

引用格式:魏慧,李国东. 基于细胞神经网络超混沌特性的图像加密算法[J]. 微电子学与计算机,2020,37(5):43-48. [WEI H, LI G D. Image encryption algorithm based on hyperchaotic characteristics of cellular neural networks[J]. Microelectronics & Computer,2020,37(5):43-48.]

基于细胞神经网络超混沌特性的图像加密算法

魏 慧^{1,2},李国东^{1,2}

(1 新疆财经大学 统计与数据科学学院, 新疆 乌鲁木齐 830012;

2 新疆财经大学 新疆社会经济统计研究中心, 新疆 乌鲁木齐 830012)

摘 要: 针对图像传输安全问题,本文提出基于细胞神经网络 CNN 超混沌的特性结合一般形式的三次函数鲁棒映射和高维 Lorenz 系统对图像采取双扩散—置乱的加密操作. 仿真结果表明本文设计的算法具有优良的加密效果,且密钥空间大、密文敏感性强、信息熵值 7.9994 接近理想值,能有效抵抗统计攻击等. 具有一定的运用价值.

关键词: CNN 超混沌;高维 Lorenz 系统;图像加密;三次函数鲁棒映射

中图分类号: TP309.7

文献标识码: A

文章编号: 1000—7180(2020)05—0043—06

Image encryption algorithm based on hyperchaotic characteristics of cellular neural networks

WEI Hui^{1,2}, LI Guo-dong^{1,2}

(1 College of Statistics and Data Science, Xinjiang University of Finance and Economics, Urumqi

830012, China;2 Center for Social and Economic Statistics, Xinjiang University

of Finance and Economics, Urumqi 830012,China)

Abstract: Images have become the main media active in the information age. There is no doubt about the importance of image encryption technology. In order to solve the problem of image transmission security, the proposed algorithm is based on the hyper chaotic features of cellular neural network CNN combined with the general form of cubic function robust mapping and high-dimensional Lorenz system to adopt double diffusion-scrambling encryption operation on images. The simulation results show that the algorithm designed in this paper has excellent encryption effect. Its key space is large, ciphertext sensitivity is strong, information entropy value is 7.9994 close to ideal value, and it can effectively resist statistical attacks. The algorithm in this paper has high security and certain application value.

Key words: CNN hyperchaos;high dimensional lorenz system;image encryption;robust mapping of cubic function

1 引言

当今社会对保密通信的高度重视,人们的目光在密码学领域也逐渐不断地转移创新,现阶段聚焦在混沌理论上. 于是混沌加密成为一个热门话题,但是也存在密钥遗失和传输过程中抗攻击能力弱的问

题. 数字图像作为当下一信息传输的主要媒介. 同时,图像加密也属于加密技术的范畴. 基于文献[1-8]存在不安全性问题的改进,本文提出了一种六阶 CNN 超混沌系统结合具有强鲁棒性的三次混沌映射与高维混沌系统^[6]对数字图像加密.

2 算法原理及步骤

本文针对数字图像加密问题,利用细胞神经网络(CNN),提出了一种基于六阶细胞神经网络和多混沌系统结合对数字图像在双扩散-置乱框架下的加密算法。由六阶细胞神经网络混沌系统选择出能够作为密钥源的变量,选择则出的密钥源作为高维 Lorenz 系统^[9-10]的初始密钥,产生伪随机序列进而生成密码 X 与 Z 对数字图像加密处理。将明文数字矩阵值量化处理后作为一级三次函数鲁棒混沌系统的初始值,迭代为伪随机序列生成密码 Y 用于明文图像的置乱操作,这使得密文与明文紧密关联如图 1 所示^[11]。

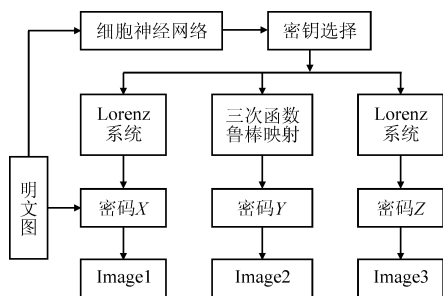


图 1 技术路线流程图

2.1 算法设计步骤

Step1: 给定样本图像 $p(m, n)$, 由 $\text{rgb2gray}(p)$ 转换为灰度图像 $I(m, n)$ (文中的明文图像)。读取明文图像矩阵 $M \times N$, 选出 $\max(M, N) = Q$, 取 $g = \text{mod}(Q, 6) + 1$ 。

Step2: 设 $x_{i(i=1, 2, \dots, 6)}$ 为初始密钥, 把明文图像的像素值作扰动因子, 实现六阶 CNN 超混沌系统生成的密钥流和明文关联, 达到该算法方案能够抵御明文攻击与选择明文攻击的目的, 即:

$$x_i = \text{mod}\left(\frac{\text{sum}(I)}{256}, 1\right) \quad (1)$$

Step3: 密钥的选取。选取上述六阶细胞神经网络系统产生的混沌序列 $x_{i(i=4, 5, 6)}$, 取给定位置上的三个数作为预设条件值(本文选取 x_3, x_4, x_5 的第 350 位数), 在满足下列条件下产生一级密钥 key_1 :

$$\begin{aligned} 0 < g \leq 2, \text{key}_1 &= x_3 \\ 2 < g \leq 4, \text{key}_1 &= x_3 + x_4 \\ 4 < g \leq 6, \text{key}_1 &= x_3 + x_4 + x_5 \end{aligned} \quad (2)$$

Step4: 前向扩散。将上步骤中的密钥 key 输入高维 Lorenz 混沌映射中, 进行反复迭代 $800 + 2 \times MN$ 次, 并且每 3 000 次对序列 s_x 利用 s_y 进行扰动,

再将其混沌序列 s_x 由式(3)处理得到密码 X 。对明文图像进行前向扩散处理, 得到密文 image_1 。

$$X = \text{mod}(\text{floor}(s_x * 2^{16}), 256) \quad (3)$$

Step5: 置乱。由明文图像选取的 Z 值做一下处理得到 16 bit 的密钥 key_2 , 作为三次函数混沌映射的初值, 反复迭代 $1\,000 + MN$ 次, 前 1 000 次消除暂态效应。对明文图像置乱处理, 得到密文 image_2 。

$$Z = T / 10^8 \quad (4)$$

式中: T 为明文图像的像素总数。

Step6: 后向扩散。首先, 选取上述六阶细胞神经网络系统产生的混沌序列 $x_{i(i=4, 5, 6)}$, 同步骤 3(本文选取 x_1, x_2, x_6 的第 255 位数), 使给定的值在满足(5)下产生第二个一级密钥 key_3 , 其次, 密钥 key_3 输入高维 Lorenz 混沌映射中, 进行反复迭代 $800 + 2 \times MN$ 次, 并且每 3 000 次对序列 s_z 利用 s_w 进行扰动, 再将其混沌序列 s_z 与 s_x 做相同处理得到密码 Z 。得到最终密文 image_C 。

$$\begin{aligned} 0 < g \leq 2, \text{key}_3 &= x_1 \\ 2 < g \leq 4, \text{key}_3 &= x_1 + x_2 \\ 4 < g \leq 6, \text{key}_3 &= x_1 + x_2 + x_6 \end{aligned} \quad (5)$$

Step7: 解密是加密的逆过程。主要为: 密文信息的提取, 逆扩散, 逆置乱, 二次逆扩散^[11-13]。

3 本文算法

3.1 细胞神经网络模型

首先, 引入比较简化的细胞神经网络模型, 即:

$$\frac{d x_i}{d t} = -x_j + a_j p_j + G_0 + G_s + i_j \quad (6)$$

式中, j 表示细胞; x_i 表示变量状态; a_j 表示常亮; i_j 表示门限值; G_0 表示连接细胞的输出值; G_s 表示状态变量线性组合; P_j 表示细胞的输出值^[3], 可由式(7)得出:

$$P_j = 0.5(|x_j + 1| - |x_j - 1|) \quad (7)$$

文献[3, 14]描述了 6 维细胞神经网络系统的混沌现象特性, 6 阶全互联 CNN 方程如下:

$$\frac{d x_i}{d t} = -x_j + a_j p_j + \sum_{\substack{k=1 \\ k \neq j}}^6 a_{j,k} p_k + \sum_{k=1}^6 s_{jk} x_k + i_j \quad (8)$$

式中, $i = 1, 2, \dots, 6$ 。

六阶细胞神经网络(CNN)的详细参数如下:

$$\begin{aligned} a_j &= 0(j = 1, 2, 3, 4, 5, 6); a_{j,k} = 0(j, k = 1, 2, \dots, 6; j \neq k); i_j = 0(j = 1, 2, \dots, 6); a_4 = 200; \end{aligned}$$

$$S_{jk} = \begin{bmatrix} 1 & 0 & -1 & -1 & 0 & 0 \\ 0 & 3 & 1 & 0 & 0 & 0 \\ 12 & -12 & 0 & 0 & 0 & 0 \\ 90 & 0 & 0 & -94 & 0 & 0 \\ 1 & 18 & 0 & 0 & 0 & 0 \\ 0 & 100 & 0 & 0 & 4 & -3 \end{bmatrix}, i_j = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

上述方程可写为:

$$\begin{cases} \frac{dx_1}{dt} = -x_3 - x_4 \\ \frac{dx_2}{dt} = 2x_2 + x_3 \\ \frac{dx_3}{dt} = 12x_1 - 13x_2 \\ \frac{dx_4}{dt} = 90x_1 - 95x_4 + 200y_4 \\ \frac{dx_5}{dt} = x_1 + 18x_2 - x_5 \\ \frac{dx_6}{dt} = 100x_2 + 4x_5 - 4x_6 \end{cases} \quad (9)$$

式中, $y_4 = \frac{|x_4 + 1| - |x_4 - 1|}{2}$.

格里波基利用 Lyapunov 指数判定混沌的存在性,证明只要有一个 Lyapunov 指数为正数,则可以说明该系统为混沌系统^[5].可计算 Lyapunov 指数法进行研究系统(8)的动力学行为,如图 2,得到的 6 个 Lyapunov 指数结果为: $\lambda_1 = 8.9017$; $\lambda_2 = -7.2989$; $\lambda_3 = -0.5895$; $\lambda_4 = -105.6794$; $\lambda_5 = -2.1141$; $\lambda_6 = -37.0429$. 计算采用四阶 Runge—Kutta 方法对式(9)进行求解,图 3 展示系统(8)的混沌吸引子图.

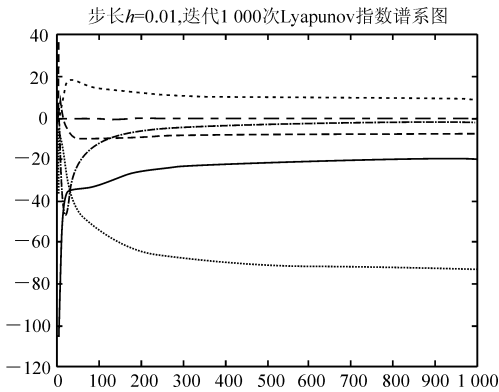


图 2 六阶 CNN 系统的 Lyapunov 指数图

3.2 一般三次映射的鲁棒混沌

Li-Yorke 混沌定义: 存在一个连续自映射 $f(x)$ 在区间 I 上满足 ① $f(x)$ 周期点的周期无上界; ② 闭区间 I 上存在不可数子集, 满足:

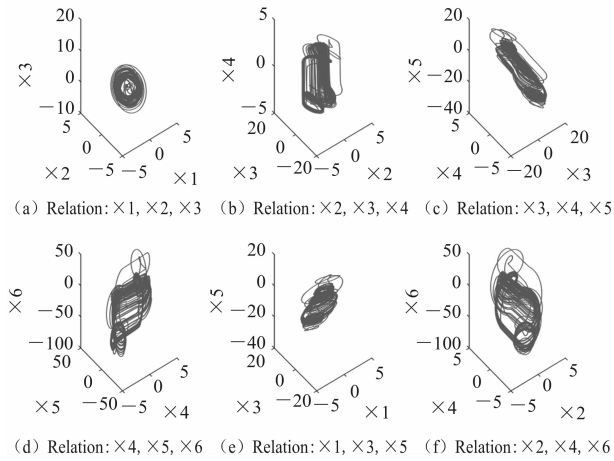


图 3 六阶 CNN 系统产生的混沌吸引子图

- (1) $\forall x, y \in S, x \neq y, \limsup |f''(x) - f''(y)| > 0$;
- (2) $\forall x, y \in S, \liminf |f'(x) - f'(y)| > 0$;
- $\forall x \in S$ 和 f 的任意周期点 y , 有 $\lim |f''(x) - f''(y)| > 0$, 则 $f(x)$ 具有混沌现象^[15].

定义 1: 映射 $\phi(x): J = [p, q] \rightarrow J$ 称为 S 单峰映射, 若满足以下条件:

- (1) 映射 $\phi(x)$ 具有连续的三阶导函数;
- (2) p 为不动点, 且存在原像 q , 即 $\phi(p) = \phi(q) = p$;
- (3) 映射 $\phi(x)$ 在区间 $[p, q]$ 上存在唯一的极大值点 m , 使得映射 $\phi(x)$ 在区间 $[p, m]$ 上严格增加, 在区间 $(m, q]$ 上严格减小;

- (4) 映射 $\phi(x)$ 具有负的 Schwarzin 导数, 即

$$S(\phi, x) = \frac{\phi'''(x)}{\phi'(x)} - \frac{3(\phi''(x))^2}{2(\phi'(x))^2} < 0$$

基于 S 单峰映射的混沌定理如下.

定理 1: 若映射 $\phi_v(x): J = [p, q] \rightarrow J$ 是一个含有参数 v 的 S 单峰映射, 且在点 $m \in (p, q)$ 存在最大值, 使得对于任意的参数 $v \in (v_{\min}, v_{\max})$, $\phi_v(m) = q$, 则映射 $\phi_v(x)$ 对任意的参数 $v \in (v_{\min}, v_{\max})$ 是混沌的.

基于定义 1 和定理 1, 谢国芳对一般三次方程的求根公式做了大量工作, 给出了更为简明的三次方程求根公式, 并发表在数学学习与研究中^[14], 从而建立一般三次函数的鲁棒混沌定理如下.

定理 2: 设三次函数为:

$$\phi(x) = ax^3 + bx^2 + cx + d (a \neq 0) \quad (10)$$

设 $b^2 = uac, v \in (-\infty, 0) \cup (3, +\infty)$, 则 $\phi(x)$ 是混沌映射, 若参数集 $S = \{a, u, v, d, \theta\}$ 满足下列任一情况: (1) 若 $a > 0$

$$\left\{ \begin{array}{l} 1 - \frac{4 \left(1 - \frac{3}{v}\right)^{\frac{3}{2}}}{\frac{9}{v} - 2 + 2 \left(1 - \frac{3}{v}\right)^{\frac{3}{2}}} \leq u \leq 1 \\ b = \frac{18a \sqrt{1 - \frac{3}{v}} \left[\cos\left(\frac{\theta}{3} - \frac{2}{3}\pi\right) - \cos\left(\frac{\theta}{3} + \frac{2}{3}\pi\right) \right]}{\sqrt{2 - 2u + \left(3 - \frac{9}{v}\right)} \sqrt{1 - \frac{3}{v} + \frac{(9u-9)}{v}} + (2u-1) \left(1 - \frac{3}{v}\right)^{\frac{3}{2}}} \\ d = \frac{9ab(uc-1) + 18a \sqrt{b^2 - 3ac} \cos\left(\frac{\theta}{3} + \frac{2}{3}\pi\right) + 2u(b^2 - 3ac)^{\frac{3}{2}} - 2ub^3}{27a^3} \\ \theta = \cos^{-1} \left[\frac{9 - 2v - 9u + 2uv}{2v \left(1 - \frac{3}{v}\right)^{\frac{3}{2}}} - u \right] \end{array} \right. \quad (11)$$

$$\left\{ \begin{array}{l} 1 - \frac{4 \left(1 - \frac{3}{v}\right)^{\frac{3}{2}}}{\frac{9}{v} - 2 - 2 \left(1 - \frac{3}{v}\right)^{\frac{3}{2}}} \leq u \leq 1 \\ b = - \frac{18a \sqrt{1 - \frac{3}{v}} \left[\cos\left(\frac{\theta}{3} + \frac{2}{3}\pi\right) - \cos\left(\frac{\theta}{3} - \frac{2}{3}\pi\right) \right]}{\sqrt{2 - 2u + \left(3 - \frac{9}{v}\right)} \sqrt{1 - \frac{3}{v} + \frac{(9u-9)}{v}} - (2u-1) \left(1 - \frac{3}{v}\right)^{\frac{3}{2}}} \\ d = \frac{9ab(uc-1) + 18a \sqrt{b^2 - 3ac} \cos\left(\frac{\theta}{3} + \frac{2}{3}\pi\right) + 2u(b^2 - 3ac)^{\frac{3}{2}} - 2ub^3}{27a^3} \\ \theta = \cos^{-1} \left[\frac{9 - 2v - 9u + 2uv}{-2v \left(1 - \frac{3}{v}\right)^{\frac{3}{2}}} - u \right] \end{array} \right. \quad (12)$$

则 $\phi(x): J = [p, q] \rightarrow J$ 是一个单峰映射, 其

$$\begin{aligned} \text{中 } p &= \frac{-b + 2\sqrt{b^2 - 3ac} \cos\left(\frac{\theta}{3} + \frac{2}{3}\pi\right)}{3a}, \\ q &= \frac{-b + 2\sqrt{b^2 - 3ac} \cos\left(\frac{\theta}{3} - \frac{2}{3}\pi\right)}{3a}, \text{ 且存在点 } m \\ &= \frac{-b - \sqrt{b^2 - 3ac}}{3a} \in [p, q], \text{ 使得 } \phi(m) = q. \text{ 同理, 若 } a < 0 \text{ 时也可证明.} \end{aligned}$$

基于一般形式的三次混沌映射(定理 2), 若参数满足任意情况, 检验其生成序列是否具有混沌特性, 在本文中只验证 $v > 0$ 的情况. 图 4 分别为 $x = -0.6$ 时的序列图与混沌映射迭代产生的散点图, 可以直观表明序列分布情况. 判断映射是否具有混沌特性, 计算 Lyapunov 指数值是方法之一, 保证计算的结果有一个 Lyapunov 指数大于零, 则能够说明此系统是混沌系统. 故而解得 Lyapunov 指数值为 1.723 4.

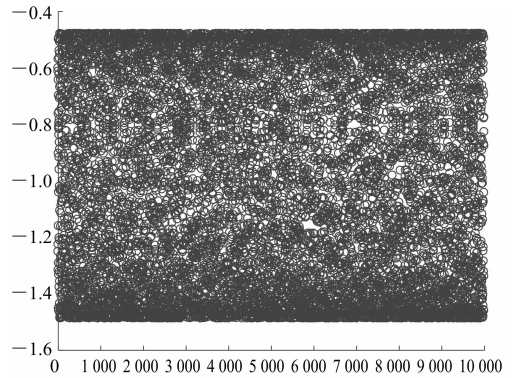


图 4 一般形式的三次鲁棒映射序列图和散点图

3.3 基于混沌系统的加密操作

采用本文加密算法, 得到的加密效果如图 5 所示. 图中 [2, 2, 1] 为明文图像, [2, 2, 2] 为由高维 Lorenz 产生的密码 X 对明文图像前向扩散处理得到的密文 image1, [2, 2, 3] 为一般形式的三次函数鲁棒映射产生的密码 Y 加密得到的密文 image2, [2, 2, 4] 为为由高维 Lorenz 产生的密码 Z 加密图像经过后向扩散处理得到的密文 image3., 即最终加

密效果图。



图5 本文算法的加密效果图

4 安全性分析

4.1 直方图分析

直方图分析从人类视觉的角度出发更为直观简洁,该分析描述的是像素密度分布色彩强度水平的关系,针对加密信息来说,如果密文信息的分布越不均匀,将很容易被密文攻击破解;直方图分析能够很好的表现这一特性.从图6可直观知,原始图像像素灰度值分布非常不均匀,即灰度值出现的概率有显著差异,经过加密处理后,得到了较为平滑的均匀分布,密文图像的直方图变得很均匀具有良好的统计特性,频数的波动程度小,并且也积大的改善了分布均匀的效果,同时提升了破译的广度及难度,能够有效抵抗统计性攻击.

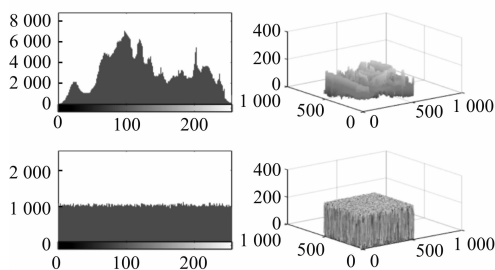


图6 明文和密文直方图

4.2 密钥空间分析

在本文算法方案中,密钥设置是双精度运算,选取高维双混沌映射的初值和参数作为初始条件的密钥,参数选择能够达到 10^{308} ,因而,该加密算法的密钥空间足够大.

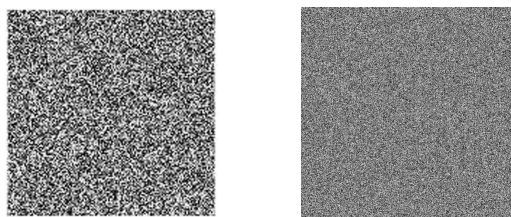
4.3 NPCR 和 UACI 分析

计算 NPCR 与 UACI 指标如下所示,所得结果越接近于理想值越好.

$$\text{NPCR}(P_1, P_2) = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N |\text{Sign}(P_1(i, j) - P_2(i, j))| \times 100\% \quad (13)$$

$$\text{UACI}(P_1, P_2) = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N \frac{|P_1(i, j) - P_2(i, j)|}{255} \times 100\% \quad (14)$$

在计算机仿真中,将明文图像 Lena 的(1,1)位置的像素原始灰度值改变为 $\text{mod}(p(1, 1) + 1, 256)$,得到的加密效果如图7所示.根据式(13~14)计算出的 NPCR 值和 UACI 值分别是0.996 4和0.333 6十分接近于理想值.



(a) 密文

(b) 改变明文像素后的密文

图7 敏感性对比

4.4 加密图像信息熵分析

信息熵也是衡量图像灰度值的分布状态的指标之一,图像灰度值的分布越均匀的,信息熵越大,信息熵的计算公式如下所示,

$$H(m) = - \sum_{i=0}^{255} p(m_i) \log_2 p(m_i) \quad (15)$$

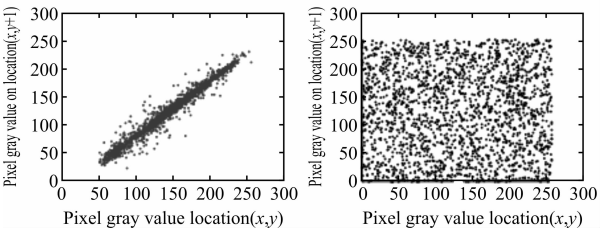
式中, $p(m_i)$ 是灰度值为 m_i 出现的概率,那么就有 $\sum_{i=0}^{255} p(m_i) = 1$,信息熵值越接近于8,说明密文的攻击性越好,抗统计攻击性越好.本文的加密算法实现信息熵是 $H = 7.999 4$,明文图像信息熵是 $H = 7.431 0$,直观地发现加密后的图像信息熵十分接近理论值8,抗统计攻击性很好.

4.5 相关性分析

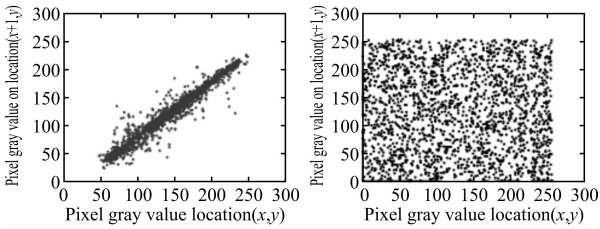
本文则分别随机选取2 000对明文与密文中相邻的像素点通过式(15)~(16),计算明文图像与密文图像不同方向的相邻像相关系数进行对比分析,并与文献[12, 15]进行比较.分析结果如表1、图8所示.从图8中可知,本文选取的明文图像相邻像素间具有很强的线性关系,且由表1可知,明文关系系数图中像素点之间的分布斜率趋近于1.而密文图像的相邻像素分布十分均匀、无序、分散,且像素值之间的分布斜率值极小,趋近于0,并且与文献[12, 14]相比较本文算法的相关系数值 ρ_{xy} 更小,说明达到更好的加密效果.

$$\rho_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)} \cdot \sqrt{D(y)}} \quad (16)$$

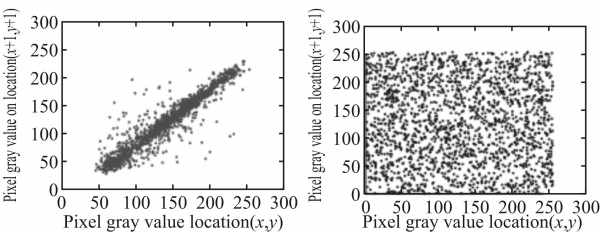
$$\begin{cases} E(x) = \frac{1}{N} \sum_{i=1}^N (x_i - \bar{x}) \\ \text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - \bar{x})(y_i - \bar{y}) \\ \bar{x} = \frac{1}{N} \sum_{i=1}^N x_i \end{cases} \quad (17)$$



(a) 明文水平方向散点图



(b) 明文垂直方向散点图



(c) 明文对角方向的散点图

图 8 明文与密文的相邻像素相关性散点图

表 1 相关系数

方向	明文	加密	文献[12]	文献[15]
水平方向	0.987 5	-0.013 8	-0.023 5	0.029 8
垂直方向	0.970 5	0.000 1	0.058 2	-0.002 1
对角方向	0.958 6	-0.007 2	0.008 7	0.017 6

本文设计的加密方案计算机仿真试验环境是在 Windows10 系统下,使用软件 Matlab2017a 仿真.在以往的单一置乱与扩散结合的框架下建立双扩散、置乱的加密模型,使得加密效果更优良,加密过程更加严谨高效.通过算法加密得到密文信息熵值 7.999 4,十分靠近理论值 8,说明信息的不确定性极好,加密效果趋近理想预期.本文加密方案的完整性更优良,提高了安全

性与鲁棒性且本文算法密钥空间足够大,数字图像冗余度降低,敏感性强,传输安全问题得到可靠保障.综上所述,本文算法方案具有优良的加密效果,还具有抗攻击性能.但仍可以考虑在加密方案中继续改进,进一步提高算法加密效率^[16-18].

5 结束语

本文提出一种以六阶 CNN 细胞神经网络产生的序列作为高维混沌系统的密钥源为基础^[17],不失一般性的同时,使得随着密钥源的选则不同获得不同的加密密码,对图像加密来说具有更良好的安全性和抗攻击性,并且高效利用了超混沌系统的良好特性.

参考文献:

[1] 蒲力. 数字签名在网上成绩管理系统中的应用研究[D]. 贵州:贵州大学,2009.

[2] 赵辽英,厉小润,赵光宙. 用细胞神经网络超混沌同步系统实现保密通信[J]. 电路与系统学报,2003(3): 41-45.

[3] 马凌,侯小毛,张福泉,等. 基于复合混沌系统与人工神经网络学习的图像加密算法[J]. 电子测量与仪器学报,2018,32(8):109-116.

[4] 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,2017,36(2): 60-66.

[5] 武凯,赵国敏,李国东. 基于多维混沌系统的图像加密技术研究[J]. 淮阴师范学院学报(自然科学版),2015, 14(1):33-38.

[6] 刘玉明,周冬明,赵东风. 基于细胞神经网络超混沌特性的图像加密[J]. 云南大学学报(自然科学版),2007 (4):355-358.

[7] 朱艳平,张小红. 基于细胞神经网络的图像加密新算法[J]. 江西理工大学学报,2008(1):27-30.

[8] ZHANG Yong. A Chaotic System Based Image Encryption Scheme with Identical Encryption and Decryption Algorithm[J]. Chinese Journal of Electronics, 2017,26(5):1022-1031.

[9] 徐扬,黄迎久,李海荣. 基于一种广义 Lorenz-Stenflo 超混沌系统的数字图像加密算法的性能研究[J]. 内蒙古科技大学学报,2017,36(3):267-272.

[10] 谈鑫杰,李丽洁,覃凤梅,等. 一类四维超混沌 Lorenz 型系统的动力学行为[J]. 科技风,2019(6):25-27.

[11] 蒲越,李国东,赵静. 基于细胞神经网络混沌特性的音频加密技术应用[J]. 云南大学学报(自然科学版), 2017,39(4):539-546.

5 结束语

本文在现有的基于 RMT 的感知算法基础上,改进了基于最大特征值的感知算法,通过增加辅助信号,另最大特征值右移出 M-P 律的特征值上边界,使目标信号和噪声的特征值更容易分辨,进而提高了低信噪比环境下的检测性能.通过理论分析和仿真验证可以看出,在低信噪比瑞利衰落环境下,本文所改进的算法相较于现有的基于 RMT 的感知算法有更好的感知性能,并且在认知用户数或者采样点有限的情况下依旧有较好的感知性能.因此在多用户瑞利信道环境下,本文算法有实际应用的价值.

参考文献:

[1] MITOLA J, MAGUIRE G Q. Cognitive radio: making software radios more personal[J]. IEEE Personal Communications, 1999, 6(4):13-18.

[2] URKOWITZ H. Energy detection of unknown deterministic signals[J]. Proceedings of the IEEE, 1967, 55(4):523-531.

[3] HO K C, W. PROKOPIW Y T. CHAN. Modulation identification of digital signals by the wavelet transform[J]. IEEE Proceedings-Radar, Sonar and Navigation, 2000, 147(4):169-170.

[4] 赵树杰, 赵建勋. 信号检测与估计理论[M]. 北京:电子工业出版社, 2013.

[5] CARDOSO L S, DEBBAH M, BIANCHI P, et al. Cooperative spectrum sensing using random matrix theory[C]// 2008 3rd International Symposium on

Wireless Pervasive Computing. Santorini, Greece , IEEE, 2008: 334-338.

[6] ZENG Y, LIANG Y C. Eigenvalue-based spectrum sensing algorithms for cognitive radio [J]. IEEE Transactions on Communications, 2009, 57 (6): 1784-1793.

[7] ZENG Y, LIANG Y. Maximum-Minimum Eigenvalue Detection for Cognitive Radio[C]// IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications. Athens, 2007:1-5.

[8] 王磊, 郑宝玉, 李雷. 基于随机矩阵理论的协作频谱感知[J]. 电子与信息学报, 2009, 31(8):1925-1929.

[9] EDELMAN A, WANG Y, EDELMAN A, et al. Random matrix theory and its innovative applications [C]// Advances in Applied Mathematics, Modeling, and Computational Science. Springer US, 2013: 91-116.

[10] CHIANI M. Distribution of the largest eigenvalue for real Wishart and Gaussian random matrices and a simple approximation for the Tracy-Widom distribution [J]. Journal of Multivariate Analysis, 2012(129): 69-81.

作者简介:

冯一舟 男,(1993-),硕士.研究方向为认知无线电及随机矩阵理论. E-mail:fengshen_009@163.com.

郑霖 男,(1975-),博士,教授.研究方向为随机矩阵和雷达通信一体化.

张文辉 女,(1970-),博士,教授.研究方向为计算机图形学和随机矩阵理论.

(上接第 48 页)

[12] 任晓霞. 细胞神经网络在数字图像加密方面的应用研究[D]. 重庆:重庆大学,2012.

[13] CHUA L O, YANG L. Cellular neural network: Theory[J]. IEEE Transactions on Circuit and System, 1998, 35(10):1257-1272.

[14] JUI-CHENG YEN, JIUN-IN GUO. A new image encryption algorithm and its VLST architecture[J]. the IEEE Workshop on Signal Processing Systems, 1999: 430-437. DOI:10.1109/SIPS.1999.822348.

[15] 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),2015,28(1):141-145.

[16] 赵国敏,李国东. 基于细胞神经网络混沌特性的图像加

密技术应用研究[J]. 绵阳师范学院学报,2014,33(2): 92-97.

[17] 汪乐乐,李国东. 最优解与二维离散分数阶 Fourier 的双混沌加密算法[J]. 中国科技论文,2018,13(17): 2024-2031.

[18] 张勇. 混沌数字图像加密[M]. 北京:清华大学出版社,2016.

作者简介:

魏慧 女,(1996-),硕士研究生.研究方向为数据挖掘与图像处理.

李国东(通讯作者) 男,(1972-),博士,教授,硕士生导师.研究方向为数据挖掘与图像处理. E-mail:lgdzhzy@126.com.