基于动态参数控制的混沌系统图像加密算法

王丽娟 李国东 吕冬梅
(新疆财经大学统计与数据科学学院 乌鲁木齐 830012)

摘 要 针对单混沌系统结构简单、安全性低、相关性强等问题,提出了一种基于动态参数控制的混沌系统图像加密算法。首先,构造新的混沌系统(LCT)产生混沌序列,并对其进行排序得到一组序列,对原始位置进行索引,得到一组位置索引序列,将图像矩阵按照得到的索引位置序列进行置乱;其次,应用 henon 混沌映射得到的两个混沌序列,设计了一种新的产生伪随机序列的方法,得到一个新的混沌序列,并将其与得到的置乱图像进行异或处理,从而得到最终的密文图像。实验结果表明:密文图像与明文图像的相关性较小;任取明文图像的两个像素值,其 NPCR 与 UACI 的测试值分别为 99.6414%,99.6380%和 33.3869%,33.3852%,较接近理论值;明文图像熵值为 7.4416,密文图像熵值为 7.9889。因此,该算法具有较强的鲁棒性、可靠的安全性,可以有效地提高加密系统的各种抗攻击能力。

关键词 LCT 混沌系统,henon 混沌系统,索引序列,图像加密
中图法分类号 TP309 **文献标识码** A

Chaotic System Image Encryption Algorithm Based on Dynamic Parameter Control

WANG Li-juan LI Guo-dong LV Dong-mei
(Xinjiang University of Finance and Economics, School of Statistics and Data Science, Urumqi 830012, China)

Abstract To solve the problems of simple structure, low security and strong correlation of single chaotic system, a chaotic system image encryption algorithm based on dynamic parameter control was proposed. Firstly, a new chaotic system (LCT) is constructed to generate chaotic sequences, which are sorted to get a set of sequences, and the original positions are indexed to get a set of position index sequences, and image moments are obtained. The array is scrambled according to the sequence of index positions obtained. Secondly, a new method of generating pseudo-random sequence is designed by using two chaotic sequences obtained from Henon chaotic map, and a new chaotic sequence is obtained. The new ch-aotic sequence and the scrambled image are XOR processed to obtain the final ciphertext image. Experiment results show that correlation between ciphertext image and plaintext image is small, and the test values of NPCR and UACI are 99.6414%, 99.6380% and 33.3869%, 33.3852%, respectively for two pixel values of plaintext image, which are close to the theoretical value; the entropy value of plaintext image is 7.4416, and that of ciphertext image is 7.9889. Therefore, the algorithm has strong robustness, reliable security, and can effectively improve the anti-attack ability of encryption system.

Keywords LCT chaotic system, Henon chaotic system, Index sequence, Image encryption

1 引言

随着计算机技术的迅猛发展与网络的普及,网络逐渐成为信息传递的主要工具,文本信息、音频、图像等一些多媒体文件通过网络来传输。其中,图像凭借其自身的直观性现已成为网络信息传输的主要载体之一,在媒介传输中发挥着不可替代的作用。因此,图像数据的安全性现已成为各界的主要关注对象,而图像加密是解决图像安全性的一种重要方法,其中混沌加密已成为国内外有关学者研究的重要领域。

由于混沌系统是非线性的动力系统,具有初值敏感性强、状态遍历性、随机性强、结构更复杂、难以分析预测等特点,因此在图像加密领域得到了广泛的应用[1]。大量实验证明,借助混沌系统产生的伪随机混沌信号来实现图像加密,其加密效果和安全性更高。Zhu 等[2]提出了用改进的帐篷映射来实现对图像加密,经过仿真实验表明加密算法能有效抵抗统计攻击、差分攻击、选择明文以及密文攻击等攻击方式;Akhshani 等[3]改进了 Logistic 混沌映射,提出了一种量子 Logistic 映射,并用该映射对图像加密,通过实验及结果安全性分析证明了该加密算法具有较高的安全性。赵国敏等[4]在广义 Henon 与 CNN 超混沌系统相结合的基础上用产生的序列进行处理,该算法图像加密抗攻击性强,较为安全;黄清梅等[5]利用细胞神经网络的超混沌性质,经图像的像素进行置乱,达到了加密的目的,得到其置乱度较高、容易实现的结论。Zhou 等[6]利用一些已有 1 维混沌系统构建新的 1 维混沌系统,提出新 1 维混沌加密算法,该算法的混沌范围宽、混沌行为好,但仅通过旋转操作置乱图像,置乱随机性不高,具有

本文受自治区自然科学基金(2017D01A24)资助。
王丽娟(1994—),女,硕士,主要研究方向为数据挖掘与图像处理,E-mail:1575516311@qq.com;**李国东**(1972—),男,博士,教授,硕士生导师,主要研究方向为数据挖掘与图像处理,E-mai:lgdzhy@126.com(通信作者)。

周期性，置乱效果欠佳。

针对混沌系统随机性不高、具有周期性等特点导致加密效果不佳，本文提出了一种基于动态参数控制的混沌系统图像加密算法方案，构造新的动态参数控制的混沌映射(LCT)，产生混沌序列的索引位置序列对原始图像进行置乱，再利用henon映射产生的混沌序列构造新的混沌序列对置乱图像进行扩散，从而得到加密图像。解决了混沌系统随机性不高、结构简单、具有周期性等问题。

2 混沌系统

2.1 动态参数控制混沌系统

动态参数控制混沌系统[7]是用一个混沌映射来控制另一个混沌系统的参数。$F(x)$表示控制混沌映射，是由一个一维混沌系统构成，$M(x)$表示种子混沌映射，是由一个一维混沌系统构成，$N(x)$表示转换关系函数，它被用来将 $F(x)$的输出映射到 $M(x)$的参数范围内。动态参数控制混沌系统的数学表达式如式(1)所示：

$$\begin{cases} x_{n+1}=M(p_{n+1},x_n) \\ p_{n+1}=N(y_{n+1}) \\ y_{n+1}=F(\mu,y_n) \end{cases} \tag{1}$$

本文利用 Logistic 和 Tent 混沌映射构造一个新的混沌系统(Logistic Control Tent，LCT)。即用 Logistic 混沌系统控制 Tent 混沌系统，Logistic 用作控制混沌映射 $F(x)$，Tent 用作种子混沌映 $M(x)$，其可以生成 1 个一维的混沌映射。

Logistic 混沌系统表达式为：

$$x_{n+1}=\mu x_n(1-x_n) \tag{2}$$

其中，μ 为映射的参数，当 $\mu=4$ 时，Logistic 映射具有混沌特性，$x_n\in[0,1]$。

Tent 混沌系统的动力学方程定义为[8]：

$$\begin{cases} x_{n+1}=\mu x_n, & 0<x_n\leqslant 0.5 \\ x_{n+1}=\mu[1-x_n], & 0.5<x_n\leqslant 1 \end{cases} \tag{3}$$

其中，$x_n\in(0,1)$，$\mu\in(0,2)$。当 $\mu>1$ 时，系统处于混沌状态。

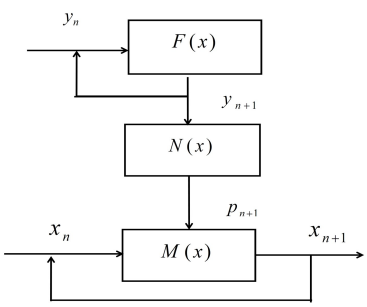


图 1 动态参数控制混沌系统结构图

图 1 中，y_n 为控制混沌映射 $F(x)$的初值，x_n 为种子混沌映射 $M(x)$的初值。

本文所用的 Tent 混沌映射作为种子映射 $M(x)$，Tent 映射具有连续的混沌范围，因此本文所构造的新的混沌系统 LCT 具有良好的混沌行为。

2.2 Henon 混沌映射

Henon 映射是一个二维非线性映射系统[9]，Henon 算法是利用混沌序列对图像像素值进行扩散。其动力学方程定义如下：

$$\begin{cases} u_{i+1}=1-au_i^2+v_i \\ v_{i+1}=bu_i \end{cases} \tag{4}$$

其中，a，b 为混沌系统控制参数，当 $a=1.4$，$b=0.3$ 时 Henon 处于混沌状态。

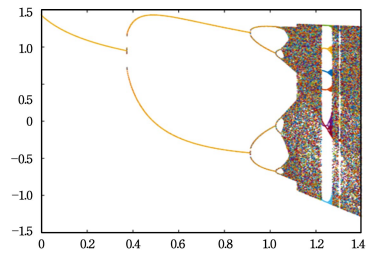


图 2 Henon 混沌映射分叉图

2.3 Henon 混沌系统的伪随机序列发生器设计

由 Henon 混沌系统的动力学方程式可知，产生 $u=\{u_1,u_2,\cdots,u_i\}$和 $v=\{v_1,v_2,\cdots,v_i\}$两个混沌序列，由此来构造一个新的混沌序列 w_i，使其具有较好的伪随机性，具体构造方法如式(5)所示：

$$w_i=\begin{cases} u_i, & u_i>v_i \\ v_i, & u_i<v_i \\ 0, & u_i=v_i \end{cases} \tag{5}$$

其中，Lyapunov 指数为 0.318，可知该序列处于混沌状态。

3 本文加密算法

本文加密算法的过程如图 3 所示。

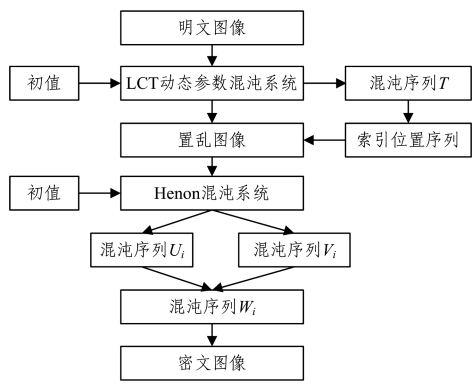


图 3 图像加密流程图

具体加密算法的步骤如下：

(1)选取一幅大小为 $M\times N$ 的灰度级数字图像，计算图像的像素值总和并记作 s，利用式(6)计算出混沌系统初始迭代的次数 k，即：

$$k=s \bmod 10^3+10^3 \tag{6}$$

(2)将 Logistic 混沌系统迭代 $M\times N-1$ 次，得到伪随机数 t_1，并对其做以下处理：

$$t=\mathrm{mod}((t_1*10^3),2)+1 \tag{7}$$

(3)根据上述步骤得到的 t，将其作为 Tent 混沌系统的控制参数 μ 及迭代次数 k，来消除初态效应的影响。

(4)继续对 Tent 混沌系统从 k 次进行迭代 100000 次，截取迭代 10000 次后长度为 $M\times N$ 的混沌序列，记作 $T=\{t_1,t_2,\cdots,t_{M\times N}\}$，产生的混沌序列的值均介于 0～1 之间。

(5)将步骤(4)产生的混沌序列 T 进行排序，得到排序序列 $E=\{e_1^T,e_2^T,\cdots,e_{M\times N}^T\}$，记录该序列在原始序列中的位置序列。

$$E=sort(T) \tag{8}$$

(6)利用索引位置序列，对原始图像的像素进行置乱操作，得到置乱图像 C'。

$$x(i,j)\leftrightarrow x[l(i),l(j)] \tag{9}$$

(7)输入密钥 u_0 和 v_0，对 Henon 混沌映射系统进行迭代 100 000，截取迭代 20 000 次后长度为 $M\times N$ 的混沌序列 $u=\{u_1,u_2,\cdots,u_{M\times N}\}$ 及 $v=\{v_1,v_2,\cdots,v_{M\times N}\}$。

(8)由 u,v 两个混沌序列，按照式(5)来构造一个新的混沌序列 w_i，使其具有较好的伪随机性。按照式(8)对新得到的伪随机序列 w_i 做处理：

$$D=floor(abs(w_i)*1000) \bmod 256 \tag{10}$$

其中，$abs()$表示取绝对值，$floor()$表示向下取整。

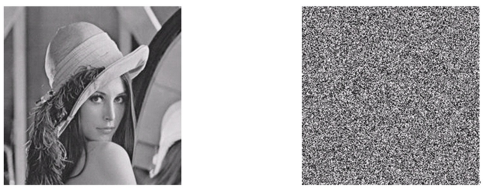
(9)将步骤(8)得到的混沌序列 D 与置乱图像 C'进行异或操作，即可得到密文图像。

$$C=D\oplus C' \tag{11}$$

4　仿真实验及安全性分析

4.1　仿真实验结果

实验选用 Lena 图像作为样本图像，其大小为 256×256，仿真实验中，将 Logistic 混沌系统中 $\mu=4,x_1=0.6$ 作为密钥；Tent 混沌系统中 $s=8018004,x_0=0.3678$，迭代次数作为密钥；Henon 混沌映射系统的控制参数为 $a=1.4,b=0.3$，将 $u_0=0.3989,v_0=0.4010$，迭代次数作为密钥，经过实验检测，密文图像如图 4 所示。

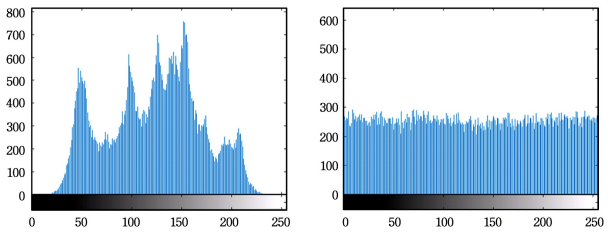


(a)明文图像　　(b)密文图像

图 4　明文与密文图像

4.2　直方图统计特性分析

从图 5(a)可以看出，明文图像的灰度直方图的像素的分布不均，波动较大；图 5(b)中，像素的直方图分布较为均匀，对信息起到了收敛作用，使明文图像各像素间的相关性被打破，使得原图没有了统计特性。



(a)明文图像直方图　　(b)密文图像直方图

图 5　明文与密文图像直方图

4.3　相邻像素的相关性分析

相邻像素的相关性分析是用来反映像素的扩散程度，用相关系数 r 来表示，一般地，在水平、垂直和对角方向上，明文图像像素点间有较强的相关性，而密文图像中的相关性较小，本文在两幅图中的水平、垂直和对角方向上进行测试，随机选取 1000 对像素进行计算。记它们的灰度值为$(u_i,v_i),i=1,2,\cdots,N$，则向量 $u=\{u_i\}$ 和 $v=\{v_i\}$ 间的相关系数计算公式如下：

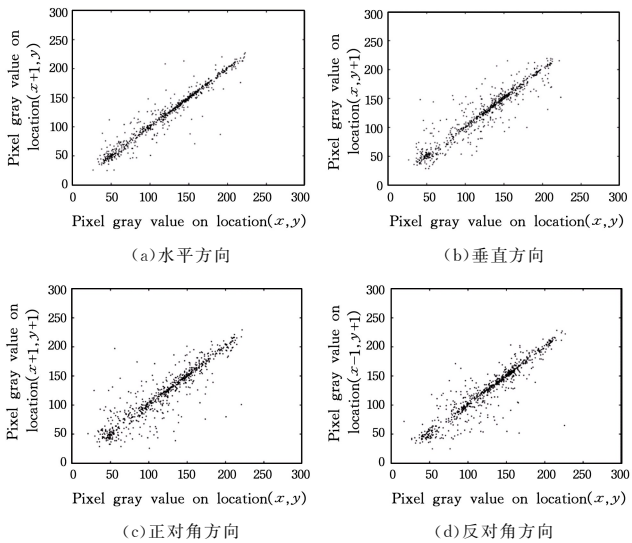
$$r_{xy}=\frac{\mathrm{cov}(u,v)}{\sqrt{D(u)}\sqrt{D(v)}} \tag{12}$$

$$\mathrm{cov}(u,v)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(u))(y_i-E(v)) \tag{13}$$

$$D(u)=\frac{1}{N}\sum_{i=1}^{N}(u_i-E(u))^2 \tag{14}$$

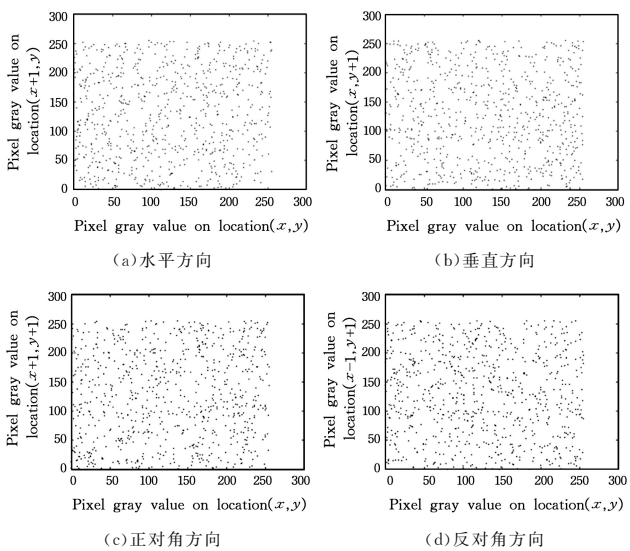
$$E(u)=\frac{1}{N}u_i \tag{15}$$

设 u_i 的坐标为$\{x_i,y_i\}$，若 v_i 的坐标为$\{x_i+1,y_i\}$，则计算水平方向上的相关系数；若 v_i 的坐标为$\{x_i,y_i+1\}$，则计算垂直方向上的相关系数；若 v_i 的坐标为$\{x_i\pm1,y_i+1\}$，则计算正反对角上的相关系数。图 6 为明文图像在水平、垂直、对角方向上的相关性图，从图中可以看出，明文图像在各个方向上具有颇强的相关性，有明显的线性关系；图 7 为密文图像在水平、垂直、对角方向上的相关性图，从图中可以看出，密文图像在各个方向上的相邻点几乎没有任何关系。



(a)水平方向　(b)垂直方向　(c)正对角方向　(d)反对角方向

图 6　明文图像相关性图



(a)水平方向　(b)垂直方向　(c)正对角方向　(d)反对角方向

图 7　密文图像相关性图

表 1　相关系数

方向	明文图像	密文图像
水平方向	0.9680	−0.0484
垂直方向	0.9247	0.0263
正对角方向	0.9202	−0.0132
反对角方向	0.9275	−0.0248

4.4　信息熵分析

信息熵分析用于描述信息的不确定性，图像灰度值的分

布越均匀，信息熵就越大，信息熵的计算式如下：

$$H(m)=-\sum_{i=0}^{255}p(m_i)\log_2 p(m_i) \tag{16}$$

其中，$p(m_i)$是灰度值为 m_i 出现的概率，那么$\sum_{i=0}^{255}p(m_i)=1$，信息熵越接近于 8，说明它的抗攻击性越好，每个像素值的概率越接近，灰度值分布越均匀，抗统计攻击性就越好。本文加密算法的信息熵是 $H=7.9889$，加密前的信息熵是 $H=7.4416$，可以看出加密后的信息熵更接近于 8，本文算法能够较好地抵抗统计攻击。

4.5 差分分析

NPCR(像素改变率)表示当明文图像中任意像素值发生微小变化或密钥做出微小的变动时，会大幅度改变密文图像的信息，NPCR 越接近理想值，说明密文对明文的敏感性越好；UACI(归一化平均改变强度)，当两个指标的值越接近理想值，说明对明文图像的细微改变越敏感，抗攻击能力越强。

$$NPCR=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)}{M\times N}\times 100\% \tag{17}$$

$$UACI=\frac{1}{M\times N}\left[\sum_i\sum_j\frac{|D_1(i,j)-D_2(i,j)|}{256}\right]\times 100\% \tag{18}$$

其中，D_1 表示密文，D_2 表示明文图像像素值发生改变时的密文。在明文图像中任取两个像素点，由式(17)计算可得，NPCR=99.6414%，NPCR=99.6380%，说明本文算法密文对明文的敏感性较好；由式(18)可得，UACI=33.3869%，UACI=33.3852%，说明本文加密算法可以较好地抵抗差分攻击。

结束语 本文采用 Logistic 混沌系统控制 Tent 混沌映射及 henon 混沌映射将混沌理论应用于图像加密领域。首先，通过构造新的动态参数控制的混沌系统(LCT)对其产生的混沌序列进行排序，从而得到一组序列，对原始位置进行索引，得到一组位置索引序列，将图像矩阵按照得到的索引位置序列进行置乱；其次，应用 henon 混沌映射得到的两个混沌序列，设计了一种新的产生伪随机序列的方法，得到一个新的混沌序列，并将其与得到的置乱图像进行异或处理，从而得到最终的密文图像。本文算法的优势在于得到的混沌序列的随机性更高，消除了其具有周期性的特点及其混沌系统较为复杂，弥补了混沌系统结构单一的缺点，增加了图像置乱与扩散的复杂度，使得其具有良好的安全性。从仿真结果及安全性能分析中可以看出，本文算法的敏感性强，安全性高。

参 考 文 献

[1] WANG X, WANG T. A novel algorithm for image encryption based on couple chaotic systems[J]. International Journal of Modern Physics B, 2012, 26(30): 395.

[2] ZHU C X, SUN K H. Chaos Image Encryption Algorithm by Correlating Keys with Plaintext[J]. China Communications, 2012, 9(1): 73-79.

[3] AKHSHANI A, AKHAVAN A, LIM S, et al. An image encryption scheme based on quantum Logistic map[J]. Communications in Nonlinear Science and Numerical Simulation, 2012, 17(12): 4653-4661.

[4] 赵国敏，李国东. 基于广义 Henon 映射以及 CNN 超混沌系统图像加密方案[J]. 信阳师范学院学报(自然科学版)，2015(1)：141-145.

[5] 黄清梅，李国东. 基于 CNN 超混沌特性对图像加密技术的应用研究[J]. 绵阳师范学院学报，2017(2)：60-66.

[6] ZHOU Y, BAO L, CHEN C. A new 1D chaotic system for image encryption[J]. Signal Processing, 2014, 97: 172-182.

[7] 薛伟，王磊. 一种基于新型混沌的彩色图像加密算法[J]. 光学技术，2018，44(3)：263-268.

[8] 平萍，李健华，毛莺池，等. 混沌映射与比特重组的图像加密[J]. 中国图象图形学报，2017，22(10)：1348-1355.

[9] 黄冬梅，耿霞，魏立斐. 基于 Henon 映射的加密遥感图像的安全检索方案 [J]. 软件学报，2016，27(7)：1729-1740.

(上接第 445 页)

[8] BUCZAK A L, GUVEN E. A survey of data mining and machine learning methods for cyber security intrusion detection [J]. IEEE Communications Surveys & Tutorials, 2016, 18(2): 1153-1176.

[9] 宋海涛，韦大伟，汤光明，等. 基于模式挖掘的用户行为异常检测算法[J]. 小型微型计算机系统，2016，37(2)：221-226.

[10] 赵刚，姚兴仁. 基于用户画像的异常行为检测模型[J]. 信息网络安全，2017(7)：18-24.

[11] 丁珊. 基于深度学习的入侵检测关键技术研究[D]. 北京：北京交通大学，2018.

[12] QIAO Y, XING Z, FADLULLAH Z M, et al. Characterizing Flow, Application, and User Behavior in Mobile Networks: A Framework for Mobile Big Data[J]. IEEE Wireless Communications, 2018, 25(1): 40-49.

[13] ALTHOFF T, JINDAL P, LESKOVEC J. Online actions with offline impact: How online social networks influence online and offline user behavior[C]// Proceedings of the Tenth ACM International Conference on Web Search and Data Mining. ACM, 2017: 537-546.

[14] MILLER D J, WANG Y, KESIDIS G. Anomaly detection of attacks (ADA) on DNN classifiers at test time[C]// 2018 IEEE 28th International Workshop on Machine Learning for Signal Processing (MLSP). IEEE, 2018: 1-6.

[15] AMARASINGHE K, KENNEY K, MANIC M. Toward explainable deep neural network based anomaly detection[C]// 2018 11th International Conference on Human System Interaction (HSI). IEEE, 2018: 311-317.

[16] KWON D, KIM H, KIM J, et al. A survey of deep learning-based network anomaly detection[J]. Cluster Computing, 2017: 1-13.

[17] LÓPEZ A U, MATEO F, NAVIO-MARCO J, et al. Analysis of Computer User Behavior, Security Incidents and Fraud Using Self-Organizing Maps[J]. Computers & Security, 2019.

[18] The Bro Network Security Monitor[OL]. http://www.bro.org.

[19] ALJAWARNEH S, ALDWAIRI M, YASSEIN M B. Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model[J]. Journal of Computational Science, 2018, 25: 152-160.

[20] HE H, GARCIA E A. Learning from imbalanced data[J]. IEEE Transactions on Knowledge and Data Engineering, 2009, 21(9): 1263-1284.