一种基于 TLM 超混沌细胞神经网络图像加密新算法

底晓强,母一宁,李锦青,杨华民

(长春理工大学 计算机科学与技术学院, 吉林 长春 130022)

摘 要:混沌对初值敏感的特性使得它适合于数据加密。以 4 阶 CNN 模型为基础,提出了一种新的超混沌细胞神经网络图像加密算法。算法分为置乱和扩散二个阶段,复合混沌映射用于生成置乱阶段控制参数,用以置乱图像行列之间的高度互相关像素。在扩散阶段,使用不同初始状态和参数的复合混沌映射生成高阶混沌细胞神经网络的初始条件,以生成扩散阶段的密钥流。算法的已知明文和选择明文攻击、密钥空间和直方图的仿真实验均取得了良好的结果。与其他相关算法相比,该算法具有密钥敏感性和抗攻击性强的优点,适用于图像加密。

关键词:超混沌; 细胞神经网络; 复合混沌映射; 图像加密

中图分类号:TP301 **文献标志码**:A **文章编号**:1007-2276(2014)12-4170-07

Novel image encryption algorithm based TLM hyperchaotic cellular neural network

Di Xiaoqiang, Mu Yining, Li Jinqing, Yang Huamin

(School of Computer Science and Technology, Changchun University of Science and Technology, Changchun 130022, China)

Abstract: Since chaos is sensitive for initial values, it is very suitable for data encryption. An image encryption algorithm based on hyper-chaotic control parameters and mixed scrambling diffusion structure of higher-order chaotic system was presented. The encryption algorithm included scrambling step and diffusion step. In the scrambling step, the composite chaotic map was used to generate the alignment phase control parameters and scramble for the high-level image cross-correlation between the adjacent pixels. In the diffusion step, the composite chaotic map with the different initial states and parameters was used to generate the initial conditions for hyper-chaotic cellular neural networks in order to generate the key stream. This method was evaluated by known plaintext attack and chosen plaintext attack, key space, image histogram, and simulations show good results. Compared with several other related algorithms, it has better anti-aggressive and key sensitivity is high. It can be applied to the image encryption.

Key words: hyper-chaos; cellular neural network; composited chaotic mapping; image encryption

收稿日期:2014-04-10; **修订日期**:2014-05-17

基金项目:吉林省科技厅发展计划项目(20140101206JC-08)

作者简介:底晓强(1978-),男,博士生,主要从事网络与信息安全方面的研究。Email: dixiaoqiang@cust.edu.cn

通讯简介:杨华民(1963-),男,教授,博士生导师,主要从事虚拟现实与数字媒体图像处理方面的研究。Email: yhm@cust.edu.cn

0 引 言

近年来，图像加密受到了国内外研究者的广泛关注,最常见的图像加密机制为置乱—扩散机制,一般分为扩散和置乱两个阶段。置乱阶段是用于掩盖明文、密文和密钥之间的关系,使得密钥和密文之间的统计关系尽可能复杂，使密码攻击者无法从密文推理得到密钥；扩散阶段是将明文冗余度分散到密文中使之分散开来,以便隐藏明文的统计结构,实现方式是使明文的每一位影响密文中多位的值。这个置乱—扩散过程要循环一定次数，以确保达到相应的加密效果。

混沌的内在随机性和对初值的敏感性，使得它非常适合于应用在密码学中[1]。神经网络的高度非线性特征也被广泛应用于数据的加密。而细胞神经网络(CNN)兼具二者的特性,具有更为复杂的时空复杂度,因此将 CNN 应用于加密的研究吸引了很多学者的关注[2-10]。Li[4]对一种 CNN 模型的混沌现象进行了分析,文中以该模型为基础,将其非线性动力学特性应用在图像加密的扩散阶段。Gao[5]根据参考文献[4]给出的混沌神经网络模型提出了一种图像识别算法,对参考文献[4]中的模型在图像识别中的应用进行了研究。在参考文献[6]中,以 Hopfield 混沌神经网络为基础设计了一种彩色图像加密算法,但后来的研究中发现，所使用的混沌并不是超混沌系统,其非线性特性不如参考文献[4]中的模型理想。参考文献[7]以 6 阶 CNN 为基础提出了一种彩色图像加密算法，但是由于 6 阶混沌系统计算更为复杂，导致加密解密运行速度较低。文中以 4 阶 CNN 模型为基础,提出了一种新的超混沌细胞神经网络(HCNN)图像加密算法。

该算法首先使用混沌复合映射控制参数进行图像置乱;然后使用 HCNN[4]预处理图像,通过像素和像素之间的预扩散机制加密图像。算法的密钥包括 6 个参数,分别是:复合混沌映射的 2 个初始条件、2 个控制参数、复合混沌映射的迭代次数和循环次数。仿真实验表明算法的密钥十分敏感,和密钥中任何一个参数 10^{-14} 的不匹配都无法正确解密图像;统计分析结果表明该算法可以抵抗各种常见的攻击。

1 复合混沌映射与细胞神经网络模型

1.1 复合混沌映射

标准帐篷映射的方程为[11]:

$$x_{n+1}=\begin{cases}2x_n, & 0<x_n<0.5\\ 2(1-x_n), & 0.5\leqslant x_n<1\end{cases} \tag{1}$$

Logistic 映射的方程为[11]:

$$x_{n+1}=\lambda x_n(1-x_n)\quad \lambda\in(0,4),x\in(0,1) \tag{2}$$

对于 Logistic 映射,当 $\lambda=4$ 时,处于混沌区,并且为(0,1)上的满映射。因此取值 $\lambda=4$ 时,公式(2)变为:

$$x_{n+1}=4x_n(1-x_n)\qquad x\in(0,1) \tag{3}$$

帐篷映射 x_n 的值一直处于(0,1)上,即无论对公式(1)怎样取值,其值域都不会超出公式(3)的定义域范围,因此,将公式(1)代入到公式(3)中,便可以得到一个新的复合混沌映射,将其简称为 TLM[11]:

$$x_{n+1}=\begin{cases}4\mu x_n(1-\mu x_n) & 0<x_n<0.5\\ 4\mu(1-x_n)(1-\mu(1-x_n)) & 0.5\leqslant x_n<1\end{cases} \tag{4}$$

式中：$\mu\in(0,2)$;$x_n\in(0,1)$。

1.2 高阶混沌细胞神经网络模型

定义高阶混沌行为的一种典型方式为有两个或两个以上正的 Lyapunov 指数。文中使用的高阶混沌系统为高阶细胞神经网络(HCNN),参考文献[4]描述其模型如下:

$$\dot{X}=-CX+Wf(x) \tag{5}$$

式中：$X=[x_1,x_2,x_3,x_4]^T$;$C=\mathrm{diag}([1,1,1,100])$;

$$W=\begin{pmatrix}2.1 & 2.5 & 0 & 0\\ -2.6 & 1 & 3 & 0\\ 0 & -2.8 & p & -1.1\\ 0 & 0 & 100 & 160\end{pmatrix};$$

$$f(x)=\frac{1}{2}(|x+1|-|x-1|);$$

公式(5)可写为:

$$\begin{aligned}x'&=-x_1+2.1f(x_1)+2.5f(x_2)\\ x'_2&=-x_2-2.6f(x_1)+f(x_2)+3f(x_3)\\ x'_3&=-x_3-2.8f(x_2)+pf(x_3)-1.1f(x_4)\\ x'_4&=-100x_4+100f(x_3)+160f(x_4)\end{aligned} \tag{6}$$

当参数 **p** 在(0.27,0.67)之间时,公式(5)所示细胞神经网络模型存在两个正的 Lyapunov 指数。当 **p**=0.4 时,4 个 Lyapunov 指数分别为 λ_1=0.125,λ_2=0.022,λ_3= 0,λ_4 =95.95,说明该模型为高阶混沌系统。其混沌吸引子分布如图 1 所示。

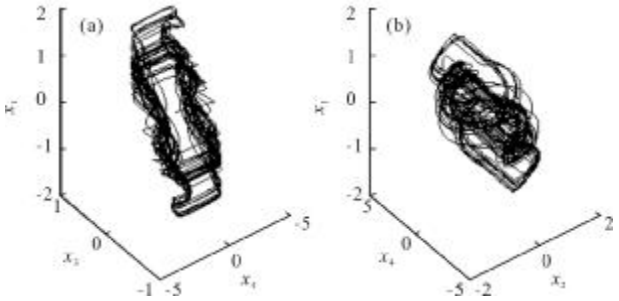


图 1 混沌吸引子分布图(**p**=0.4)

Fig.1 Chaotic attractor distribution (**p**=0.4)

2 图像加密解密算法

2.1 加密算法

文中所提出的加密算法包括置乱和扩散两个阶段。其中,置乱阶段使用 Cat 映射的混沌控制参数,令第 1 个 TML 映射的参数和初始条件分别为 $\mathbf{m}_{TL_1}$ 和 $\mathbf{X}_{TL_1}(0)$,其迭代 **M** 次生成 Cat 映射的控制参数,其中迭代次数 **M** 也是本算法中 6 个密钥之一。

在扩散阶段,高阶 **CNN** 输出 4 个序列信号用于改变像素的值(图像均衡化),完成图像洗牌。令第 2 个 TML 映射的参数和初始条件为 $\mathbf{X}_{TL_2}(0)$和 $\mathbf{m}_{TL_2}$,该 TML 映射也迭代 **M** 次,生成高阶 CNN 的初始参数。该置乱-扩散过程循环 **R** 次完成图像的加密。加密算法流程图如图 2 所示。

令原始图像 **D** 为 **N**×**N** 像素。6 个密钥分别为:$\mathbf{X}_{TL_1}(0)$、$\mathbf{m}_{TL_1}$、$\mathbf{X}_{TL_2}(0)$、$\mathbf{m}_{TL_2}$、**M** 和 **R**,初始时循环计数器 r=1。

当初始条件分别为 $\mathbf{X}_{TL_1}(0)$和 $\mathbf{X}_{TL_2}(0)$,迭代第 1 和第 2 TLM 映射 **M** 次,得到 $\mathbf{X}_{TL_1}(r)$和 $\mathbf{X}_{TL_2}(r)$。分别用于置乱阶段和扩散阶段。

置乱阶段使用可变参数 Cat 映射,Cat 映射的方程定义为:

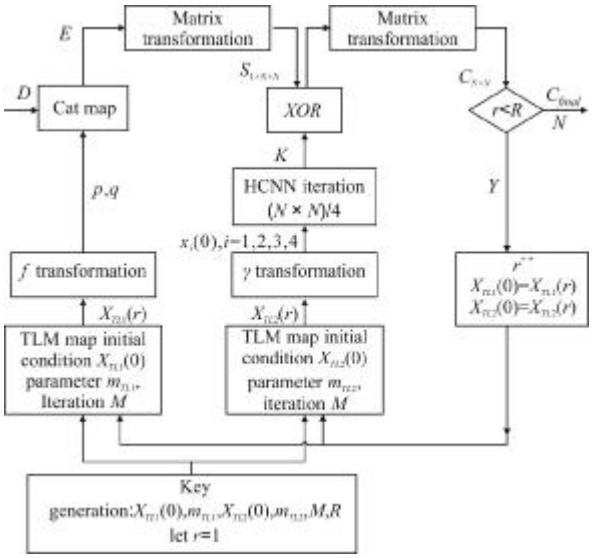


图 2 加密流程图

Fig.2 Encryption flowchart

$$\begin{pmatrix} x_n+1 \\ y_n+1 \end{pmatrix} = \mathbf{A}\begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod(\mathbf{N}) = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}\begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod(\mathbf{N}) \quad (7)$$

由于 det(**A**)=1,控制参数 **p**,**q** 如下式描述:

$$\begin{cases} p=f_1(\mathbf{X}_{TL1}(r)) \\ q=f_1(\mathbf{X}_{TL1}(r)) \end{cases} \quad (8)$$

式中:$f_1(x)=\mathbf{floor}[\mathbf{mod}(x\times 2^{24},\mathbf{N})]$,$f_2(x)=\mathbf{floor}[\mathbf{mod}(x\times 2^{48},2^{24},\mathbf{N})]$使用 **p** 和 **q**,根据公式(7)排列图像,将原始图像 **D** 转化为置乱图像 **E**。

置乱图像 **E** 的像素按照从左到右从上到下的顺序得到序列 $S=\{\mathbf{S}_1,\mathbf{S}_2,\cdots,\mathbf{S}_{N\times N}\}$。S 为 1×(**N**×**N**)的列矩阵。

在扩散阶段,使用公式(6)描述的高阶混沌系统。使用 $\mathbf{X}_{TL_2}(r)$,用公式(9)生成高阶混沌系统的初始条件:

$$x_i(0)=\gamma_i\mathbf{X}_{TL_2}(r) \quad (9)$$

式中:参数 γ_i(i=1,2)为某恰当整数。由于 $\mathbf{X}_{TL_2}(r)$由混沌逻辑映射获取,所以,公式(9)所示初始值仍为混沌值。

通过迭代(**N**×**N**)/4 次公式(6)的高阶混沌系统,实现图像均衡化。当第(i=1,2,…,(**N**×**N**))次迭代细胞神经网络时,产生的 4 个值$\{x_1(i),x_2(i),x_3(i),x_4(i)\}$用于生成密钥流$\{\cdots,\mathbf{K}_{x_1(i)},\mathbf{K}_{x_2(i)},\mathbf{K}_{x_3(i)},\mathbf{K}_{x_4(i)},\cdots\}$,i=1,…,(**N**×**N**)/4 通过公式(10)求取:

$$\begin{cases} \mathbf{K}_{x_1(i)}=\mathbf{mod}\left(\mathbf{round}\left(\left(\mathbf{abs}(x_1(i))-\mathbf{floor}(\mathbf{abs}(x_1(i)))\right)\times 10^4+\mathbf{S}_{4(i-1)}\right),256\right) \\ \mathbf{K}_{x_2(i)}=\mathbf{mod}\left(\mathbf{round}\left(\left(\mathbf{abs}(x_2(i))-\mathbf{floor}(\mathbf{abs}(x_2(i)))\right)\times 10^4+\mathbf{S}_{4(i-1)+1}\right),256\right) \\ \mathbf{K}_{x_3(i)}=\mathbf{mod}\left(\mathbf{round}\left(\left(\mathbf{abs}(x_3(i))-\mathbf{floor}(\mathbf{abs}(x_3(i)))\right)\times 10^4+\mathbf{S}_{4(i-1)+2}\right),256\right) \\ \mathbf{K}_{x_4(i)}=\mathbf{mod}\left(\mathbf{round}\left(\left(\mathbf{abs}(x_4(i))-\mathbf{floor}(\mathbf{abs}(x_4(i)))\right)\times 10^4+\mathbf{S}_{4(i-1)+3}\right),256\right) \end{cases} \tag{10}$$

令 S 序列初值 $\mathbf{S}_0=127$。

序列 S 通过式(10)密钥流 **K** 进行加密,得:

$$\begin{cases} \mathbf{C}_{4(i-1)+1}=\mathbf{bitxor}(\mathbf{S}_{4(i-1)+1},\mathbf{K}_{x_1(i)}) \\ \mathbf{C}_{4(i-1)+2}=\mathbf{bitxor}(\mathbf{S}_{4(i-1)+2},\mathbf{K}_{x_2(i)}) \\ \mathbf{C}_{4(i-1)+3}=\mathbf{bitxor}(\mathbf{S}_{4(i-1)+31},\mathbf{K}_{x_3(i)}) \\ \mathbf{C}_{4i}=\mathbf{bitxor}(\mathbf{S}_{4i},\mathbf{K}_{x_4(i)}) \end{cases} \tag{11}$$

式中:**bitxor**(x,y)为返回两个整数 x 和 y 的位异或值,i=1,2,…,(**N**×**N**)/4,表示的是高阶混沌系统迭代次,数。高阶混沌系统迭代(**N**×**N**)/4 次,直到矩阵 S=$\mathbf{S}_1,\mathbf{S}_2,\cdots,\mathbf{S}_{N\times N}$ 中的所有元素都被加密,加密结果表示为集合 $\mathbf{C}=\mathbf{C}_1,\mathbf{C}_2,\cdots,\mathbf{C}_{N\times N}$。集合 $\mathbf{C}=\mathbf{C}_1,\mathbf{C}_2,\cdots,\mathbf{C}_{N\times N}$ 中的所有元素构成一个 $1\times\mathbf{C}_{N\times N}$ 的行向量。转换为的矩阵以获得加密图像 **C**,若 r<**R**,则继续执行以上过程,若 r=**R**,则 **C** 为加密结果 $\mathbf{C}_{final}$。

2.2 解密算法

该算法为对称加密算法,因此解密是加密的逆过程。将加密时反转的扩散和置乱分别应用在加密图像 $\mathbf{C}_{final}$ 中既可完成解密。解密过程流程图如图 3 所示。

将加密图像($\mathbf{C}_{final}$)排列为序列 $\mathbf{C}=\mathbf{C}_1,\mathbf{C}_2,\cdots,\mathbf{C}_{N\times N}$。**C** 图像像素灰度值从左到右从上到下排列而成的 $1\times\mathbf{C}_{N\times N}$ 列矩阵。令 r=**R**。

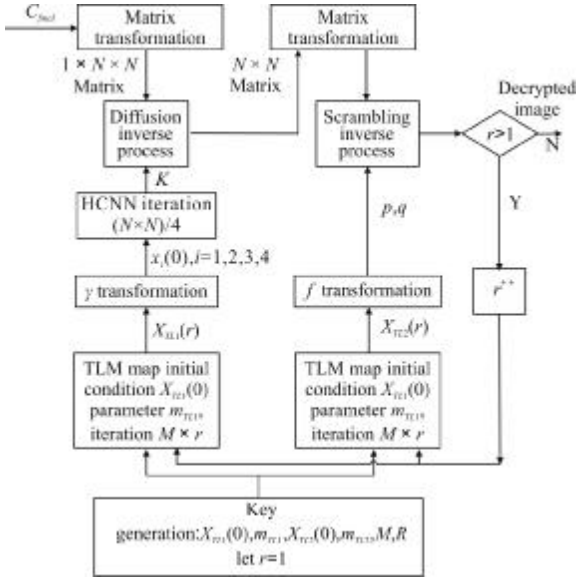


图 3 解密流程图

Fig.3 Decryption flowchart

两个 TLM 混沌映射函数的初始条件为 $\mathbf{X}_{TL_1}(0)$ 和 $\mathbf{X}_{TL_2}(0)$,参数分别为 $\mathbf{m}_{TL_1}$ 和 $\mathbf{m}_{TL_2}$。迭代每个复合混沌映射 **M**×r 次得到 $\mathbf{X}_{TL_1}(r)$和 $\mathbf{X}_{TL_2}(r)$。使用 $\mathbf{X}_{TL_2}(r)$根据公式(9)可以获取到高阶混沌系统的初始条件。以该条件迭代高阶混沌系统公式(6)i 次。

接下来,以下面方法反向执行第 r 轮加密的逆过程:

$$\begin{cases} \mathbf{K}_{x_1(i)}=\mathbf{mod}\left(\mathbf{round}\left(\left(\mathbf{abs}(x_1(i))-\mathbf{floor}(\mathbf{abs}(x_1(i)))\right)\times 10^{14}+\mathbf{S}_{4(i-1)}\right)\right) \\ \quad \mathbf{S}_{4(i-1)+1}=\mathbf{bitxor}(\mathbf{C}_{4(i-1)+1},\mathbf{K}_{x_1(i)}) \\ \mathbf{K}_{x_2(i)}=\mathbf{mod}\left(\mathbf{round}\left(\left(\mathbf{abs}(x_2(i))-\mathbf{floor}(\mathbf{abs}(x_2(i)))\right)\times 10^4+\mathbf{S}_{4(i-1)+1}\right)\right) \\ \quad \mathbf{S}_{4(i-1)+2}=\mathbf{bitxor}(\mathbf{C}_{4(i-1)+2},\mathbf{K}_{x_2(i)}) \\ \mathbf{K}_{x_3(i)}=\mathbf{mod}\left(\mathbf{round}\left(\left(\mathbf{abs}(x_3(i))-\mathbf{floor}(\mathbf{abs}(x_3(i)))\right)\times 10^4+\mathbf{S}_{4(i-1)+2}\right)\right) \\ \quad \mathbf{S}_{4(i-1)+3}=\mathbf{bitxor}(\mathbf{C}_{4(i-1)+3},\mathbf{K}_{x_3(i)}) \\ \mathbf{K}_{x_4(i)}=\mathbf{mod}\left(\mathbf{round}\left(\left(\mathbf{abs}(x_4(i))-\mathbf{floor}(\mathbf{abs}(x_4(i)))\right)\times 10^4+\mathbf{S}_{4(i-1)+3}\right)\right) \\ \quad \mathbf{S}_{4i}=\mathbf{bitxor}(\mathbf{C}_{4i},\mathbf{K}_{x_4(i)}) \end{cases} \tag{12}$$

令初始值 S_0=127。将 1×N×N 的单行矩阵 S 转换为 N×N 的矩阵形式。使用 $X_{TL1}(r)$和公式(8)计算 p 与 q 的值。执行公式(7)的排列逆过程。若 r>1,令 r=r-1,循环以上过程。否则,输出解密图像。

3 性能分析

一个良好的加密算法应具有密钥敏感性和鲁棒性。此节对所提出加密算法的性能进行分析,主要包括已知明文和选择明文攻击分析, 密钥空间及密文统计分析。实验结果表明,文中加密算法可以保护密钥和明文,能抵抗各种常见的攻击。

3.1 已知明文和选择明文攻击

已知明文攻击是攻击者有一些已知的 “明文密文对”样本用来破译密码。选择明文攻击是攻击者可以选择被加密的明文, 以并获得相应的密文用来破译密码。公式(7)所使用的密钥流$\{\cdots, K_{x_1(i)}, K_{x_2(i)}, K_{x_3(i)}, K_{x_4(i)}\}$不仅取决于加密密钥,而且还取决于明文,因此对于不同的明文,即使是相同密钥,算法的密钥流也是不相同的。由于置乱和扩散阶段的初始条件和控制参数都是与明文相关的,所以,这两种攻击对文中算法无效。

3.2 密钥空间

文中加密算法,共有 6 个值组成密钥,对于置乱和扩散这这 2 个阶段,每个阶段均使用 TLM 初始值和控制参数作为密钥。假设每一个密钥小于 10,精确度为 10^{-14}, 在不考虑循环次数 R 和 M 的情况下,密钥空间为 10^{56},大于建议的密钥空间 2^{64}[12],因此能够抵抗暴力破解攻击[13]。

3.3 统计分析

为验证加密算法的可行性, 使用 256×256 的“Lena”图像作为明文图像。加密密钥为:

$$X_{TL_1}(0)=0.618,\ m_{TL_1}=1.5,\ X_{TL_2}(0)=0.6,\ m_{TL_2}=1.7,\ M=200,\ R=3 \tag{13}$$

下面对加密解密图像的属性进行统计分析。

3.3.1 直方图分析

图像直方图所描述的是不同色彩在整幅图像中所占的比例。明文图像,密文图像和它们的直方图分别见图 4 和图 5。如图 4 和图 5 所示,明文图像的直方图可以看出各种灰度值所占的比例并不相同,而加密图像的直方图色彩强度分布均匀, 类似于白噪声, 因此不能从密文你图像中获得原始图像像素的相关信息。

图 4 256×256“Lena”图像加密解密对比

Fig.4 256 × 256 "Lena" image encryption and decryption contrast

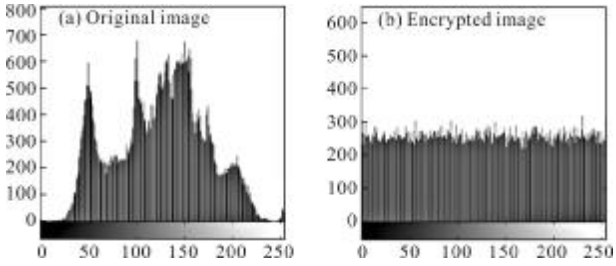


图 5 “Lena”原始图像,加密图像直方图

Fig.5 Original "Lena" image, and its encrypted image histogram

3.3.2 密钥敏感性

为了验证文中算法的密钥敏感性, 与公式(13)表示算法在相同条件下进行密钥敏感性实验。将密钥中的 4 个参数 $X_{TL_1}(0)$、$X_{TL_2}(0)$、m_{TL_1} 和 m_{TL_2}分别增加 10^{-14},其他参数不变,具体变化如下:

(1) $X_{TL_1}(0)=0.618+10^{-14}$, $m_{TL_1}=1.5$, $X_{TL_2}(0)=0.6$, $m_{TL_2}=1.7$, $M=200$, $R=3$

(2) $X_{TL_1}(0)=0.618$, $m_{TL_1}=1.5+10^{-14}$, $X_{TL_2}(0)=0.6$, $m_{TL_2}=1.7$, $M=200$, $R=3$

(3) $X_{TL_1}(0)=0.618$, $m_{TL_1}=1.5$, $X_{TL_2}(0)=0.6+10^{-14}$, $m_{TL_2}=1.7$, $M=200$, $R=3$

(4) $X_{TL_1}(0)=0.618$, $m_{TL_1}=1.5$, $X_{TL_2}(0)=0.6$, $m_{TL_2}=1.7+10^{-14}$, $M=200$, $R=3$

图 6 所示为 Lena 密文图像使用这四组密钥解密的结果, 可以发现根本无法恢复出明文图像,这也印证了混沌系统对初值非常敏感, 非常适合数据加密。

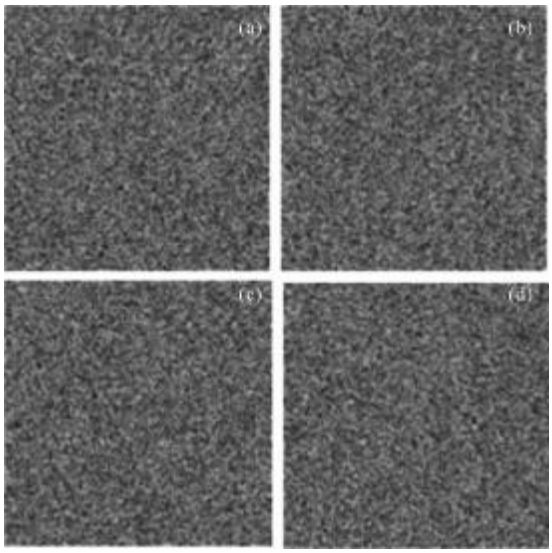


图 6 密钥的 4 种微小误差导致的错误解密结果

Fig.6 Error results of decryption key form four slight error

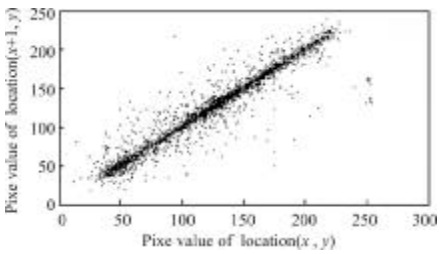
3.3.3 信息熵分析

信息熵描述了系统的不确定性。对于明文信息 m,信息熵 $H(m)$可通过下式计算:

$$H(m)=-\sum_{i=0}^{2^{N_m-1}} p(m_i)\log(p(m_i)) \qquad (14)$$

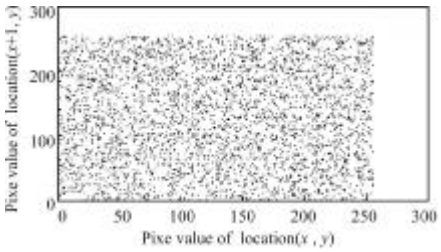
其中 $m_i,i=0,\cdots,2^{N_m-1}$为色彩强度值 (或灰度值)。对于一个随机过程,每个分量有相同的概率。例如,对于 $m=8$,每个符号(分量)$m=\{m_1,m_2,\cdots,m_{2^8}\}$具有相等的概率,这样分布结构的信息熵 $H(m)=8$。事实上,如果加密图像的信息熵分布不够单调,将可能被攻击者猜测到某些数值信息。因此,一个图像加密算法期望有一个更为平滑信息熵分布。

计算图 4 中“Lena”密文图像灰度值的信息熵为 $H(m)=7.9591$,用 AES 算法[14]加密图像的信息熵值为 $H(m)=7.91$。文中加密算法信息熵更接近于理想值 8。实验结果表明,密文图像接近于随机信号源,文中算法可以抵抗熵攻击。



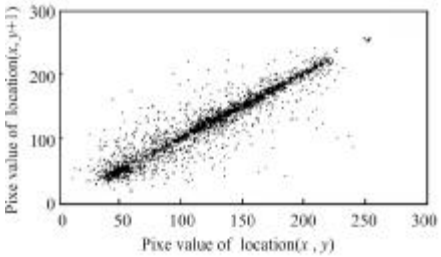
(a) 原始图像水平方向相邻像素

(a) Original image horizontally adjacent pixels



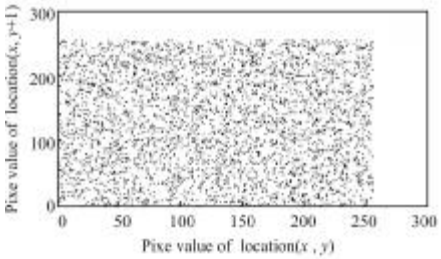
(b) 加密图像水平方向相邻像素

(b) Encrypted image horizontally adjacent pixels



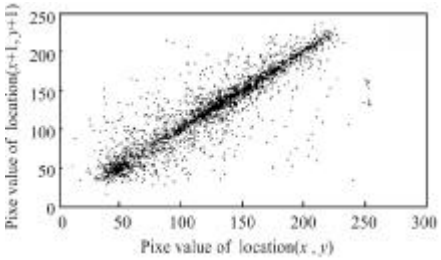
(c) 原始图像垂直方向相邻像素

(c) Vertically adjacent pixels of original image



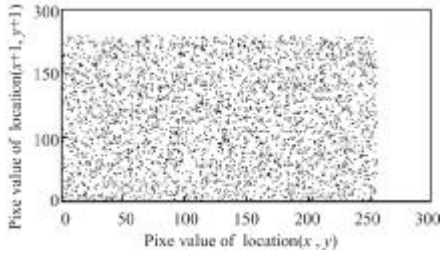
(d) 加密图像垂直方向相邻像素

(d) Encrypted image vertically adjacent pixels



(e) 原始图像对角方向相邻像素

(e) Original image adjacent pixels in a diagonal direction



(f) 加密图像对角方向相邻像素

(f) Encrypted image adjacent pixels in a diagonal direction

图 7 “Lena”图像的相关性

Fig.7 "Lena" image correlation

3.3.4 相关系数分析

密文图像像素之间相关性的大小是决定算法优劣的重要指标。相关系数 r_{xy} 是图像灰度值的一组相邻像素对 $(x_i, y_i), i=1,2,\cdots,N$，可以通过公式(15)计算。

$$e(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \qquad d(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-e(x))^2$$

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

$$r_{xy}=\frac{cov(x,y)}{\sqrt{d(x)}\sqrt{d(y)}} \tag{15}$$

图 7 所示为计算得到的“Lena”明文图像和密文图像的 4 000 对水平相邻像素、垂直相邻像素，以及对角相邻像素的相关性。明文图像的相邻像素相关性大于 0.9，而加密图像相邻像素之间的相关性在 0.01 左右。表 1 对比了 AES[15]算法、参考文献[13]、[14]算法和文中算法的相关系数值，由于在文中算法中应用了超混沌系统，其良好的非线性特征比其他算法更好地破坏了相邻像素之间的相关性，因此文中算好具有更好的加密性能。

表 1 相关系数对比

Tab.1 Correlation coefficient comparison

	Vertical	Horizontal	Diagonal
Original image	0.962 2	0.940 4	0.900 4
Ref.[12] algorithm	0.066	0.077	-
Ref.[13] algorithm	0.068 1	0.084 5	-
Ref.[14] algorithm	-0.031 8	0.096 5	0.036 2
Proposed algorithm "Lena"	-0.014 8	-0.003 7	0.023 5

4 结 论

文中提出了一种密钥敏感和具有鲁棒性的图像加密算法，由 2 个复合混沌映射和参数生成置乱和扩散阶段的控制参数。文中算法密钥空间达到 10^{56} 足以抵抗暴力破解攻击；通过实验验证，对密钥 10^{-14} 的微小变化也无法获得正确的明文，算法表现出优异的密钥敏感性；通过对相关系数、加密图像信息熵的计算及分析，表明文中算法具有出色的统计特性。

参考文献：

[1] Shannon C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 656-715.

[2] Yan Huang, Yang Xiaosong. Hyperchaos and bifurcation in a new class of four-dimensional Hopfield neural networks[J]. Neurocomputing, 2006, 69(13-15): 1787-1795.

[3] Fang Jingyue, Zhou Pu, Kang Qiang. Encrypting optical image based on compound encoding on space-fractional domain[J]. Infrared and Laser Engineering, 2005, 34(3): 345. (in Chinese)

[4] Li Qingdu, Yang Xiaosong, Yang Fangyan. Hyperchaos in a simple CNN [J]. International Journal of Bifurcation and Chaos, 2006, 16(8): 2453-2457.

[5] Gao Tiegang, Gu Qiaolun, Emmanuel Sabu. A novel image authentication scheme based on hyper-chaotic cell neural network[J]. Chaos, Solitons & Fractals, 2009, 42(1): 548-553.

[6] Li Jinqing, Bai Fengming, Di Xiaoqiang. Color image encryption algorithm based on hopfield chaotic neural networks [J]. Journal of Changchun University of Science and Technology, 2012, 35(4): 117-121. (in Chinese)

[7] Li Jinqin, Bai Fengming, Di Xiaoqiang. New color image encryption algorithm based on compound chaos mapping and hyperchaotic cellular neural network[J]. Journal of Electronic Imaging, 2013, 22(1): 013036-013036. (in Chinese)

[8] Liu Li, Zhou Yajian, Zhang Bin. Digital watermarking method for QR code images based on DCT and SVD [J]. Infrared and Laser Engineering, 2013, 42(z2): 304-311. (in Chinese)

[9] Bigdeli Nooshin, Farid Yousef, Afshar Karim. A robust hybrid method for image encryption based on Hopfield neural network [J]. Computers & Electrical Engineering, 2012, 38(2): 356-369.

[10] Ren Xiaoxia, Liao Xiaofeng, Xiong Yonghong. New image encryption algorithm based on cellular neural network [J]. Journal of Computer Applications, 2011, 31(6): 1528-1530.

[11] Bai Fengming. Opto-electronic hybrid system chaos control, synchronization and applied research[D]. Changchun: Changchun University of Science and Technology, 2003. (in Chinese)

[12] Lian S. A block cipher based on chaotic neural networks[J]. Neurocomputing, 2009, 72(4): 1296-1301.

[13] Liu Hongjun, Wang Xingyuan. Color image encryption based on one-time keys and robust chaotic maps[J]. Computers & Mathematics with Applications, 2010, 59(10): 3320-3327.

[14] Rhouma R, Meherzi S, Belghith S. OCML-based colour image encryption [J]. Chaos, Solitons & Fractals, 2009, 40(1): 309-318.

[15] Zeghid M, Machhout M, Khriji L, et al. A modified AES based algorithm for image encryption [J]. International Journal of Computer Science and Engineering, 2007, 1(1): 70-75.