物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

基于深度学习的新混沌信号及其在图像加密中的应用

赵智鹏　周双　王兴元

A new chaotic signal based on deep learning and its application in image encryption

Zhao Zhi-Peng　Zhou Shuang　Wang Xing-Yuan

引用信息 Citation: Acta Physica Sinica, 70, 230502 (2021)　DOI: 10.7498/aps.70.20210561
在线阅读 View online: https://doi.org/10.7498/aps.70.20210561
当期内容 View table of contents: http://wulixb.iphy.ac.cn

基于深度学习的新混沌信号及其在图像加密中的应用*

赵智鹏[1)] 周双[1)†] 王兴元[2)‡]

1) (重庆师范大学数学科学学院, 重庆 401331)

2) (大连海事大学信息科学技术学院, 大连 116026)

(2021 年 3 月 25 日收到; 2021 年 7 月 8 日收到修改稿)

为提高单一混沌系统图像加密的安全性, 本文提出了基于深度学习的图像加密算法. 首先, 利用超混沌 Lorenz 系统产生混沌序列. 其次, 利用长短期记忆人工神经网络 (long-short term memory, LSTM) 复杂的网络结构模拟混沌特征构造新的混沌信号. 然后, 利用最大 Lyapunov 指数, 0-1 测试, 功率谱分析、相图以及 NIST 测试对新信号的动力学特征进行分析. 最后, 将新信号应用到图像加密中. 由于该方法生成的新信号不同于原有混沌信号, 而且加密系统具有很高的复杂结构和非线性特征, 故很难被攻击者攻击. 仿真实验结果表明, 本文提出的图像加密算法相比其他一些传统方法具有更高的安全性, 能够抵抗常见的攻击方式.

关键词: 混沌系统, 图像加密, 深度学习

PACS: 05.45.Gg, 05.45.Vx **DOI:** 10.7498/aps.70.20210561

1 引 言

近年来, 随着互联网快速的发展, 通过网络进行信息传输越来越频繁, 由于攻击者可以截取信息或者改变信息的数据, 从而达到破坏数据传输的目的, 对信息的传输带来了巨大的威胁. 图像作为信息传递的主要载体, 找到一种实用的图像加密算法是很重要的[1−4]. 为了提高图像传输过程中的安全性, 研究人员提出了很多传输方案[5,6]. 随着混沌理论的发展, 研究表明混沌系统具有复杂的动力学行为和初值敏感性等特征[7−10], 使得其在图像加密中有很好的效果[11−13]. 因此研究人员结合混沌理论提出了越来越多的混沌图像加密算法[14−35].

混沌信号是混沌图像加密的核心, 一个具有复杂动力学行为的混沌信号对图像加密有很好的效果, 混沌信号主要由以下主要由以下 2 种混沌系统产生. 第 1 种是低维混沌系统, 如 Logistic 映射和 Tent 映射[36,37]. 该系统结构简单, 运行快, 易于硬件实现, 但是该系统容易退化且密钥空间较小. 第 2 种是高维混沌系统, 该系统具有较复杂的行为和更多的参数, 并且具有很强的抗退化能力[38], 例如 Wang 系统, Lorenz 系统和 Chen系统等. 此外, 在时间和空间方向上均具有混沌行为的时空混沌也是高维混沌系统, 如耦合映像格子系统 (coupled map lattice, CML)[39], 随机连接耦合格子时空混沌系统[40], 线性与非线性混合耦合时空混沌系统 (mixed linear-nonlinear coupled map lattice,

* 国家自然科学基金 (批准号: 61672124)、国家密码学发展“十三五”密码理论基金 (批准号: MMJJ20170203)、辽宁省科技创新领军人才基金 (批准号: XLYC1802013)、辽宁省重点研发计划 (批准号: 2019020105-JH2/103)、济南市“高校 20 条”资助项目引进创新团队计划 (批准号: 2019GXRC031) 和重庆市教委科学技术研究项目 (批准号: KJQN201900529) 资助的课题.

† 通信作者. E-mail: zhoushuang@cqnu.edu.cn

‡ 通信作者. E-mail: xywang@dlmu.edu.cn

MLNCML)[41].

为了更好地把混沌信号应用到图像加密中, 近年来, 很多学者对此进行了研究, 产生了很多基于混沌系统的图像加密算法. 一类是基于非 AI 技术的混沌图像加密算法, 如 Yasser 等[13] 提出了一种基于混合混沌系统的图像加密算法; 石航和王丽丹[42] 提出了一种基于压缩感知和多维混沌系统的多过程图像加密方案; 庄志本等[43] 提出了基于新的五维多环多翼超混沌系统的图像加密算法; Zhang 和 Wei[44] 结合 Lorenz 系统和 DNA 计算提出的彩色图像加密算法; Zhang 和 Wang[45] 结合线性与非线性混合耦合时空混沌系统 (MLNCML) 提出的对称图像加密算法等. 另一类是基于 AI 技术的混沌图像加密算法, 如陈炜等[46] 利用 BCNN 模型对图像进行压缩, 再利用混沌系统对图像进行加密; He 等[47] 使用了 LSTM 的网络结构对图像进行置乱和扩散也取得了不错的效果; 葛钊成和胡汉平[48] 的研究成果表明神经网络在图像加密中已有一定的积累, 并展现出比传统技术更好的应用效果. 虽然这方面的研究成果并不是很多, 但是为混沌密码学开辟了新的思路.

近年来, 随着深度学习技术和硬件条件的提高, 已经有研究人员将深度学习算法运用到混沌时间序列的预测中, 如熊有成和赵鸿[49] 用 LSTM 搭配合适的组合策略, 验证了低维情况下 LSTM 预测混沌时间序列能取得较好效果; Sangiorgio 等[50] 进一步验证了使用 LSTM 预测混沌时间序列不仅能取得较好效果, 还可以获得不错的鲁棒性; 黄伟建等[51] 结合混沌系统相空间重构理论, 提出了一种基于深度学习算法的混沌时间序列混合预测模型 (Att-CNN-LSTM). 因为深度学习具有较复杂的结构, 它预测生成的新混沌信号与原有混沌信号相比有一定差异, 且具有良好的混沌特性, 所以能够应用在图像加密中. 为了提高单一混沌系统的安全性, 本文提出了一种基于深度学习的混沌图像加密算法. 首先通过深度学习产生新的混沌信号, 然后将其用在图像加密中. 由于深度学习的参数具有敏感性, 故其可以作为加密算法的密钥, 整个加密算法的密钥空间相对传统的混沌系统图像加密算法更大, 增大了穷举攻击的难度, 通过统计分析及与文献的对比可知, 本文具有较高的安全性. 本文首先介绍所提方法使用的混沌系统及神经网络, 接着提出加密算法, 最后进行仿真实验及安全性能分析.

2 预备知识

利用深度学习生成新混沌信号用来进行图像加密, 由于新的混沌信号可以基于任意混沌系统 (如 Logistic 映射, Lorenz 系统, Chen 系统等), 因此选择其中一种混沌系统来说明本文的方法. 接下来, 介绍所提出的加密算法中用到的混沌系统及 LSTM 神经网络.

2.1 混沌系统

由于超混沌系统有多个正的 Lyapunov 指数, 相对于一般混沌系统具有较强的抗退化的能力, 系统的动态行为更加难以预测, 因此在保密通信方面比一般的混沌系统具有更高的使用价值[52]. 由于篇幅原因, 本文选择超混沌 Lorenz 系统来实现本文的方法, 超混沌 Lorenz 系统可表示为如下方程:

$$\begin{cases} \dot{x} = a(y-x)+w, \\ \dot{y} = cx - y - xz, \\ \dot{z} = xy - bz, \\ \dot{w} = -yz + rw, \end{cases} \tag{1}$$

其中, a, b, c 和 r 为超混沌 Lorenz 系统的参数. 当 $a=10$, $b=8/3$, $c=28$, $-1.52<r<-0.06$ 时, 该系统呈现超混沌态, 如图 1 所示, 当 $r=-1$ 时, (1) 式具有 4 个 Lyapunov 指数, $\lambda_1=0.3381$, $\lambda_2=0.1586$, $\lambda_3=0$, $\lambda_4=-15.1752$.

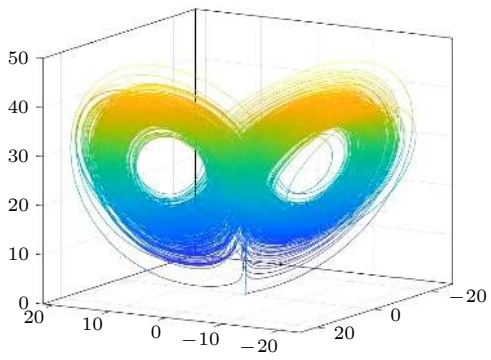

图 1 超混沌 Lorenz 相图三维投影

Fig. 1. Three dimensional projection of hyperchaotic Lorenz phase diagram.

2.2 LSTM 神经网络

长短期记忆人工神经网络 (long-short term memory, LSTM) 是一种时间递归的神经网络 (RNN)[53]. 在实际的应用中, RNN 容易受梯度消

失或梯度爆炸的影响, 难以捕获到序列之间的长期依赖, 使得训练异常困难. 所以为了解决 RNN 梯度消失的问题, LSTM 被提出并广泛被使用. 本文选择 LSTM神经网络来实现本文的方法.

LSTM 的结构有很多种形式, 但是都有类似的结构 (如图 2 所示), 主要都包含输入门、输出门、遗忘门. LSTM 单元的计算公式如下:

$$I_t = \sigma\left(X_t W_{xi} + H_{t-1} W_{hi} + b_i\right),$$

$$F_t = \sigma\left(X_t W_{xf} + H_{t-1} W_{hf} + b_f\right),$$

$$O_t = \sigma\left(X_t W_{xo} + H_{t-1} W_{ho} + b_o\right),$$

$$\tilde{C}_t = \tanh\left(X_t W_{xc} + H_{t-1} W_{hc} + b_c\right),$$

$$C_t = F_t C_{t-1} + I_t \tilde{C}_t,$$

$$H_t = O_t \tanh\left(C_t\right),$$

其中, I_t 是输入门, F_t 是遗忘门, O_t 是输出门. X_t 是时间步 t 的输入, H_t 是隐藏状态, C_t 是记忆细胞, FC 代表全连接层. 训练模型示意如图 2 所示.

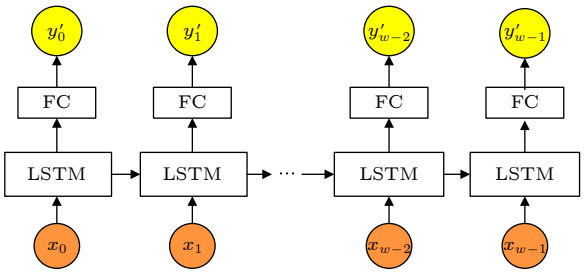

图 2 LSTM 训练模型示意

Fig. 2. LSTM training model diagram.

3 加密算法

本文提出的加密算法是一个扩散到置乱再到扩散的过程. 该加密算法主要步骤如图 3 和图 4 所示, 设明文图像记为 P, 其大小为 $M \times N$, 灰度等级为256.

1) 设置混沌系统的参数以及初值并产生混沌信号. 密钥 $K = \{x_0, y_0, z_0, w_0, r_1, r_2\}$, 其中 $\{x_0, y_0, z_0, w_0\}$ 为状态初值, r_1, r_2 是取值范围为 $[0, 255]$ 的整数随机数.

2) 设置深度学习的参数并产生新的混沌信号. 借助超混沌 Lorenz 系统产生 4 个伪随机信号, 依次记为 X, Y, Z, W, 其大小均为 $M \times N$, 具体步骤如下.

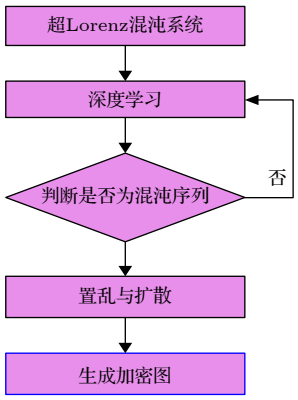

图 3 混沌图像加密算法流程图 (I)

Fig. 3. Chaotic image encryption flow chart algorithm (I).

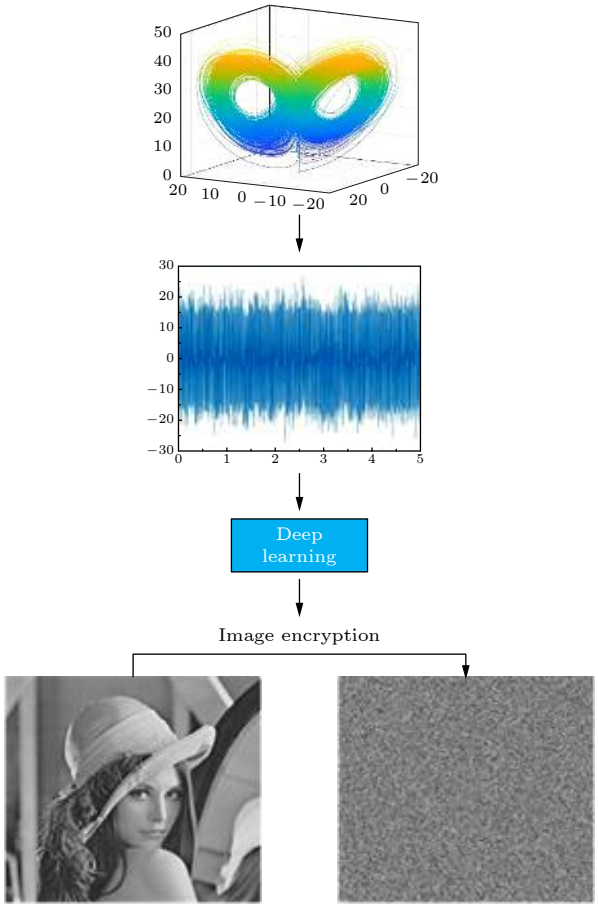

图 4 混沌图像加密算法流程图 (Ⅱ)

Fig. 4. Chaotic image encryption flow chart algorithm (Ⅱ).

Step 1 使用密钥 K 中的 $\{x_0, y_0, z_0, w_0\}$ 作为超混沌 Lorenz 系统的迭代初始值, 使用 ode45 函数迭代超混沌 Lorenz 系统, 得到 4 个伪随机序列, 依次记为 $\{x_i\}$, $\{y_i\}$, $\{z_i\}$, $\{w_i\}$, $i = 1, 2, \cdots, MN$;

Step 2 将伪随机序列 $\{y_i\}$ 截取长度为 s 的部分序列用 LSTM 网络深度学习, 训练数据的比例

是 p, 初始学习率为 q, 学习率下降因子为 u, 隐藏节点数为 o, 截取训练的序列长度为 s. 得到预测后新的序列 $\{y'_i, i=1,2,\cdots,MN\}$;

Step 3 对 $\{y'_i\}$ 进行混沌特性判断, 如果 $\{y'_i\}$ 为混沌序列, 则进入 Step 4; 否则重新设置参数, 返回 Step2;

Step 4 借助于下列公式将序列 $\{x_i\}$, $\{y'_i\}$, $\{z_i\}$ 和 $\{w_i\}$, $i=1,2,\cdots,MN$ 依次生成矩阵 X, Y, Z, W:

$$X(k,l)=\left\{\text{floor}\left[\left(\left|x_{(k-1)\times N+l}+y'_{(k-1)\times N+l}\right| \bmod 1\right)\times 10^{13}\right] \bmod MN\right\}+1,$$

$$Y(k,l)=\left\{\text{floor}\left[\left(\left|y'_{(k-1)\times N+l}\right| \bmod 1\right)\times 10^{13}\right]\right\} \bmod 256,$$

$$Z(k,l)=\left\{\text{floor}\left[\left(\left|z_{(k-1)\times N+l}\right| \bmod 1\right)\times 10^{13}\right] \bmod M\right\}+1,$$

$$W(k,l)=\left\{\text{floor}\left[\left(\left|w_{(k-1)\times N+l}\right| \bmod 1\right)\times 10^{13}\right] \bmod N\right\}+1,$$

这里, $k=1,2,\cdots,M$; $l=1,2,\cdots,N$, $\text{floor}(t)$ 返回小于或等于 t 的最大整数, mod1用于取序列的小数部分, 绝对值用于将负的状态值 $x+y'$, y', z 和 w 转化为正数.

3) 置乱与扩散对图像进行加密

① 进行扩散算法 Ⅰ, 借助伪随机矩阵 Y 将明文图像 P 变换为矩阵 A, 具体步骤如下.

Step 1 令 $i=1$, $j=1$;

Step 2 将 $P(i,j)$ 变换为 $A(i,j)$, 即

$$A(i,j)=[P(i,j)\oplus Y(i,j)\oplus r_1] \bmod 256;$$

Step 3 令 $j=j+1$;

Step 4 将 $P(i,j)$ 变换为 $A(i,j)$, 即

$$A(i,j)=[P(i,j)\oplus A(i,j-1)\oplus Y(i,j)] \bmod 256;$$

Step 5 如果 $j<N$, 跳转到 Step 3; 否则, 令 $j=1, i=i+1$, 如果 $i\leqslant M$, 跳转到 Step 6; 否则, 跳转到 Step 8;

Step 6 将 $P(i,j)$ 变换为 $A(i,j)$, 即

$$A(i,j)=\left[P(i,j)\oplus\sum_{i=1}^{N}A(i-1,j)\oplus Y(i,j)\right] \bmod 256;$$

Step 7 跳转到 Step 3;

Step 8 结束.

② 进行置乱算法. 置乱算法将图像 A 置乱为图像 B, 具体步骤如下.

Step 1 对于图像 A 中给定的一个像素点坐标 (i,j), 根据 (2) 式和 (3) 式计算得到 (m,n) 的值:

$$m=\left[\sum_{l=1}^{N}A(Z(i,j),l)\times 10^{13} \bmod M\right]+1, \quad (2)$$

$$n=\left[\sum_{k=1}^{M}A(k,W(i,j))\times 10^{13} \bmod N\right]+1. \quad (3)$$

如果 $m=i$ 或 $Z(i,j)$, 或者 $n=j$ 或 $W(i,j)$, 或者 $Z(i,j)=i$, 或者 $W(i,j)=j$, 则 $A(i,j)$ 位置保持不变; 否则, $A(i,j)$ 与 $A(m,n)$ 互换位置.

Step 2 当坐标 (i,j) 按从左到右、从上到下的扫描顺序遍历图像 A 中的所有像素点时, 重复 Step 1, 将图像 A 转化为图像 A'.

Step 3 将图像 A' 做如下处理:

$$A'=\text{reshape}(A,1,MN),$$

$\text{reshape}(A',1,MN)$ 把图像 A 转换成 MN 维行向量.

Step 4 将伪随机矩阵 $\boldsymbol{X}$ 做如下处理:

$$\boldsymbol{X}=\text{reshape}(X,1,MN),$$

$\text{reshape}(X,1,MN)$ 把伪随机矩阵 $\boldsymbol{X}$ 转换成 MN 维行向量.

Step 5 将 $\boldsymbol{X}$ 中重复的元素只保留一个.

Step 6 将集合 $\{1,2,\cdots,MN\}$ 中未出现在 $\boldsymbol{X}$ 中的元素按从小到大的顺序排列在 $\boldsymbol{X}$ 的末尾.

Step 7 对 A' 做如下处理:

$$A'(X_i)=A'(X_{MN-i+1})$$

$i=1,2,\cdots,\text{floor}(MN/2)$, $\text{floor}(t)$ 表示返回小于或等于 t 的最大整数.

Step 8 对 B 做如下处理, 将图像 A' 转化为图像 B:

$$B=\text{reshape}(A',M,N).$$

③ 最后进行扩散算法 Ⅱ, 扩散算法 Ⅱ 是从图像的最后一个像素点向前扩散, 借助于伪随机矩阵 Y 将图像 B 变成矩阵 $\boldsymbol{C}$, 具体步骤如下.

Step 1 令 $i=M, j=N$;

Step 2 将 $B(i,j)$ 变换为 $C(i,j)$, 即

$$C(i,j)=[B(i,j)\oplus Y(i,j)\oplus r_2] \bmod 256;$$

Step 3 令 $j=j-1$;

Step 4 将 $B(i,j)$ 变换为 $C(i,j)$, 即

$C(i,j)=[B(i,j)\oplus C(i,j+1)\oplus Y(i,j)]$ mod 256;

Step 5 如果 $j>1$, 跳转到 Step 3. 否则 $j=N, i=i-1$, 如果 $i\geqslant 1$, 跳转到 Step 6; 否则, 跳转到 Step 8;

Step 6 将 $B(i,j)$ 变换为 $C(i,j)$, 即

$$C(i,j)=\left[B(i,j)\oplus\sum_{j=1}^{N}(C(i+1,j))\oplus Y(i,j)\right] \text{ mod } 256;$$

Step 7 跳转到 Step 3;

Step 8 结束.

矩阵 $\boldsymbol{C}$ 即为所得密文图像.

4 解密过程

解密过程为加密过程的逆过程.

Step 1 输入密文图像 C, 4 个伪随机矩阵 $\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z},\boldsymbol{W}$ 以及 2 个伪随机数 r_1,r_2;

Step 2 进行扩散算法 Ⅱ 的逆算法, 得到矩阵 $\boldsymbol{B}_1$;

Step 3 进行置乱算法的逆算法, 得到矩阵 $\boldsymbol{A}_1$;

Step 4 进行扩散算法 Ⅰ 的逆算法, 得到明文图像 P.

5 计算机仿真试验结果

5.1 深度学习产生新混沌信号

为了得到新的序列 $\{y_i'\}$, 利用 LSTM 网络对超混沌 Lorenz 系统生成的序列 $\{y_i\}$ 进行深度学习. 模型训练过程如图 5 所示, 可以看出, 在 250 次迭代后, 得到的 LSTM 模型的均方根误差 (RMSE) 和损失函数 (Loss) 均接近于 0, 表示模型的拟合程度较好, 可以进行预测. 从图 6 和图 7 可以看出, 深度学习得到的新混沌信号 $\{y_i'\}$ 与超混沌 Lorenz 系统生成的混沌信号 $\{y_i\}$ 是不一样的.

5.2 动力系统分析

为了说明新混沌信号特点, 在最大 Lyapunov 指数、0-1 测试、功率谱、随机性等方面对新混沌信号 $\{y_i'\}$ 进行分析, 并与超混沌 Lorenz 系统产生的混沌信号 $\{y_i\}$ 进行对比.

5.2.1 最大 Lyapunov 指数分析

最大 Lyapunov 指数 (largest Lyapunov exponent, LLE) 是一个较为典型的判断一个系统是否具有混沌特性的工具. 从时间序列提取最大 Lyapunov 指数是 Wolf 等[54] 在 1985 年提出的一种数值方法, 此方法现已广泛应用, 具体如下.

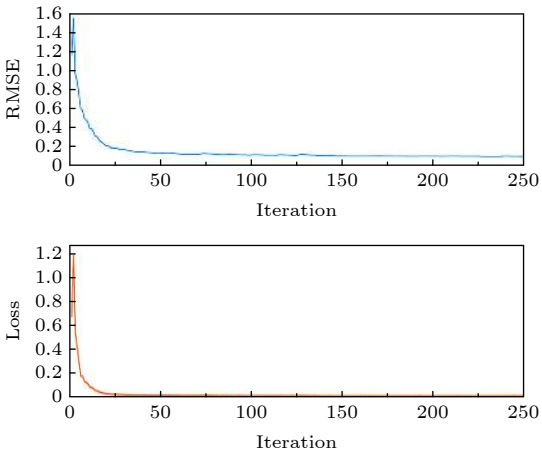

图 5 $\{y_i'\}$ LSTM 模型训练过程

Fig. 5. LSTM model training process of $\{y_i'\}$.

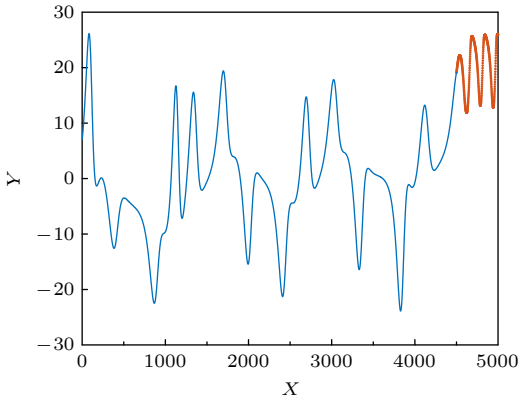

图 6 LSTM 模型预测

Fig. 6. Forecast of LSTM model.

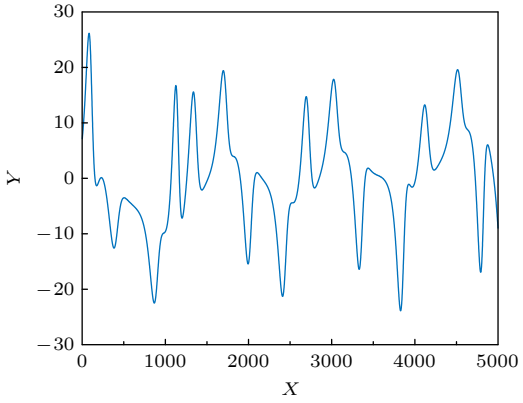

图 7 截取的 $\{y_i\}$

Fig. 7. Part of $\{y_i\}$.

1) 设给定时间序列$\{y(k)\}$, 重构的 m 维的相空间为

$$Y(k)=\{y(k),y(k+\tau),\cdots,y(k+(m-1)\tau)\},$$

其中 τ 为延迟时间.

2) 任意选取初始点$Y(k_0)$, 设其与最近的邻近点$Y_0(k_0)$的距离为$d(k_0)$, 从k_0时刻到k_1时刻两点的距离超过设定值 μ:

$$d'(k_1)=|Y(k_1)-Y_0(k_1)|>\mu,\ \mu>0.$$

3) 保留$Y(k_1)$, 并找其最近邻点$Y_1(k_1)$, 使得

$$d(k_1)=|Y(k_1)-Y_1(k_1)|<\mu,$$

并使得$d'(k_1)$与$d(k_1)$的夹角达到最小, 然后重复2)—3) 过程, 直到穷尽所有的数据点, 此时追踪演化过程中总迭代次数为 N, 则最大 Lyapunov 指数为

$$\lambda_1=\frac{1}{k_N-k_0}\sum_{i=1}^{N}\log_2\frac{d'(k_i)}{d(k_{i-1})}.$$

为了检验 LSTM 预测的序列$\{y_i'\}$是否具有混沌特性, 我们使用 Wolf 方法计算该序列的最大 Lyapunov 指数. 从图 8 可以看出, LLE 指数曲线一直在 $y=0$ 的上方, 因此, 该信号的 LLE 大于 0, 由于$\{y_i'\}$是有界的, 因此该序列是混沌的.

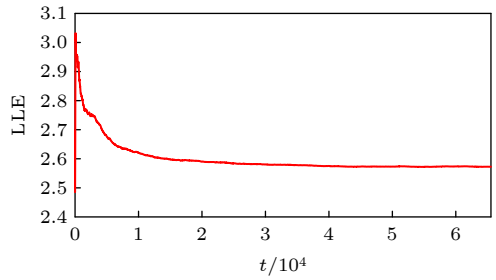

图 8 Wolf 方法求$\{y_i'\}$最大 Lyapunov 指数过程图

Fig. 8. Using wolf method to find the largest Lyapunov exponent process of $\{y_i'\}$.

5.2.2 0-1 测试

0-1 测试是一个能够衡量时间序列是否有混沌的一种测试算法, 与李雅普诺夫指数不同的是, 它不需要进行相空间重构, 通过输出结果是否接近于 1, 来判别混沌现象的产生[55,56].

对于给定的时间序列$\{x(i),i=1,2,\cdots,N\}$, 选取任意的$c\in[0,\pi]$, 定义函数$p(n)$与$q(n)$如下:

$$p(n)=\sum_{i=1}^{n}x(i)\cos(\mu(i)),\ \ n=1,2,\cdots,N,$$

$$q(n)=\sum_{i=1}^{n}x(i)\sin(\mu(i)),\ \ n=1,2,\cdots,N,$$

$$\mu(i)=ic,\ \ i=1,2,\cdots,n,$$

基于函数$p(n)$与$q(n)$, 均方位移$M(n)$为

$$M(n)=M_c(n)-(E(\eta))^2\frac{1-\cos nc}{1-\cos c},$$

其中

$$M_c(n)=\lim_{n\to\infty}\sum_{i=1}^{N}\left[(p(i+n)-p(i))^2+(q(i+n)-q(i))^2\right],$$

$$E(\eta)=\lim_{N\to\infty}\frac{1}{N}\sum_{i=1}^{N}x(i).$$

如果函数$p(n)$与$q(n)$的轨迹表现为布朗运动, 则函数$M(n)$随时间线性增长; 如果函数$p(n)$与$q(n)$的轨迹是有界的, 则函数$M(n)$是有界的. 定义均方位移$M(n)$的渐进线性增长率K_c如下:

$$K_c=\lim_{n\to\infty}\lg M(n)/\lg n,$$

如果$K_c\approx1$, 表示该时间序列具有混沌的特性; 如果$K_c\approx0$, 则表示该时间序列不具有混沌特性.

为了验证序列$\{y_i'\}$与$\{y_i\}$是否具有混沌特性, 对序列$\{y_i'\}$与$\{y_i\}$进行 0-1 测试. 测试结果如图 9和图 10 所示, 均方位移$M(n)$的渐进线性增长率K_c接近于 1, 所以序列$\{y_i'\}$与$\{y_i\}$均具有混沌特性.

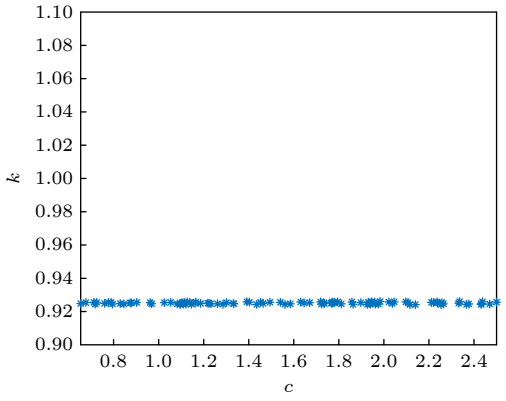

图 9 新混沌信号 0-1 测试图

Fig. 9. 0-1 test image of the new chaotic signal.

5.2.3 功率谱分析

为了验证序列$\{y_i'\}$与$\{y_i\}$是否具有周期性, 进行功率谱分析, 如图 11 和图 12 所示, 实验结果表

明, 序列 $\{y_i'\}$ 与 $\{y_i\}$ 不具有周期性, 且具有连续性和噪声背景, 因此可以用来进行图像加密.

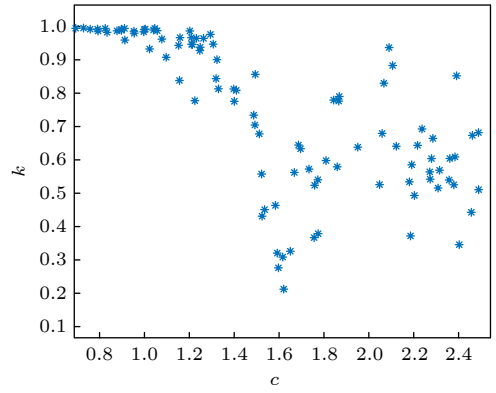

图 10 超混沌 Lorenz 系统混沌信号 0-1 测试图

Fig. 10. 0-1 test image of the hyperchaotic Lorenz signal.

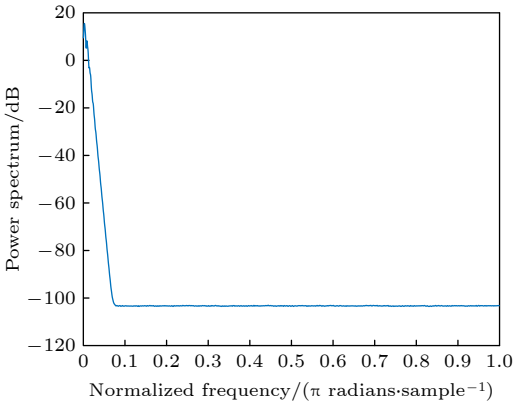

图 11 新混沌信号功率谱图

Fig. 11. The spectrum image of the new chaotic signal.

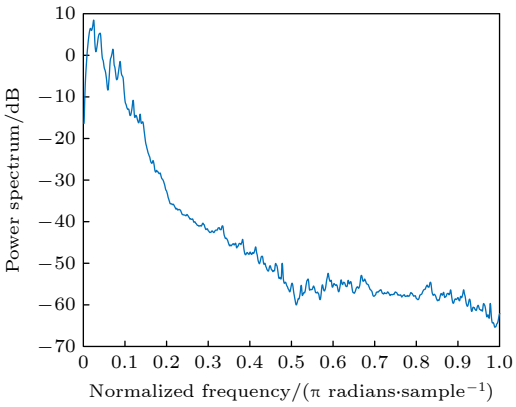

图 12 超混沌 Lorenz 信号功率谱图

Fig. 12. Spectrum image of hyperchaotic Lorenz signal.

5.2.4 三维相图

观察序列 $\{y_i'\}$ 与 $\{y_i\}$ 的三维相图, 如图 13 和图 14 所示, 从图中可以看出存在一个吸引域, 各个相点不断绕圈、折叠, 不断地靠近和远离这个吸引域, 但又不同于随机运动, 像这样的绕圈运动表示序列是混沌的, 因此序列 $\{y_i'\}$ 与 $\{y_i\}$ 是混沌的.

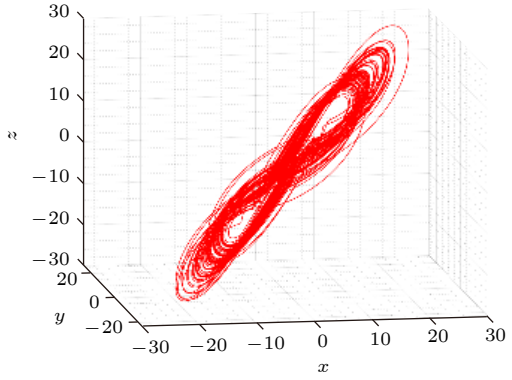

图 13 序列 $\{y_i'\}$ 的相图

Fig. 13. Phase diagram of $\{y_i'\}$.

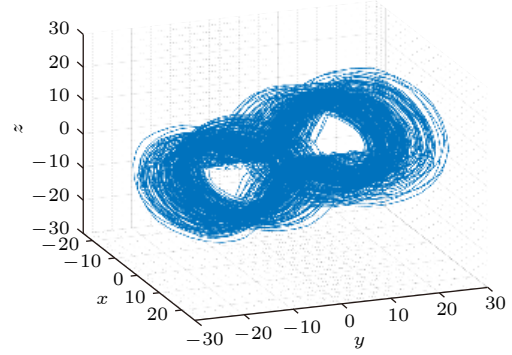

图 14 序列 $\{y_i\}$ 的相图

Fig. 14. Phase diagram of $\{y_i\}$.

5.2.5 随机性分析

为了验证序列 $\{y_i'\}$ 与 $\{y_i\}$ 的随机性, 选择了包括了 15 个测试的 NIST, 统计结果后得到概率 (p 值), 表 1 与表 2 中列出了序列 $\{y_i'\}$ 与 $\{y_i\}$ 的 NIST 测试结果. 从表 1 和表 2 可以看出, 所有 p 值明显大于 0.01, 所以序列 $\{y_i'\}$ 与 $\{y_i\}$ 与通过了 NIST 测试, 这意味着序列 $\{y_i'\}$ 与 $\{y_i\}$ 具有很好的随机性.

5.2.6 混沌信号的特征对比

通过以上实验, 将对比结果列在表 3 中. 从此表可知, 新混沌信号与原混沌信号通过功率谱分析、相图及 NIST 测试结果可以说明均具有混沌特征与随机性. 然而新信号的最大 Lyapunov 指数与 0-1 测试结果均高于原信号, 说明其具有更明显的混沌特征. 所以基于深度学习生成的新混沌信号更适合用于图像加密.

表 1 新混沌时间序列 NIST 测试

Table 1. NIST test of the new chotic time series.

统计测试	p 值	结果
单比特频率测试	0.8752	通过
块内频率测试	0.8523	通过
游程测试	0.6121	通过
块内最长1游程测试	0.0828	通过
二进制矩阵秩测试	0.1445	通过
离散傅里叶(谱)测试	0.8152	通过
非重叠模板匹配测试	0.3527	通过
重叠模板匹配测试	0.4305	通过
Maurer通用统计测试	0.4214	通过
线性复杂度测试	0.2341	通过
序列测试	0.3053	通过
近似熵测试	0.1568	通过
累加和测试	0.3257	通过
随机旅行测试	0.1523	通过
随机旅行变种测试	0.1057	通过

表 2 超混沌 Lorenz 混沌序列 NIST 测试

Table 2. NIST test of the hyperchaotic Lorenz time series.

统计测试	p 值	结果
单比特频率测试	0.8815	通过
块内频率测试	0.7253	通过
游程测试	0.5986	通过
块内最长1游程测试	0.0823	通过
二进制矩阵秩测试	0.1263	通过
离散傅里叶(谱)测试	0.8164	通过
非重叠模板匹配测试	0.3580	通过
重叠模板匹配测试	0.5216	通过
Maurer通用统计测试	0.4418	通过
线性复杂度测试	0.5052	通过
序列测试	0.6015	通过
近似熵测试	0.1435	通过
累加和测试	0.4863	通过
随机旅行测试	0.3997	通过
随机旅行变种测试	0.2265	通过

表 3 混沌信号统计参数对比

Table 3. Comparison of statistical parameters of chaotic signals.

信号来源	最大 Lyapunov 指数	0-1 测试	功率谱分析	相图	NIST 测试
超混沌 Lorenz	0.3381[52]	0.7937	混沌	混沌	随机
深度学习	2.6002	0.9250	混沌	混沌	随机

5.3 新混沌信号的应用

本节展示了一些常见的灰度图像仿真结果, 其中 Lena 图来自网址 (https://www.ece.rice.edu/~wakin/images/ [2021-01-01]), 其余图像来自网址 (http://sipi.usc.edu/database/database.php?volume=misc [2021-01-01]). 图像大小分别为 256×256, 512×512, 1024×1024, 灰度图像的加密与解密实验结果如图 15 所示. 从图 15 可以看出, 本文方法可以进行有效的加密和解密.

5.4 安全性分析

5.4.1 差分攻击

差分攻击是攻击者针对明文图像, 改变一个像素值然后加密图像, 观察两个加密后的密文图像之间的差距, 从而找到规律, 破解算法.

NPCR (number of pixels change rate) 与UACI (unified average changing intensity) 是差分攻击的两个重要指标, 它们通过 (4) 式和 (5) 式计算出来[57]:

$$\mathrm{NPCR}=\frac{\sum_{i,j}D(i,j)}{W\times H}\times100, \tag{4}$$

$$\mathrm{UACI}=\frac{1}{W\times H}\left[\sum_{i,j}\frac{|c_1(i,j)-c_2(i,j)|}{255}\right]\times100, \tag{5}$$

c_1 和 c_2 是两幅图像, 图像的尺寸是 $W\times H$. 如果 $c_1(i,j)\neq c_2(i,j)$, 则 $D(i,j)=1$, 否则, $D(i,j)=0$.

理论上 NPCR 与 UACI 的值越接近 99.6094% 和 33.4635% 越好. 本文选取 $P(256, 256)$ 的像素值做出改变, 并计算出它们的 NPCR 与 UACI 结果, 如表 4 所示. 对比代表性的文献 [10, 13, 58, 59] 中的 NPCR 与 UACI, 对比结果如表 5 所示. 实验结果及对比结果表明, 该算法的 NPCR 与 UACI 已经很接近理论值了, 因此本文提出的加密算法具有很好的抵抗差分攻击的能力.

5.4.2 密钥空间分析

在此图像加密系统中, x_0, y_0, z_0 和 w_0 的精度为 10^{-14}, r_1 和 r_2 为 0 至 255 的整数随机数. 训练数据的比例 p 的精度为 10^{-14}, 初始学习率 q 的精度为 10^{-14}, 学习率下降因子 u 的精度为 10^{-14}, 隐藏节点数 o 的取值范围为 $[1, M\times N-2]$, 截取进行深度学习的序列长度 s 的取值范围为

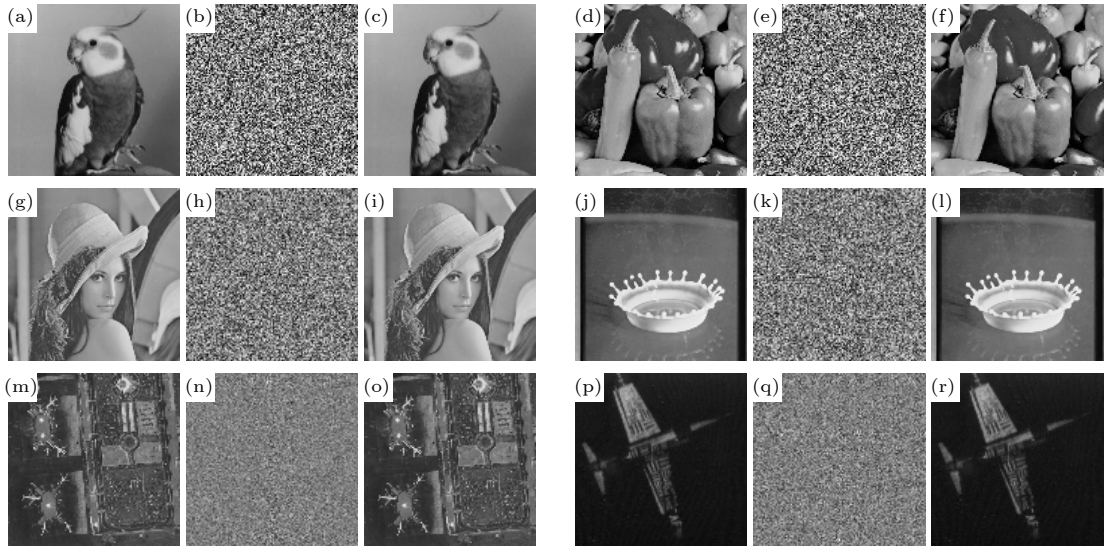

图 15 数字图像加密解密实验图 (a) 鸟 (256 × 256) 原图; (b) 鸟 (256 × 256) 加密图; (c) 鸟 (256 × 256) 解密图; (d) 辣椒 (256 × 256) 原图; (e) 辣椒 (256 × 256) 加密图; (f) 辣椒 (256 × 256) 解密图; (g)Lena(512 × 512) 原图; (h) Lena(512 × 512) 加密图; (i) Lena (512 × 512) 解密图; (j) 液体泼洒 (512 × 512) 原图; (k) 液体泼洒 (512 × 512) 加密图; (l) 液体泼洒 (512 × 512) 解密图; (m) 机场 (1024 × 1024) 原图; (n) 机场 (1024 × 1024) 加密图; (o) 机场 (1024 × 1024) 解密图; (p) 飞机 (1024 × 1024) 原图; (q) 飞机 (1024 × 1024) 加密图; (r) 飞机 (1024 × 1024) 解密图

Fig. 15. Experimental picture of digital image encryption and decryption: (a) Original bird image; (b) encrypted bird image; (c) decrypted bird image; (d) original pepper (256 × 256) image; (e) encrypted pepper (256 × 256) image; (f) decrypted pepper (256 × 256) image; (g) original Lena (512 × 512) image; (h) encrypted Lena (512 × 512) image; (i) decrypted Lena (512 × 512) image; (j) original splash (512 × 512) image; (k) encrypted splash (512 × 512) image; (l) decrypted splash (512 × 512) image; (m) original airport (1024 × 1024) image; (n) encrypted airport (1024 × 1024) image; (o) decrypted airport (1024 × 1024) image; (p) original airplane (1024 × 1024) image; (q) encrypted airplane (1024 × 1024) image; (r) decrypted airplane (1024 × 1024) image.

表 4 NPCR 和 UACI

Table 4. NPCR and UACI.

图片	改变 $P(256,256)$	
	NPCR/%	UACI/%
Bird (256 × 256)	99.56	33.35
Cameraman (256 × 256)	99.63	33.30
Pepper (256 × 256)	99.62	33.39
House (256 × 256)	99.63	33.37
Lena (512 × 512)	99.58	33.38
Airplane (512 × 512)	99.59	33.42
Tank (512 × 512)	99.61	33.49
Splash (512 × 512)	99.64	33.54
Truck (512 × 512)	99.60	33.47
Airport (1024 × 1024)	99.62	33.48
Airplane (1024 × 1024)	99.60	33.47

表 5 NPCR 和 UACI 的平均值与其他加密算法的比较

Table 5. The average of NPCR and UACI and comparison with other algorithms.

	本文平均值	文献[10]	文献[13]	文献[58]	文献[59]
NPCR/%	99.604	99.61	99.6641	99.61	99.6114
UACI/%	33.46	33.48	33.6124	33.46	33.4523

$$256\times256\times M\times N\times(M\times N-2)\times10^{98}$$

$$\approx 6.5536\times M\times N\times(M\times N-2)\times2^{339}>2^{100}.$$

而代表性的文献 [10, 13, 58—61] 中的密钥空间分别为 10^{98}, $>255\times1014^5$, 2^{283}, 2^{399}, 24×10^{45} 和 2^{256}, 实验结果及对比结果表明, 本算法是足够安全的.

5.4.3 密钥敏感性分析

一个好的算法是对密钥敏感的, 即对密钥做出微小的改变, 然后还原, 会得到完全不同的结果. 本文选取的密钥 x_0:

$$x_0=1.0,$$

对 x_0 改变生成新密钥:

$$x_0'=x_0+10^{-14}.$$

由于用错误的密钥进行还原, 所以不能有效解密, 如图 16(a)—(c) 所示. 此外, 由于本文中对 $\{y_i\}$ 进行深度学习后生成了新的序列 $\{y_i'\}$ 进行加密, 因此对加密图用 $\{y_i\}$ 不能进行有效解密, 如图 16(c) 所示. 综上, 本文加密方法具有较高的密钥敏感性.

5.4.4 直方图分析

直方图分析是检测密文像素值分布是否均匀, 一个好的加密算法, 密文直方图应该是均匀的. 否

则该加密算法是不安全的, 攻击者就能从密文中找到规律, 从而破解该算法.

图 17 展示了不同分辨率的灰度图像明文直方图与密文直方图. 通过观察, 明文直方图分布是不均匀的, 当经过本文的加密算法, 密文直方图分布是均匀的. 因此攻击者很难从密文中找到规律从而破解算法. 因此本文具有很好的抵抗统计攻击的能力.

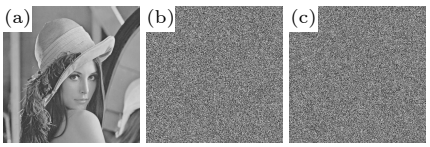

图 16 密钥敏感性 (a) 明文图像; (b) 密文用 x_0' 解密结果; (c) 密文用 $\{y_i\}$ 解密结果

Fig. 16. Sensitivity of secret key: (a) Original image; (b) error key x_0' restoring diagram; (c) error key $\{y_i\}$ restoring diagram.

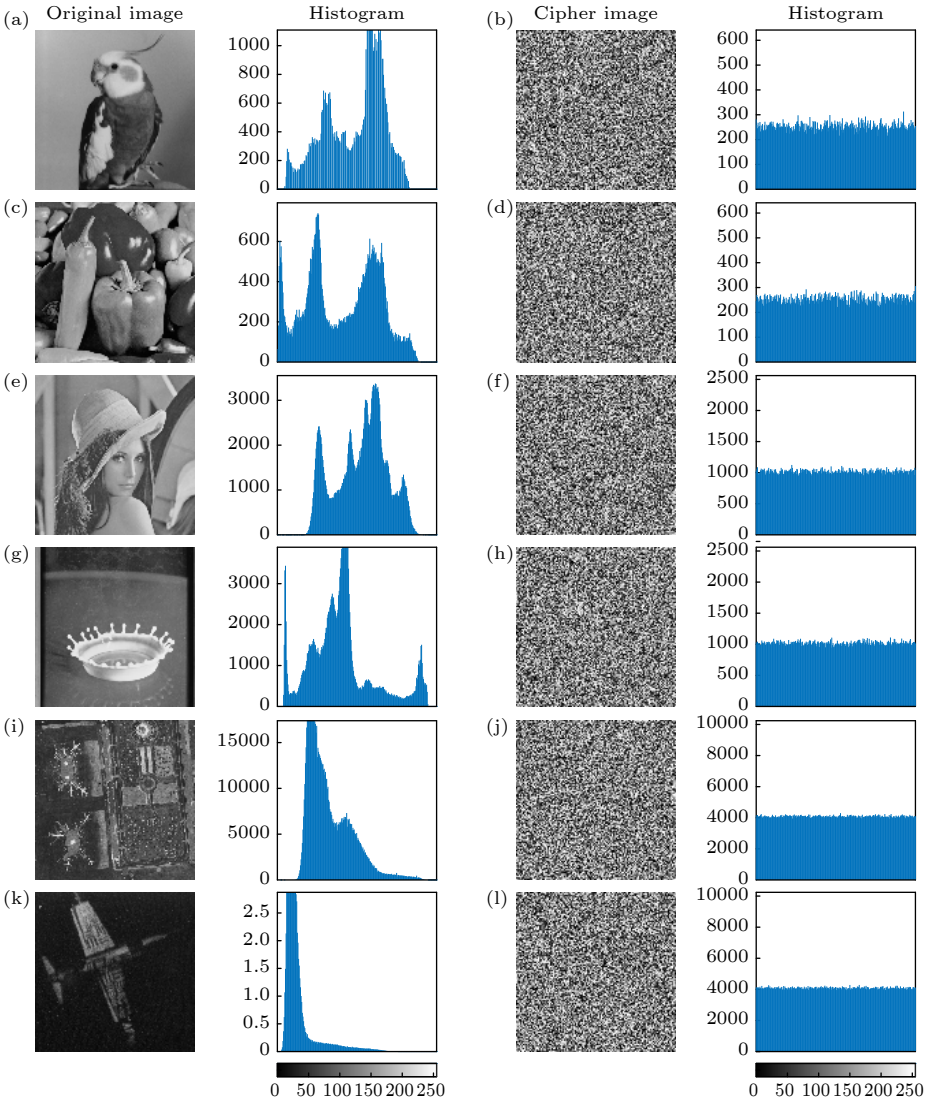

图 17 加密解密图像直方图 (a) 鸟 (256 × 256) 原图与明文直方图; (b) 鸟 (256 × 256) 加密图和密图直方图; (c) 辣椒 (256 × 256) 原图与明文直方图; (d) 辣椒 (256 × 256) 加密图和密图直方图; (e) Lena(512 × 512) 原图与明文直方图; (f) Lena(512 × 512) 加密图和密图直方图; (g) 水滴泼洒 (512 × 512) 原图与明文直方图; (h) 水滴泼洒 (512 × 512) 加密图和密图直方图; (i) 机场 (1024 × 1024) 原图与明文直方图; (j) 机场 (1024 × 1024) 加密图和密图直方图; (k) 飞机 (1024 × 1024) 原图与明文直方图; (l) 飞机 (1024 × 1024) 加密图和密图直方图

Fig. 17. Histograms of plain images and ciphered images: (a) Original image and histogram of bird (256 × 256); (b)cipher image and histogram of bird (256 × 256); (c) original image and histogram of pepper (256 × 256); (d) cipher image and histogram of pepper (256 × 256); (e) original image and histogram of Lena (512 × 512); (f) cipher image and histogram of Lena (512 × 512); (g) original image and histogram of splash (512 × 512); (h) cipher image and histogram of splash (512 × 512); (i) original image and histogram of airport (1024 × 1024); (j) cipher image and histogram of airport (1024 × 1024); (k) original image and histogram of airplane (1024 × 1024); (l) cipher image and histogram of airplane (1024 × 1024).

5.4.5 相关性分析

除上述直方图分析外, 统计分析中还有一种检测指标, 相邻像素值的相关性, 其包括水平相邻像素相关性, 垂直相邻像素相关性, 对角相邻像素相关性. 一个好的加密系统, 加密后得到的密文各个相邻像素值的相关性越接近于 0 代表加密效果越好, 这样攻击者就不能从密文中得到有效地信息, 很好的保护了加密算法. 接下来, 我们使用下面的公式来计算相邻像素值的相关性[62]:

$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}},$$

其中

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)).$$

$$D(x)=\frac{1}{N}\sum_{i+1}^{N}(x_i-E(x))^2, E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i.$$

首先, 本文在 Lena 明文和密文中随机选取 5000 对像素点进行测试, 如图 18 所示. 从图 18 可以看出, 明文各个方向具有很强的相关性, 而从密文的相关性具有很小的相关性.

接下来, 对其他图片进行仿真, 计算结果陈列在表 6 中, 并与一些代表性的文献 [10, 13, 58, 59] 的密文相关性作对比, 其结果展示在表 7 中. 实验结果表明, 本文的算法与一些代表性的文献作对比, 可以发现, 明文的 3 个方向上相关性很高, 经过本文算法的加密, 密文的 3 个方向上相关性变得很低, 与其他方法一样都接近于 0. 因此本文具有更好的安全性, 能够抵抗统计攻击.

5.4.6 信息熵分析

信息熵代表信息混乱的程度, 像素值越混乱信息熵越接近 8, 信息泄露的可能性越小, 信息熵通过 (6) 式计算[63]:

$$H(s)=\sum_{i=0}^{2^L-1}p(s_i)\log_2\frac{1}{p(s_i)}, \tag{6}$$

在 (6) 式中, $p(s_i)$代表 s_i 发生概率. 理论上信息熵的值越接近 8, 代表像素值分布越混乱, 信息泄露的可能性就越小. 采用灰度图像房屋 (house), 摄影师 (cameraman), 鸟 (bird), 辣椒 (pepper), Lena, 水滴泼洒 (splash), 飞机 (airplane)(512×512), 坦克(tank), 卡车 (truck), 机场 (airport), 飞机 (airplane)(1024×1024) 进行检测. 选取不同的差分攻击位置, 在表 8 中分别给出了明文的信息熵以及密文的信息熵, 代表性文献[10,13,58,59] 中 Lena (512×512)的信息熵分别为 7.9993, 7.9993, 7.9993, 7.999239. 实验结果表明我们得到的密文信息熵 7.9993 和其他方法一样都非常接近于 8, 表示信息泄露的可能性很小, 攻击者几乎不能从密文中找到有效信息, 因此本文提出的算法具有很好的安全性.

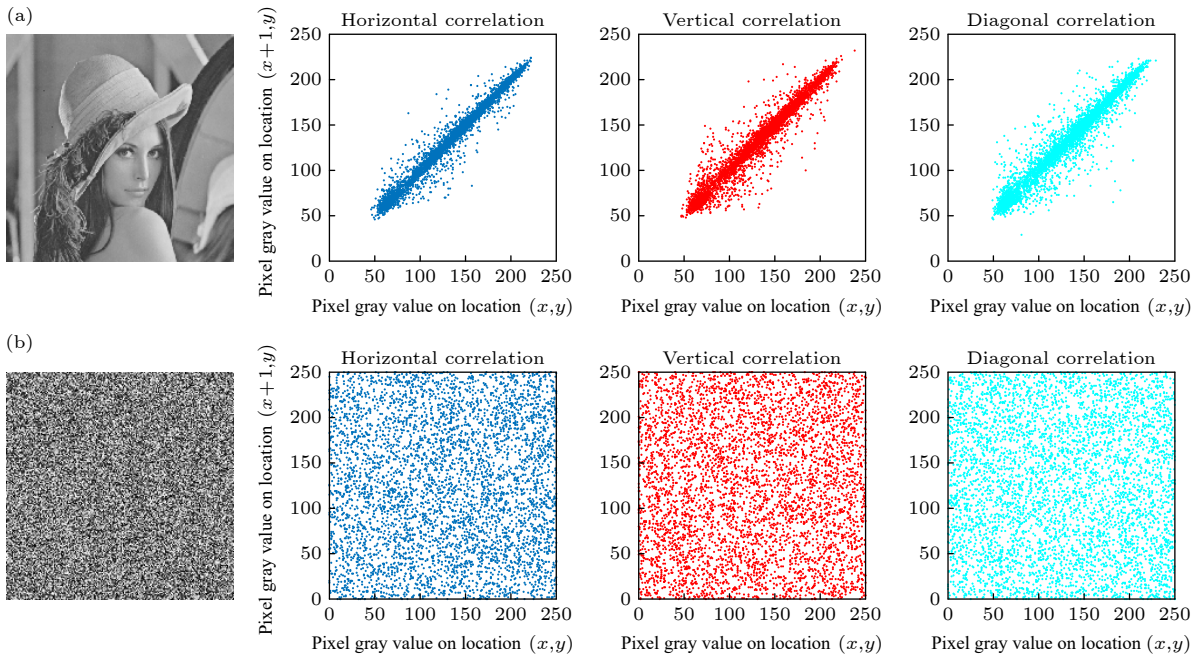

图 18 Lena 图相关性分析 (a) 明文; (b) 密图

Fig. 18. Correlation coefficients of Lena: (a) Original image; (b) encrypted image.

表 6 图像相关系数

Table 6. Correlation coefficients of images.

图片	明文				密文			
	水平	垂直	对角	反对角	水平	垂直	对角	反对角
Lena	0.9844	0.9668	0.9620	0.9790	–0.0016	0.0014	–0.0014	–0.0010
Bird	0.9889	0.9826	0.9713	0.9519	0.0114	0.0103	0.0104	–0.0031
Cameraman	0.9591	0.9335	0.9101	0.9377	–0.0099	0.0141	–0.0165	–0.0028
Pepper	0.9638	0.9585	0.9368	0.9339	–0.0127	–0.0014	–0.0079	0.0134
Airport	0.9066	0.9072	0.8446	0.8752	–0.0091	0.0088	–0.0014	–0.0054
Splash	0.9925	0.9850	0.9797	0.9507	0.0082	0.0016	0.0039	–0.0060
Airplane	0.9476	0.9664	0.9418	0.9299	–0.0278	–0.0105	0.0013	–0.0083
House	0.9549	0.9780	0.9399	0.9027	0.0141	–0.0115	–0.0176	0.0005
Tank	0.8678	0.8815	0.8414	0.7949	–0.0036	0.0003	–0.0098	–0.0065
Truck	0.9258	0.9561	0.9114	0.8194	0.0028	–0.0041	0.0018	0.0074

表 7 密文图像相关系数比较

Table 7. Comparison of the correlation coefficients of images.

	Lena	文献[10]	文献[13]	文献[58]	文献[59]
水平	–0.0016	–0.00007	0.00047	–0.00251	–0.038118
垂直	0.0014	–0.0024	–0.03911	–0.00292	–0.029142
对角	–0.0014	0.0019	0.00305	–0.00156	0.002736

表 8 信息熵

Table 8. Information entropy of images.

图片	图片大小	信息熵
House	256 × 256	7.9969
Cameraman	256 × 256	7.9971
Bird	256 × 256	7.9968
Pepper	256 × 256	7.9971
Lena	512 × 512	7.9993
Splash	512 × 512	7.9993
Airplane	512 × 512	7.9993
Tank	512 × 512	7.9994
Truck	512 × 512	7.9993
Airport	1024 × 1024	7.9998
Airplane	1024 × 1024	7.9998

5.4.7 鲁棒性分析

鲁棒性是检验加密算法抗干扰能力的重要指标. 在传输过程中信息有可能部分丢失或受到噪声污染, 因此需要设计一个加密算法, 即使丢失一部分信息, 也可以通过解密程序得到明文的一些主要信息. 我们通过剪切攻击和噪声攻击两种方式来检测本文加密算法的鲁棒性.

图 19(a)—(c) 展示了不同程度的剪切攻击, 图 19(d)—(f) 展示了不同程度的高斯白噪声攻击, 从图中可以看出, 尽管密文丢失一些信息或者一些信息被污染, 还可以通过解密得到明文的一些主要信息, 因此本文的加密算法具有较好的鲁棒性.

5.4.8 已知明文和选择明文攻击的分析

全黑或全白图像经常被用来评估所提出的密码系统对已知明文和选择明文攻击的抵抗力. 对全黑图像与全白图像进行加密解密, 结果如图 20 所示, 可见我们的方法可以对这两个图进行有效的加密和解密. 接着对全黑图像与全白图像进行统计分析, 如表 9 所列. 通过此表可以得出, 各种指标均接近理论值, 因此本图像加密算法对已知明文和选择明文攻击具有较好的抗攻击性.

表 9 全黑全白图的统计分析

Table 9. The statistical analysis of all-black image and all-white image.

	NPCR	UACI	信息熵	相关系数		
				水平	垂直	对角
全黑图	0.9958	0.3332	7.9970	0.0016	0.0003	0.0036
全白图	0.9961	0.3351	7.9971	0.0070	0.0004	0.0070

6 结 论

本文提出了一种基于深度学习的图像加密算法, 利用 LSTM 神经网络对混沌序列进行深度学习, 生成了新的混沌信号, 将其用来进行图像加密. 相对于其他神经网络模型, 深度学习模型具有复杂的结构和较多的参数, 这给破解带来了很大的难度. 通过对比实验结果表明, 该算法具有更好的安全性, 能抵抗常见的攻击. 但是由于设备条件限制, 对于较大数据集, 加密算法的效率有待提高.

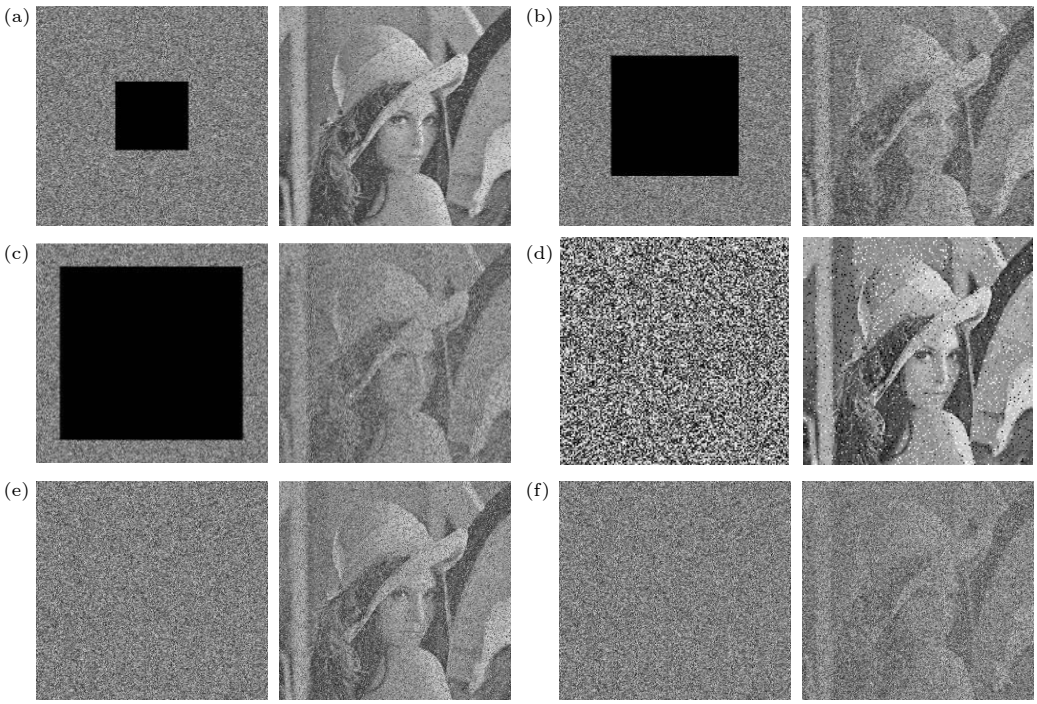

图 19 抗攻击性检验 (a) 10% 剪切; (b) 30% 剪切; (c) 80% 剪切; (d) 0.001 高斯白噪声攻击; (e) 0.01 高斯白噪声攻击; (f) 0.1 高斯白噪声攻击

Fig. 19. Anti attack test: (a) 10% data missed; (b) 30% date missed; (c) 80% data missed; (d) attack of 0.001 Gaussian white noise; (e) attack of 0.01 Gaussian white noise; (f) attack of 0.1 Gaussian white noise.

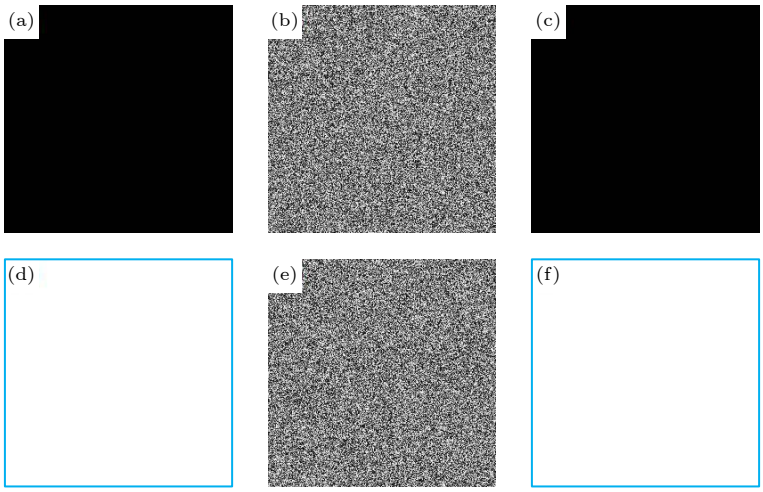

图 20 全黑全白图加密解密图像

Fig. 20. Encryption and decryption image of all black and all white image.

参考文献

[1] Wang X Y, Teng L, Qin X 2012 *Signal Pro.* **92** 1101
[2] Liu W H, Sun K H, Zhu C X 2016 *Optics Lasers Eng.* **84** 26
[3] Wu X J, Kan H C, Kurths J 2015 *Appl. Soft Comput.* **37** 24
[4] Hua Z Y, Zhou Y C, Pun C M, Chen C. L. P 2015 *Inf. Sci.* **297** 80
[5] Zheng H Y, Li L, Xiao D 2021 *Net Inf. Security* **21** 10 (in Chinese) [郑洪英, 李琳, 肖迪 2021 信息网络安全 **21** 10]
[6] Dharavathu K, Mosa A 2020 *Int. J. Commun. Syst.* **33** e4369
[7] Zhao J F, Wang S Y, Chang Y X, Li X F 2015 *Nonlinear Dyn.* **80** 1721
[8] Khan M 2015 *Nonlinear Dyn.* **82** 527
[9] Chai X L, Gan Z H, Yuan K, Yang L Chen Y R 2017 *Chin. Phys. B* **26** 020504
[10] Chai X L, Fu J Y, Zhang J T, Han D J, Gan Z H 2021 *Neural Comput. Appl.* **33** 10271
[11] Ran Q W, Yuan L, Zhao T Y 2015 *Opt. Commun.* **348** 43
[12] Kaur M, Kumar V 2018 *Int. J. Bifurcat. Chaos* **28** 1850132
[13] Yasser I, Khalifa F, Mohamed M A, Samrah A S 2020 *Complexity* **2020** 9597619
[14] Wu J H, Liao X F, Yang B 2017 *Signal Pro.* **141** 109
[15] Wang X Y, Feng L, Zhao H Y 2019 *Inf. Sci.* **486** 340
[16] Wang X Y, Li Z M 2019 *Optics Lasers Engin.* **115** 107
[17] Zhang Y 2018 *Multimed. Tools Appl.* **77** 21589

[18] Bansal R, Gupta S, Sharma G 2017 *Multimed. Tools. Appl.* **76** 16529
[19] Hua Z Y, Zhou Y C, Huang H J 2019 *Inf. Sci.* **480** 403
[20] Wang X Y, Yang J J 2021 *Inf. Sci.* **569** 217
[21] Mandal M K, Kar M, Singh S K, Barnwal V K 2014 *Secur. Commun. Netw.* **7** 2145
[22] Wang X Y, Gao S 2020 *Inf. Sci.* **539** 195
[23] Wang M X, Wang X Y, Zhao T T, Zhang C, Xia Z Q, Yao N M 2021 *Inf. Sci.* **544** 1
[24] Wang X Y, Wang T, Xu D H, Chen F 2014 *Int. J. Modern Phys. B* **28** 1450023
[25] Zhou S, Wang X Y, Wang M X, Zhang Y Q 2020 *Chaos Solitons & Fract.* **141** 110225
[26] Wang X Y, Gao S 2020 *Inf. Sci.* **507** 16
[27] Wang X Y, Liu C, Jiang D H 2021 *Inf. Sci.* **574** 505
[28] Zhang Y Q, Wang X Y 2015 *Appl. Soft Comput.* **26** 10
[29] Zhang Y Q, Jia Y R, Wang X Y, Niu Q, Chen N D 2020 *IEEE Access* **8** 213296
[30] He Y, Zhang Y Q, Wang X Y 2020 *Neural Comput. Appl.* **32** 247
[31] Zhang Y Q, Wang X Y, Liu L Y, Liu J 2018 *Int. J. Bifurcat. Chaos* **28** 1850020
[32] Zhang Y Q, He Y, Wang X Y 2018 *Physica A* **490** 148
[33] Zhou S, Wang X Y, Zhang Y Q, Ge B, Wang M X, Gao S 2021 *Multimed. Syst. (Published Online)*
[34] Zhang Y 2016 *Chaotic Digital Image Cryptosystem* (Beijing: Tsinghua University Press) pp106–205 (in Chinese) [张勇 2016 混沌数字图像加密 (北京: 清华大学出版社) 第106—205页]
[35] Liu S T, Sun F Y 2009 *Sci. Sin-Phys. Mech. Astron.* **39** 387 (in Chinese) [刘树堂, 孙福艳 2009 中国科学 (G 辑: 物理学 力学 天文学) **39** 387]
[36] May R M 1976 *Nature* **261** 459
[37] Kanso A 2011 *Commun. Nonlinear Sci. Numer. Simul.* **16** 822
[38] Li S L, Liu C X, Hu X Y, Ni J K 2017 *J. Xi'an Jiaotong Univ.* **51** 35 (in (in Chinese) [Chinese) [李石磊, 刘崇新, 胡晓宇, 倪骏康 2017 西安交通大学学报 **51** 35]
[39] Kaneko K 1989 *Physica D* **34** 1
[40] Sinha S 2002 *Phys. Rev. E* **66** 016209
[41] Zhang Y Q 2015 *Ph. D. Dissertation* (Dalian: Dalian University of Technology) (in Chinese) (in Chinese) [张盈谦 2015 博士学位论文 (大连: 大连理工大学)]
[42] Shi H, Wang L D 2019 *Acta Phys. Sin.* **68** 200501 (in Chinese) [石航, 王丽丹 2019 物理学报 **68** 200501]
[43] Zhuang Z B, Li J, Liu J Y, Chen S Q 2020 *Acta Phys. Sin.* **69** 040502 (in Chinese) [庄志本, 李军, 刘静漪, 陈世强 2020 物理学报 **69** 040502]
[44] Zhang Q, Wei X P 2013 *IETE Techn. Re.* **30** 404
[45] Zhang Y Q, Wang X Y 2014 *Inf. Sci.* **273** 329
[46] Chen W, Guo Y, Jing S W 2020 *Acta Phys. Sin.* **69** 240502 (in Chinese) [陈炜, 郭媛, 敬世伟 2020 物理学报 **69** 240502]
[47] He Y, Zhang Y Q, He X, Wang X Y 2021 *Sci. Rep.* **11** 6398
[48] Ge Z C, Hu H P 2021 *Cryptol. Res.* **8** 215 (in Chinese) [葛钊成, 胡汉平 2021 密码学报 **8** 215]
[49] Xiong Y C, Zhao H 2019 *Sci. Sin-Phys. Mech. Astron.* **49** 92 (in Chinese) [熊有成, 赵鸿 2019 中国科学: 物理学 力学 天文学 **49** 92]
[50] Sangiorgio M, Dercole F 2020 *Chaos, Solitons Fract.* **139** 110045
[51] Huang W J, Li Y T, Huang Y 2021 *Acta Phys. Sin.* **70** 010501 (in Chinese) [黄伟建, 李永涛, 黄远 2021 物理学报 **70** 010501]
[52] Wang X Y, Wang M J 2007 *Acta Phys. Sin.* **56** 5136 (in Chinese) [王兴元, 王明军 2007 物理学报 **56** 5136]
[53] Hochreiter S, Schmidhuber J 1997 *Neural Comput.* **9** 1735
[54] Wolf A, Swift J B, Swinney H L, Vastano J A 1985 *Phys. D:Nonlinear Phenomena* **16** 285
[55] Gottwald G A, Melbourne I 2009 *SIAM J. Appl. Dyn. Syst.* **8** 129
[56] Gottwald G A, Melbourne I 2004 *P. Roy. Soc. A-Math. Phy.* **460** 603
[57] Wu Y, Noonan J P, Agaian S 2011 *Cyber J.* **1** 31
[58] Nepomuceno E G, Nardo L G, Arias-Garcia J, Butusov D N, Tutueva A 2019 *Chaos* **29** 061101
[59] Zhou M J, Wang C H 2020 *Signal Pro.* **171** 107484
[60] Xian Y J, Wang X Y 2021 *Inf. Sci.* **547** 1154
[61] Wang X Y, Xue W H, An J B 2020 *Chaos, Solitons Fract.* **141** 110309
[62] Boriga R, Dăscălescu A C, Priescu I 2014 *Signal Processing: Image Communication* **29** 887
[63] Abolfazl Y N, Mohammad H M, Masood N T 2017 *Optics Lasers Eng.* **90** 225

A new chaotic signal based on deep learning and its application in image encryption*

Zhao Zhi-Peng [1)] Zhou Shuang [1)†] Wang Xing-Yuan [2)‡]

1) (*School of Mathematical Sciences, Chongqing Normal University, Chongqing* 401331, *China*)

2) (*School of Information Science and Technology, Dalian Maritime University, Dalian* 116026, *China*)

(Received 25 March 2021; revised manuscript received 8 July 2021)

Abstract

To improve the security of image encryption in singular chaotic systems, an encryption algorithm based on deep-learning is proposed in this paper. To begin with, the chaos sequence is generated by using a hyperchaotic Lorenz system, prior to creating new chaotic signals based on chaotic characteristics obtained from he simulations of the powerful complex network structure of long-short term memory artificial neural network (LSTM-ANN). Then, dynamic characteristics of the new signals are analyzed with the largest Lyapunov exponent, 0-1 test, power spectral analysis, phase diagrams and NIST test. In the end, the new signals are applied to image encryption, the results of which verify the expected increased difficulty in attacking the encrypted system. This is attributable to the differences of the new signals generated using the proposed method from the original chaotic signals, as well as arises from the high complexity and nonlinearity of the system. Considering its ability to withstand common encryption attacks, it is hence reasonable to conclude that the proposed method exhibits higher safety and security than other traditional methods.

Keywords: chaotic system, image encryption, deep learning

PACS: 05.45.Gg, 05.45.Vx **DOI:** 10.7498/aps.70.20210561

* Project supported by the National Natural Science Foundation of China (Grant No. 61672124), the Password Theory Project of the 13th Five-Year Plan National Cryptography Development Fund, China (Grant No. MMJJ20170203), the Liaoning Province Science and Technology Innovation Leading Talents Program Project, China (Grant No. XLYC1802013), the Key R&D Projects of Liaoning Province, China (Grant No. 2019020105-JH2/103), the Jinan City' 20 Universities' Funding Projects-Introducing Innovation Team Program, China (Grant No. 2019GXRC031), and the Science and Technology Research Program of Chongqing Municipal Education Commission, China (Grant No. KJQN201900529).

† Corresponding author. E-mail: zhoushuang@cqnu.edu.cn

‡ Corresponding author. E-mail: xywang@dlmu.edu.cn