输提供文献参考。

1　网络传输波动性判断

1.1　ARMA 预测模型优化设计

网络数据在传输过程中，若想完成传输数据的加密，就要先对网络中存在异常数据进行检测。本次采用时间序列分析法完成对网络传输数据中异常数据的检测[9]。目前，通常会采用各种模型来达到在预测网络中传输数据的目的，通常会采用各种模型，如自回归移动平均模型（ARMA，auto-regressive and moving average model）等，其是通过自回归模型（AR 模型）与移动平均模型（MA 模型）相结合而成，可提升预测效果。为能更加有效地检测出所用网络中是否存有异常点，需要利用 ARMA 模型检测网络[10]，对网络传输波动进行预测，以实现网络异常数据的检测。在检测网络之前，先要获取网络数据传输特征，从中得知：在各个特征集中，每个特征序列都会随着时间的变化而变化。这样就可依据网络传输时间序列图识别网络的稳定性。如果网络中存有不平稳的时间序列，就对其开展差分处理，然后再建立一个 ARMA 预测模型，确定该模型参数后，利用该模型对网络实行预测。

在 ARMA 模型预测过程中，需要将预测指标按照时间顺序记录，使指标数据形成一个数据列。如此就可利用这一组数据列所具有的依存关系表现原始数据在时间上的连续性。ARMA 模型是由 AR 模型和 MA 模型相结合而成，故可根据 X_t 与历史值 $X_{t-1},X_{t-2},\cdots,X_{t-p}$ 之间具有相关性，定义 AR 模型为：

$$X_{AR}=c+\sum_{i=1}^{p}\varphi_i+\varepsilon_t \tag{1}$$

式中，c 表示常数项；φ 表示参数项；ε_t 表示白噪声扰动项；p 表示阶数；i 表示时刻值[11]。

若 AR 模型中的当前值与历史值之间的 ε_t 具有相关性，则利用时间序列构建 MA 模型，其具体表达式为：

$$X_{MR}=c+\sum_{i=1}^{q}\theta_i+\varepsilon_{t-i} \tag{2}$$

式中，X_t 表示随机变量；θ_i 表示参数项；q 表示阶数，ε_{t-i} 表示白噪声扰动项[12]。在式（1）、式（2）的基础上，可完成 ARMA 基础模型的建立，表达式如下所示：

$$X=c+\varepsilon_t+\sum_{i=1}^{p}\varphi_i+X_{i-1}+\sum_{i=1}^{q}\theta_i+\varepsilon_{t-i} \tag{3}$$

ARMA 基础模型在预测过程中，会受到外界影响因素和自身变动规律的影响，需对基础模型进行回归分许，设影响因素为 $x_1,x_2,\cdots,x_k$，则回归分析表达式为：

$$X_1=\beta_0+\beta_1x_1+\beta_2x_2+\cdots+\beta_kx_k+\varepsilon_t \tag{4}$$

式中，X_1 代表预测对象的观测值。预测对象 Y 受自身变化影响，自身变动规律可由下式进行表示：

$$X_2=\beta_0+\beta_1x_{t-1}+\beta_2x_{t-2}+\cdots+\beta_px_{t-p}+\varepsilon_t \tag{5}$$

当白噪声扰动误差 ε_t 在不同时期存在一定的依存关系时，扰动误差为：

$$\varepsilon_t=\alpha_0+\alpha_1\varepsilon_{t-1}+\alpha_2\varepsilon_{t-}2+\cdots\alpha_q\varepsilon_{q-2} \tag{6}$$

综合上式，即可完成 ARMA 模型的优化设计，其可用下式表示：

$$X'=\beta_p\alpha_q\left(c+\varepsilon_t+\sum_{i=1}^{p}\varphi_i+X_{t-1}+\sum_{i=1}^{q}\theta_i+\varepsilon_{t-i}\right) \tag{7}$$

以上优化的 ARMA 预测模型证明了在 t 时刻时，当前值与历史值之间具有一定相关性，同时还具有随机扰动的关系。若网络中存有异常数据波动，那么网络的真实值就会偏离获取的预测值。故要想完成网络异常数据的检测，需要再对其扰动造成的网络传输波动偏离度进行分析。

1.2 网络传输波动偏离度分析

当网络在数据传输过程中发出异常波动时，就会改变 ARMA 模型的传输特征，因此需要对 ARMA 模型的传输时间序列偏离度实行检测分析，检验网络中是否存有异常波动。

在网络内，残差[13]是网络的传输偏差，可将其看作偏离度，根据目前网络传输与正常网络传输数据的偏离度分析网络传输特征的残差序列，以此来衡量目前的网络传输残差值，并对其进行定期更新。由于本次研究中的网络传输残差序列所呈现的特征不符合平稳时间序列的特征，故本次研究先对其序列进行平稳化处理，即对原序列进行一次或几次差分，使其转变成平稳序列后开展建模分析。在对序列进行平稳性处理之后，利用 ARMA 模型对其进行模拟，使之符合其波动，从而实现对该序列波动的预测，整个过程如下：

首先，先求解样本的自相关系数（ACF）和采样偏移自相关系数（PACF）。

其次，通过对样本自相关和偏自相关特性的研究，选取合适的序列来拟合 ARMA 模型，并对模型中的未知参数进行估算。

再次，对模型的正确性进行验证，当拟合模型未被验证时，必须重新选取模型，才能进行拟合。在经过验证的情况下，对模型进行进一步优化，并以此为基础，综合考虑多种可能性，从已验证的模型中选取最佳的模型[14]。

最后，采用最佳拟合方法对未来时间序列进行预测。ARMA 模型预测流程如图 1 所示。

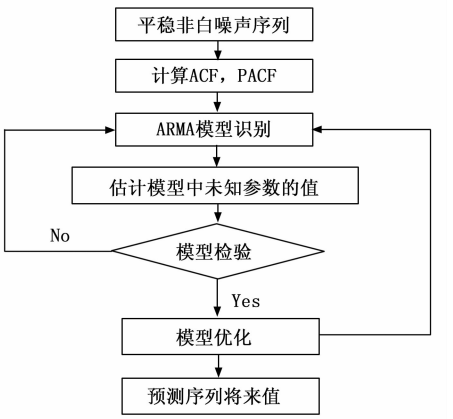

图 1 ARMA 模型预测流程图

完成其拟合后，设置网络传输残差序列为 $e_1,e_2,\cdots,e_t,t=1,2,\cdots,N$，计算实际网络传输时间序列异常偏离度，计算式为：

$$\delta_t=\exp\frac{|e_t-\bar{e}_{t-1}|}{\sigma_{t-1}} \tag{8}$$

式中，δ_t 表示在 t 时刻的偏离度；e 表示残差；$\bar{e}_{t-1}$ 表示在 $t-1$ 时刻的残差均值；σ_{t-1} 表示标准差。

对比预测值和实际值，其偏差逐渐加大时，就说明网络传输的真实值及预测值偏差相差大，这时网络当前传输数据就要偏离历史数据，因而发现网络中存在异常数据。

基于时间序列分析出网络中存在异常值时，为降低残差值带来的影响，需要对异常值处理，因而对时间序列偏离度实行更新。那么网络传输异常波动的检测流程如下所示：

1）获取网络传输中的传输数据特征，即 x，对 ARMA 模型的参数确立完成后，通过模型预测 t 时段内的网络数据特征的预测值，即 y_t。

2）通过式（4）计算网络 t 时段的真实值 x_t 和预测值 y_t 之间的时间序列偏离度 δ_t。若计算结果出现异常，就需要对历史残差序列调整，并及时更新[15]。

3）设置网络特征为（$f_1,f_2,f_3,\cdots,f_n$），重复步骤 1）与步骤 2），直至取得网络特征在某一时段内的偏离度，组建成偏离度向量，将其表示如下：$D_{1t},D_{2t},\cdots,D_{mt}$。

4）利用分类器[16]对 $D_{1t},D_{2t},\cdots,D_{mt}$ 分类判断，根据各个数据特征的偏离情况，验证网络传输中是否存有异常波动。

2 网络传输安全加密方法设计

2.1 混沌加密算法设计

根据上述流程得知网络中是否存在异常数据，依据检测结果对网络数据实行加密，确保网络传输安全性。网络数据在传输期间，需要对加密的时效及解密的正确效果考虑，所以在加密、解密的时候需要确保密钥可保持不变，不然就会导致解密失败。依据网络传输性能，本次研究将混沌理论引用其中，利用双混沌互反馈加密方法加密网络传输数据。

混沌理论与密码学有着本质的关联，其结构具有一定的相似性，例如混沌的类随机性、对系统参数的敏感度，以及混沌的轨道混合性质与常规加密体系的扩散特征类似，这些都为在密码学中进一步深入应用混沌理论奠定了基础。本文所讨论的双混沌体系，即逻辑混沌映射与 Tent 混沌映射。其中，Logistic 混沌映射系统是一种很有代表性的一维混沌系统，它具有复杂的混沌动力学性质，是一种常用的密码算法[17]，其可用方程表达式定义如下：

$$x_{i+1}=\mu x_i(1-x),i=1,2,\cdots \tag{9}$$

式中，x_{i+1} 表示第 $i+1$ 次的迭代结果；μ 表示混沌系统中的偏离度参数，且 $\mu\in[3.57,4]$；x 表示系统变量，且 $x\in[0,1]$；i 表示次数。利用 Logistic 映射加密网络传输数据时，要先设定其参数，具体设定流程如下所示：

1）当 x 满足 $0<x\leqslant 1$ 这一条件时，Logistic 映射中的偏离度也就会变得简易，这时 $x_1=0$，且在系统内没有其余周期点。

2）当 μ 满足 $0<\mu\leqslant 3.256\ 412\cdots$ 时，系统内只有两个周期点。而满足 $4\leqslant\mu\leqslant 5$ 条件时，系统中所有周期都会向混沌系统内涌进。

3）$\mu>5$ 时，就说明混沌系统中的动力学复杂[18]。

如单纯采用 Logistic 混沌映射，其混沌范围受到 μ 影

响，参数的部分取值不能使系统产生混沌行为，而且在 $\mu>3.25$ 时，李雅普诺夫指数为负数。当系统参数值不在［0，1］时，生成的混沌序列不均匀，无法法用于信息加密。

Tent 混沌系统又称为帐篷映射，是一种分段线性的一维映射，具有良好的自相关性，可将 Tent 映射方程定义如下：

$$y_{n+1}=\begin{cases}\lambda y_n, & 0<y_n\leqslant 0.3\\ \lambda(1-y_n), & 0.3<y_n<1\end{cases} \tag{10}$$

式中，y_{n+1} 表示第 $n+1$ 次迭代结果；y_n 表示迭代次数，且 $y\in[0,1]$；λ 表示控制参数。当 λ 在［2.4］范围内时系统会处于混沌状态。如单纯采用 Tent 混沌映射，其会因为控制参数较差，导致混沌区间有限的问题。因此，本文将一维 Logistic 混沌映射与 Tent 混沌映射相结合，构成 Logistic-Tent 的双重混沌体系。它综合了 Logistic 混沌系统的复杂动态性质，以及 Tent 混沌系统的快速迭代速度、自相关性和适用性强等优点，将其与密码算法相结合，实现了双混沌互反馈网络的信息加密，实现双混沌互反馈网络信息加密，表达式为：

$$Y_{n+1}=\begin{cases}r_{xi}(1-x_n)+(4-r)y_n, & 0<y_n\leqslant 0.3\\ r_{xi}(1-x_n)+(4-r)(1-y_n), & 0.3<y_n<1\end{cases} \tag{11}$$

依据上式，在 Logistic 映射与 Tent 映射中生成混沌波动序列，完成网络信息加密。双混沌互反馈网络信息加密流程如下：

1）通过 Logistic 映射优先生成混沌序列；

2）以生成的混沌序列结果为初始值输送到 Tent 映射内进行映射；

3）判断其加密序列是否生成，生成则利用偏离度参数加密网络传输明文密码；反之，将 Tent 映射结果输入回步骤 1）Logistic 中，直至生成明文密码；

4）完成网络信息安全明文密码的生成。

2.2　加密流程

基于上述分析的双混沌系统，采用双混沌系统加密算法，即 EDC 算法，对网络传输安全加密[19]。具体的加密流程如下所示：

1）首先要对网络传输的密钥实行初始化。将 Logistic 映射与 Tent 映射之间的初始值确立，即 x_0、x'_0、y_0，及其三个偏离度参数 μ、a、b，把这些参数全部用作初始密钥。

2）对上述制定的密钥实行初始化迭代，且迭代次数为 14 次，以此提升网络传输安全性。

3）根据迭代后的结果，利用 Logistic 对其映射，具体的迭代流程如图 2 所示。

4）将步骤 3）中的迭代结果看作 P，利用 P 获取不同位数的取余运算，用方程定义如下：

$$P'=P_i \bmod 256, i=2,4,6 \tag{12}$$

式中，P' 表示混沌密钥，mod 表示位数，i 表示系数。

5）根据获取的网络传输明文字节 M 与密钥字节 P'，分

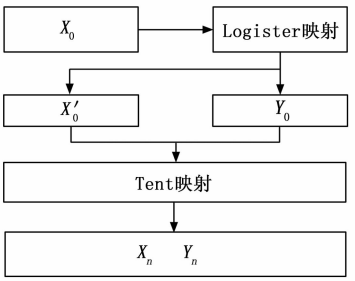

图 2　迭代过程

别对 M、P' 开展异或运算，以此取得网络传输密文字节，用方程表达式定义为：$S=M\otimes P'$，其中，S 表示密文[20]字节。

6）对全部明文字节 S 实行检验，验证 S 是否全部加密。若是，则结束加密；若不是，则转至步骤 3），反复开展下一轮加密，直至加密成功为止。

通过对网络传输实行时间序列分析后，检测信息网络中存有异常数据，对其处理后再对信息数据实行加密，从而实现网络信息双混沌系统安全加密方法研究。

3　实验与分析

为验证网络信息双混沌系统安全加密方法的整体有效性，需要对该方法开展实验测试。本文研究对象选取某三甲医院的医疗网络信息管理系统。

3.1　实验设置

采用 Windows 10 作为实验的操作系统，启动开发工具 SDSoc2018，新建 SDSoc projrct 工程，在信息管理系统中随机抽取医疗数据作为数据样本，组成数据集，然后，完成网络波动环境的建立，在 STARMA 模型复杂网络波形数据库中选取了 Probe 模式下 ipsweep 和 smurf 两种波动引入其中，以使实验环境的模拟更加真实，方便对网络波动性条件下的双混沌系统进行安全性分析。在此环境下，将其杂波噪音样本数设定为 1 024 点、访问次数设定为 13 000 次、病毒攻击样本数设置为 928 点、信息交互波动次数设置为 100 次。本次研究所有的试验都是在这样的环境下完成的，并给出了相应的参数设定，如表 1 所示。

表 1　实验环境配置

名称	参数
操作系统	Windows server 2010
系统内存	IntelCore5-630 128 GB
CPU	X2500
网络信噪比	1.121
网络信噪频率	120 kHz

以此为基础，开展实验研究。

3.2　性能测试

3.2.1　ARMA 模型测试

首先验证 ARMA 模型网络波动预测的有效性，其预测

步骤如下所示：首先提取网络波动数据，为方便后续的分析，对网络中的原始数据进行了均质化处理；分别求取置信度为 95%的自相关与偏相关函数；通过自相关函数的拖尾和偏相关函数的截尾特点，对 ARMA 模型进行了初步判定，利用最少信息标准对最优模型进行识别，并对其进行进一步的预测。预测误差由式（13）表示：

$$e_t = x_t - Y_t \tag{13}$$

由此，模型平均绝对误差和均方差误差可分别如式（13）～（14）表示：

$$MAE = \frac{1}{N}\sum_{t=1}^{N} |e_t| \tag{14}$$

$$MSE = \frac{1}{N}\sum_{t=1}^{N} (e_t)^2 \tag{15}$$

依据其预测的平均绝对误差和均方差误差可对其预测精度进行全面分析。根据上述步骤完成本文建立 ARMA 模型预测准确度的判断，通过对其网络波动数据进行分析，得到了可信度为 95%的自相关和偏相关函数。以此为基础，建立了 ARMA（40、7）、ARMA 40、8、ARMA（41、7）等 9 个模型参数，分别计算出与上述 9 种模式参数相对应的最小化值，其结果如表 2 所示。

表 2 不同阶次对应的 AIC 值

MA 模型阶次 q AR 模型阶次 p	7	8	9
40	−12.507	−12.509	−12.471
41	−12.5813	−12.464	−12.536
42	−11.786	−12.007	−12.518

如表 2 所示，根据 AIC 准则选择最优模型参数，建立了模型 ARMA（41，7）。最后采用该模型完成网络波动预测，得到其预测误差曲线、平均绝对误差曲线及平均绝对误差曲线如图 3～5 所示。

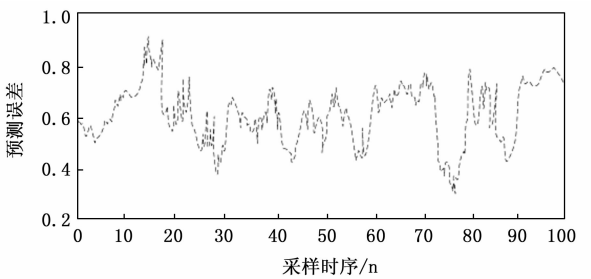

图 3 预测误差曲线

结合上述图像可以看出，此预测模型具有良好的追踪速度，当出现大的变动趋势时，可迅速地对时间序列中的突变情况做出反应，具有较好的快速追踪和自我校正能力，从而使预报结果与实际情况符合良好。该模型预测结果具有很好的准确性，其平均绝对误差为 7.71×10^{-4}、1.39×10^{-6}，并且预测误差函数和预测自相关函数所显示的错误序列满足了白噪声的需求，可证明该预测模型具有较好的应用性能。

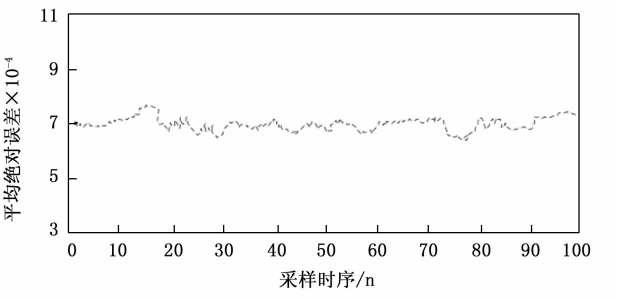

图 4 平均绝对误差曲线

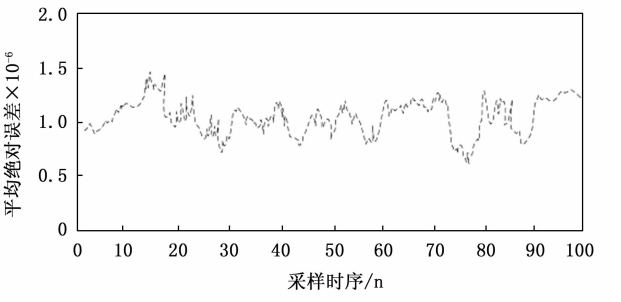

图 5 均方误差曲线

3.2.2 加密性能测试

在该算法之中，由于其加密产生的密钥流序列与明文无关，故其极易遭到明文攻击，故为检测应用所设计网络信息加密方法进行网络数据传输的安全性，开展如下实验。设两个明文块如下可表示为：

P1 为 6162，6264，6566，6768，696A，6B6C，6D6E，6F70，7172，7374，666B，6769，726D，766A，6768，6467，726C，7375，7279，7770. P2 = 646B，6E76，666A，6869，6161，6B63，6E76，6265，7566，6A66，7269，6772，686A，7664，666C，7367，6165，7967。

采用本次研究的基于一维 Logistic 映射和二维 Tent 映射双混沌思路的网络信息加密方法产生密钥流，分别加密 P1 和 P2，加密过程中的变量信息如表 3、4 所示。

表 3 明文块 P1 加密过程

Mj	Dj	Pj	Aj	Cj
6162636465666768	804A30F53B394136	E12853915E5F265E	CC8C92943A000AD8	2DA4C10B645F2C86
696A6B6C6D6E6F70	CFB0C75AA6B34114	A6DAAC26CBDD2E64	78254554121CE067	DEFFE972D9C1CE03
71727374666B6769	6281F9C28D245BD0	13F38AB6EB4F3CB9	6D27F65919DFE1FC	7ED47CEFF290DD45
726D766A67686467	CF1A3E83762FE229	BD7748E91447864E	821A7876FFAC811E	3F6D309FEBEB0750
726C737592797770	7263BDEBF7C116B3	000FCE9E85B861C3	DC4DA2F923F4B9C4	DC426C67A64CD807

表 4　明文块 P2 加密过程

Mj	Dj	Pj	Aj	Cj
646B6E76666A6869	804A30F53B394136	E4215E835D53295F	CC8C929A3A000AD8	28ADCC1967532387
61616B636E766265	0C75AA6B34114113	6D15C1085A672376	54554121CE067CFB	3940802994615F8D
75666A6672697566	553D9A7639EA21B9	205BF0104B8354DF	C1E73F89877FBF47	E1BCCF99CCFCEB98
72796772686A7664	046C88C0A1DD4726	7615EFB2C9B73142	C6281F9C28D245BD	B03DF02EE16575FF
666C736761657967	F3B551FD5CE9AF6A	95D9229A3D8CD60D	920BAEC98EE8BC62	07D28C53B3646A6F

从表 3 和表 4 可看出基于一维 Logistic 映射和二维 Tent 映射双混沌思路的网络信息加密方法对于不同的明文会产生差异很大的密文，甚至会产生不同的加密序列 Aj 和不同的移位序列 Dj。从第二组加密开始后，两个表中的密钥流就完全不同，同时序列 Dj 也不同，故本次设计方法对明文具有较好的敏感性。由于选择明文攻击需要选择至少同一个加密密钥下产生至少两组相同密钥流的密钥，从上表可以看出，本次设计的双混沌网络信息加密方法除两个表中了第一组密钥流相同之外，其它的密钥流均不同。即使两个表中的第一组密钥流和移位序列是相同的，但是攻击者仍然不能使用选择明文攻击分析出密钥流，因为选择明文攻击还必须猜测移位序列，而移位序列的空间足够大，使得攻击者无法穷举获得正确的移位序列，从而无法获得密钥流。通过上述过程，可验证本文设计方法在进行数据传输的过程中可保障信息安全，在一定程度上避免其受到网络攻击。

3.3　对比测试

选取文献［3］基于神经网络与复合离散混沌系统的双重加密方法和文献［6］基于混沌序列的网络信息加密方法作为对比方法，与所提方法一同对网络中待传输的医疗数据进行加密，对比其加解密效果。

1）网络传输数据在加密时，会根据加密的网络传输数据长度，设置不同长度的字符串，而字符串的长度会对加密、解密的效率造成影响。为了检验本方法的正确性，采用本文提出的方法、文献［3］方法和文献［6］方法分别进行加密和解密时间的测试，获得其加解密时间结果，得到其结果展示如图 6～7 所示。

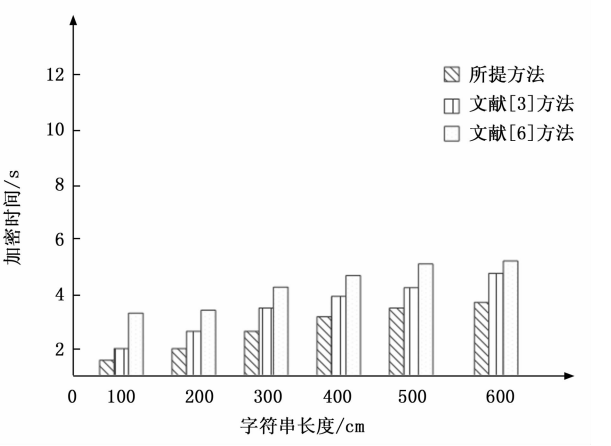

图 6　加密时间测试

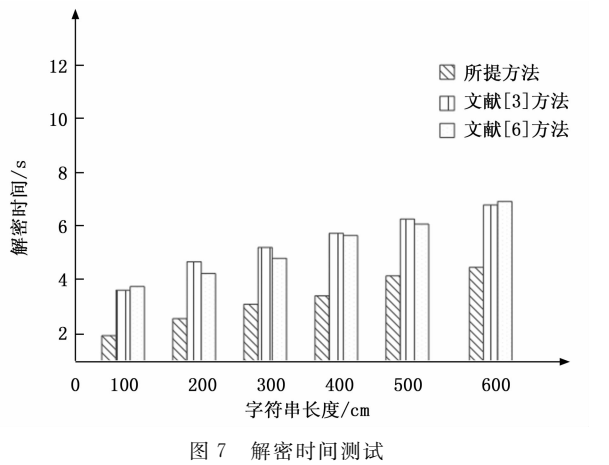

图 7　解密时间测试

分析图 6 中的数据发现，随着字符串长度的不断增加，三种方法所呈现出的加密时间均有所不同。虽然三种方法在整体测试中都有着上升趋势，但经对比发现，所提方法在不同字符串长度的情况下，加密时间均低于文献［3］方法和文献［6］方法，其在字符串长度为 600 cm 时，加密时间小于 4 s，而文献［3］方法需要 5 s，文献［6］方法需要5.7 s，由此表明所提方法加密效率要优于其余两种对比方法。

以加密时间测试为基础，利用所提方法、文献［3］方法和文献［6］方法分别对不同字符串长度的网络传输数据实行解密测试。解密时间越小，说明该方法的解密效率越好；解密时间越大，说明该方法的解密效率越差。具体测试结果如图 7 所示。

从图 7 中的数据可知，与加密时间对比，三种方法的解密时间要比加密时间的所用时间长。在相同的字符串长度下，三种方法所表现出的解密时间存有差异。在最初测试时，所提方法的解密时间就低于文献［3］方法和文献［4］方法，仅为 2 s。在后续测试过程中，所提方法的上升速度较慢，在字符串长度为 600 cm 时，应用所提方法解密时间为 4.3 s，应用文献［3］方法解密时间为 6.5 s，应用文献［6］方法解密时间为 6.1 s，由此验证了所提方法的解密时间短，说明所提方法的解密效率高。

综上所述，所提方法的加密、解密时间都要小于其余两种对比方法，这主要是因为所提方法对网络传输数据开展时间序列分析，分析了波动性因素，以此减少了加密数据量，进而降低了加解密时间。

2）网络数据在传输过程中，过多的数据会加重网络传

输负载，导致网络数据传输时安全性差，容易遭到异常攻击。所以为验证网络传输安全性能，需要利用所提方法、文献［3］方法和文献［4］方法分别对网络传输负载实行实验测试。设置网络传输数据的最佳负载在 500～600 kW·h 之间，若三种方法测试的传输负载处于最佳范围内，那么就表明该方法的传输安全性能强，反之则差。具体测试结果如图 8 所示。

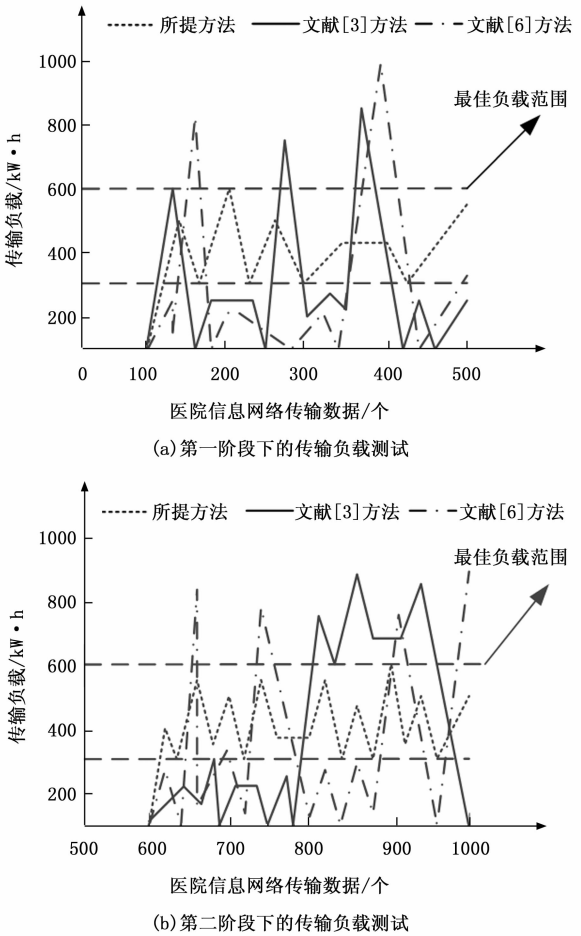

图 8 传输负载测试

通过图 8 中的数据发现，在整体测试期间，不论网络传输数据数量为多少，所提方法的传输负载始终处于设定的最佳范围内，而其余两种对比方法时而低于最佳负载范围，时而高于最佳负载范围。由此可断定所提方法的传输负载最佳，网络传输安全性能最强。

4 结束语

由于现如今的信息量庞大，网络数据在传输过程中经常会遭受到外界攻击。本次研究针对网络传输安全加密方法存在的问题，提出网络信息双混沌系统安全加密方法研究。首先对网络传输数据开展时间序列分析，以此检验网络中是否存有异常数据，再对网络传输数据实行加密，从而实现网络信息双混沌系统安全加密方法研究。所提方法可对网络波动进行良好预测，并加强了其加密性能，经过实验表明，其在字符串为 600 时，加密时间仅为 4 s，解密时间仅为 4.3 s，且传输时其负载始终处于设定的最佳范围，均优于对比方法，验证了该方法有着较强的安全性、可靠性，具有较大的应用价值。

参考文献：

[1] 毛 盼，白文辉，张俊梅，等. 信息化技术在新型冠状病毒肺炎防控救治工作中的应用［J］. 中华护理杂志，2020，55（S1）：284－285.

[2] 吴振君. 基于 Hadoop 的医院智慧医疗信息管理系统设计［J］. 信息技术，2019，43（12）：62－66.

[3] 肖成龙，孙 颖，林邦姜，等. 基于神经网络与复合离散混沌系统的双重加密方法［J］. 电子与信息学报，2020，42（3）：687－694.

[4] 李西明，吴嘉润，吴少乾，等. 基于生成对抗网络的抗泄露加密算法研究［J］. 计算机工程与应用，2020，56（10）：69－74.

[5] 江健豪，蒋 睿，裴 蓓，等. 基于 NTRU 格的云数据可撤销属性基加密方案［J］. 东南大学学报（自然科学版），2020，50（6）：1052－1061.

[6] 何翠萍. 基于混沌序列的网络信息加密方法［J］. 电脑知识与技术，2021，17（23）：36－37.

[7] 刘 银. 基于双混沌算法的网络信息安全加密系统设计［J］. 信息记录材料，2022，23（4）：118－120.

[8] 龙 瑞. 基于超混沌双向认证的网络信息安全加密方法［J］. 信息与电脑（理论版），2021，33（9）：213－215.

[9] 司存友，李 珂，周金玉. 基于相似性搜索的水文时间序列预测模型研究［J］. 信息技术，2020，44（3）：19－24，31.

[10] 崔 华，冯思哲，王兰玲，等. 基于残差网络的线上考试防替考系统设计［J］. 信息技术，2019，43（12）：53－56，61.

[11] 于思皓，郭嘉丰，范意兴，等. 基于知识线记忆的多分类器集成算法［J］. 计算机学报，2021，44（3）：462－475.

[12] 奚晨婧，高媛媛，沙 楠. 信道估计误差对物理层安全加密方案的影响［J］. 计算机工程，2020，46（6）：122－129.

[13] 李 玮，汪梦林，谷大武，等. 轻量级密码算法 TWINE 的唯密文故障分析［J］. 通信学报，2021，42（3）：135－149.

[14] 杨 亮. 基于区块链技术的机器人数据加密传输控制系统设计［J］. 计算机测量与控制，2021，29（6）：119－122，163.

[15] 丁 璇. 基于区块链的智能机器人多传感信息加密控制研究［J］. 计算机测量与控制，2021，29（3）：252－257.

[16] 马 天，赵会敏，杨 嫣，等. 神经网络域水印信息优化与加密［J］. 西安科技大学学报，2022，42（3）：580－588.

[17] 李 玎，林 伟，芦 斌，等. 面向中文搜索的网络加密流量侧信道分析方法［J］. 电子与信息学报，2022，44（5）：1763－1772.

[18] 赵键锦，李 祺，刘胜利，等. 面向 6G 流量监控：基于图神经网络的加密恶意流量检测方法［J］. 中国科学：信息科学，2022，52（2）：270－286.

[19] 马艳娥，李瑞金. 基于 DFT-S-OFDM 的网络信息安全加密传输仿真［J］. 计算机仿真，2022，39（1）：358－361，393.

[20] 乔俊峰. 假设检验技术下舰船通信网络信息安全加密建模研究［J］. 舰船科学技术，2021，43（10）：121－123.