DOI: 10.3979/j.issn.1673-825X.2020.06.017

基于二维耦合映像格子模型的图像压缩加密方案

刘　卓[1,2],王　永[2]
(1.贵州师范学院 数学与大数据学院,贵阳 550000;2.重庆邮电大学 计算机科学与技术学院,重庆 400065)

摘　要: 二维耦合映像格子(two-dimensional coupled map lattice,2D CML)模型具有很复杂的动力学行为,它的最大李雅普诺夫指数(maximum Lyapunov exponent,MLE)是由局部混沌映射函数决定。选择具有较大的李雅普诺夫指数(Lyapunov exponent,LE)的分段 logistic 函数(piecewise logistic map,PLM)作为模型的局部映射函数。通过独立性假设实验,验证 2D CML 模型在一定条件下拟服从独立同分布。在并行压缩感知条件下,基于 2D CML 模型产生压缩测量矩阵,使用测量矩阵对原始图像的每一列并行压缩采样。对采样图像进行处理和多轮扩散,实现对图像的加密,并对加密后的图像性能进行实验分析。实验表明,基于 2D CML 模型的图像压缩加密方案具有较好的加密性能和应用前景。

关键词: 2D CML 模型; 并行压缩感知; 独立性假设实验; 扩散
中图分类号: TP309.7　　**文献标志码:** A　　**文章编号:** 1673-825X(2020)06-1048-10

Image compression and encryption scheme based on the two-dimensional coupled map lattice model

LIU Zhuo[1,2], WANG Yong[2]
(1.School of Mathematics and Big Data, Guizhou Education University, Guiyang 550000, P. R. China;
2.College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, P. R. China)

Abstract: Two-dimensional coupled map lattice (2D CML) model has quite complex dynamic behavior. Its maximum Lyapunov exponent (MLE) is only determined by the local chaotic map. Therefore, a piecewise logistic map (PLM) with much larger Lyapunov exponent (LE) value is selected as the local mapping function of the 2D CML model. According to the independence hypothesis experiment, it is proved that the 2D CML model is intended to obey independent and identical distribution under certain conditions. With the parallel compressed sensing, a compressed sensing measurement matrix is generated by the 2D CML model, and the original image is sampled by compressed sensing measurement matrix. The image is encrypted by processing and multi-round diffusion of the sampled image, and the performance of the encrypted image is analyzed experimentally. Experiments show that the image compression encryption scheme based on 2D CML model has good encryption performance and application prospects.

Keywords: 2D CML model; parallel compression sensing; independence hypothesis experiment; diffuse

收稿日期: 2020-05-08　**修订日期:** 2020-10-13　**通讯作者:** 王　永　wangyong1@cqupt.edu.cn
基金项目: 国家自然科学基金(61876200);贵州省教育厅青年科技人才成长项目(黔教合 KY 字[2017]210,黔教合 KY 字[2018]260);贵州省科学技术基金计划(黔科合基础[2020]1Y422,黔科合基础[2019]1249,黔科合基础[2019]1425)
Foundation Items: The National Natural Science Foundation of China (61876200); The Guizhou Education Department Youth Science and Technology Talent Growth Project (QianJiaoHe-KY-Zi [2017] 210, QianJiaoHe-KY-Zi [2018] 260); The Science and Technology Foundation Project of Guizhou Province (QianKeHeJiChu [2020] 1Y422, QianKeHeJiChu [2019] 1249, QianKeHeJiChu [2019] 1425)

0 引　言

近年来，随着国家“互联网+”、“区块链+”发展战略的执行，各种信息技术得到了迅速发展与普及。移动支付、智能家居、智能手机、网络视频平台、微博微信等社交平台已经深入人们生活中，人们进入大数据时代。大数据的快速健康发展离不开数据的安全，数字图像是数据的一个极其重要的组成部分，也是多媒体信息技术的基础。多媒体图像被广泛应用于军事、经济、医学等领域，成为信息安全领域的重要研究问题。将新的技术手段引入传统密码学算法中，设计更加安全高效的信息安全保护方案成为了当前的研究热点。混沌理论是当今密码学重要的研究课题之一。它在气象、地震灾害预告和经济发展预测等领域有广泛的应用[1-3]。混沌是非线性动力系统中出现的一种确定的、貌似无规则的类随机现象。它具有初值敏感性和高度的伪随机性特性，这些特性与加密算法非常类似[3-4]。这些相似性启发研究者将混沌应用于信息安全领域，使混沌密码成为了非线性科学与信息科学交叉研究的热点问题。

耦合映像格子模型(coupled map lattice，CML) 是一种复杂的时空混沌模型。它是由简单混沌映射构成的在空间和时间上的多维扩散系统，不仅对初始条件和边界条件敏感，而且具有更好的不可预测性和更复杂的动力特性。将 CML 模型应用于混沌密码中，具有如下的特点和优势[5]。

1) CML 模型虽然整体很复杂，但每个局部格子的结构却很简单;

2) 各个格子的结构相同，可以并行运算，易于提高效率;

3) 单个的格子通常由简单的局部混沌映射组成，运算速度非常快。

压缩感知技术是一种信号获取理论，在一定条件下可完成数据的采样与压缩。Cande 和 Tao[6] 认为，压缩感知框架可以视作对称加密方案，能同时对图像进行压缩与加密。因此，基于压缩感知的图像加密方案成为了研究的热点问题。Orsdemi[7] 提出在压缩感知框架下加密可以抵抗穷举攻击和结构攻击; Huang 等[8] 提出了先进行压缩感知采样，再对测量值进行置乱的加密方案; Zhang 等[9] 的方案则恰好相反，先对图像的频域系数进行置乱，然后进行压缩感知采样。这种方案的好处是能够提高图像的重构质量。一些研究者提出将图像编码技术与压缩感知结合构造图像加密方案[10]，这类方案最大优势是具有很好的解密鲁棒性。然而，上述这 3 类设计方法都要求对每个加密信号均使用不同的压缩感知测量矩阵，否则这些加密设计方案将难以抵抗选择明文攻击[11]。Cambareri 等[12] 量化了压缩感知抵抗已知明文攻击的能力; Rachlin 等[13] 发现压缩感知框架下对每个明文信息采用不相同的测量矩阵，加密方案可以满足计算性安全。然而，对每个加密信息均使用不同的测量矩阵进行处理，类似于加密算法中的“一次一密”，对整个加密系统的运行环境要求很高，不利于实际应用[14]。为了抵抗选择明文攻击，一些新的结合压缩感知框架的加密算法被提出。Huang 等[15] 提出在压缩感知采样完成后再引入分组加密操作，增强图像加密的安全，该方法虽然解决了安全性问题，但是压缩和加密是 2 个串行的操作过程，不利于效率的提高; Zhang 等[16] 提出双层保护压缩感知加密模型，通过密钥构造不满足有限等距性质(restricted isometry property，RIP) 的测量矩阵，攻击者使用选择明文攻击无法恢复原图像的测量矩阵，从而抵抗选择明文攻击。为了满足对每个加密信息采用不同的测量矩阵，一些研究者提出利用混沌伪随机来产生测量矩阵[17]。混沌伪随机序列具有很好的随机性，因此，由它所产生的测量矩阵满足 RIP 特性的概率很高。Gan 等[18] 指出混沌序列是否满足独立同分布与它所产生的测量矩阵是否满足约束等距特性 RIP 条件有高度的相关性; 石航等[19] 提出了一种基于压缩感知和多维混沌系统的图像加密方案，并结合小波变换等理论; 田宝强等[20] 提出了基于压缩感知和随机像素交换算法，提出一种高效的多图像联合加密方案; Li 等[21] 结合压缩感知和奇异值分解，提出了一种高效的图像加密方案。但这些研究中多以简单混沌系统和复合混沌模型作为加密模型，很少有以 CML 作为模型实现压缩和扩散的。由于混沌系统的参数易于存储，通过混沌系统的迭代可以源源不断地产生混沌序列，进而为每个加密信息构建不同的测量矩阵，从而有效解决了大量使用测量矩阵的存储问题，为抵御选择明文攻击的压缩感知图像加密设计提供了新的思路。

基于上述研究，基于 2D CML 模型产生混沌序列。通过独立性假设检验试验，证明混沌序列在某些条件下是拟独立的。拟独立的混沌序列能够满足 RIP 性质。在并行压缩感知框架下，使用该混沌序列进行并行采样压缩; 然后，对采样图像进行多轮扩

散;最后,对加密图像进行性能分析和对比分析。分析结果表明,本文提出的算法具有较好的统计学特征和加密特性。

1 预备知识

1.1 2D CML 模型

2D CML 模型,最早由 K.Kaneko 提出,是一种常用的时空混沌模型。它是对时空系统半宏观描述,在时间和空间 2 个方向都具有混沌现象。

在 2D CML 模型中,每个格子受临近上、下、左和右相邻 4 个格子的影响,数学表达式为

$$x_{n+1}^{u,v}=(1-\varepsilon)f(x_n^{u,v})+\frac{\varepsilon}{4}[f(x_n^{u+1,v})+f(x_n^{u-1,v})+f(x_n^{u,v+1})+f(x_n^{u,v-1})] \quad (1)$$

(1) 式中: $u=1,2,\cdots,R$ 和 $v=1,2,\cdots,L$ 是 2D CML 模型的行坐标和列坐标; $x_n^{u,v}$ 是第 u 行和第 v 列个格子在时刻 n 的状态值。它的周期边界条件是 $x_n^{u+R,v}=x_n^{u,v}$ 和 $x_n^{u,v+L}=x_n^{u,v}$。在(1)式中,每求一次状态值需计算局部函数 5 次。为了提高 2D CML 模型计算的效率,本文将(1)式简化成

$$x_{n+1}^{u,v}=(1-\varepsilon)f(x_n^{u,v})+\frac{\varepsilon}{2}[f(x_n^{u+1,v})+f(x_n^{u,v+1})] \quad (2)$$

1.2 LE

李雅普诺夫指数(Lyapunov exponent,LE)是判断动力学系统是否混沌的重要依据,在工程中,如果系统的 LE 大于 0,它是混沌的。否则,系统则是规则的。2D CML 模型的 LE 指数的表达式为[23]

$$LE=\lambda_f+\frac{1}{2}\ln\left|1+\frac{3}{2}\varepsilon^2-2\varepsilon+\varepsilon(1-\varepsilon)\left(\cos\frac{2\pi r}{R}+\cos\frac{2\pi l}{L}\right)+\frac{\varepsilon^2}{2}\cos\left(\frac{2\pi r}{R}-\frac{2\pi l}{L}\right)\right| \quad (3)$$

根据(3)式,在 2D CML 模型中,当 $r=R$ 和 $l=L$,取得最大李雅普诺夫指数(maximum Lyapunov exponent,MLE),此时,MLE 的值是 λ_f。即 MLE 是由模型的局部混沌映射决定的。因此,为了增强 2D CML 模型的混沌复杂性行为,选择 LE 较大的分段 logistic 函数(piecewise logistic map,PLM)作为模型的局部映射函数。

1.3 PLM

PLM 是对经典的 logistic 函数进行分段化处理,它具有更大的 LE 和更复杂的混沌行为。选择 PLM 函数作为局部混沌映射,能使 2D CML 模型具有较好的混沌特性。它的数学表达式为

$$x_{m+1}=PLM(x_m)=\begin{cases}N^2\mu x_m\left(\frac{1}{N}-x_m\right), & 0<x_m<\frac{1}{N}\\ 1-N^2\mu x_m\left(x_m-\frac{1}{N}\right)\left(\frac{2}{N}-x_m\right), & \frac{1}{N}<x_m<\frac{2}{N}\\ N^2\mu\left(x_m-\frac{i-1}{N}\right)\left(\frac{i}{N}-x_m\right), & \frac{i-1}{N}<x_m<\frac{i}{N}\\ 1-N^2\mu\left(x_m-\frac{i-1}{N}\right)\left(\frac{i+1}{N}-x_m\right), & \frac{i}{N}<x_m<\frac{i+1}{N}\\ \vdots & \\ N^2\mu\left(x_m-\frac{N-2}{N}\right)\left(\frac{N-1}{N}-x_m\right), & \frac{N-2}{N}<x_m<\frac{N-1}{N}\\ N^2\mu\left(x_m-\frac{N-1}{N}\right)(1-x_m), & \frac{N-1}{N}<x_m<1\\ x_m+\frac{1}{100N}, & x_m=0,\frac{1}{N},\frac{1}{N}\cdots\frac{N-1}{N}\\ x_m-\frac{1}{100N}, & x_m=1\end{cases} \quad (4)$$

(4)式中:分段数 $N=64$;耦合参数 $\mu=4$,此时,PLM 的 LE 的值是 4.574 594,根据(3)式可知,2D CML 的 MLE 是 $\lambda_f=4.574\ 594$。此时 2D CML 模型具有最好的复杂性和混沌特性。

2　压缩感知框架

2.1　并行压缩感知

在对原始图像 $A_{M\times N}$ 进行并行压缩感知采样过程中，采用压缩感知测量矩阵 $\boldsymbol{\Phi}_{N\times M}$ 对原始图像的每一列 $A_i \in R^{M\times M}$ 分别进行采样和重构。并行压缩感知的过程可以表示为

$$\boldsymbol{B}_i = \boldsymbol{\Phi} A_i \tag{5}$$

(5) 式中: $i=1,\cdots,N$; $\boldsymbol{B}_i \in R^N$ 经过并行压缩感知后，测量值图像 $\boldsymbol{B}_{M\times N}$ 可表示为 $\boldsymbol{B}_{M\times N} = [\boldsymbol{B}_1,\boldsymbol{B}_2,\cdots,\boldsymbol{B}_M]$。

2.2　独立性检验

混沌序列满足近似独立同分布，才能满足 RIP，应用于并行压缩感知中[18]。在 2D CML 模型中，使用如下方法进行混沌序列的独立性检验。

步骤 1　假设 2 个随机变量 X 和 Y 的方差分别是 S_{xx} 和 S_{yy}，协方差是 S_{xy}，则它们存在如下关系

$$P_{xy} = \frac{S_{xy}}{\sqrt{S_{xx}\cdot S_{yy}}} \tag{6}$$

步骤 2　假设 X 和 Y 独立，根据(7)式进行假设检验，如果(8)式成立，则在显著水平下，假设成立; 否则，假设不成立。

$$T = (Z^2_{\alpha/2} + n - 2)^{\frac{1}{2}} \times P_{xy} \tag{7}$$

$$-Z_{\alpha/2} < T < Z_{\alpha/2} \tag{8}$$

(7)—(8) 式中，Z 是标准正态分布变量，令 $\alpha = 0.05$，则 $Z_{\alpha/2} = 1.96$。

在 2D CML 模型中，取 $R=L=8$，$N=64$，$\mu=4$ 和 $\varepsilon=0.1$，时间序列间隔 $d=60$，根据步骤 1 和步骤 2 进行独立性假设检验，结果如图 1。重复 50 次测试实验，每组测试序列的长度是 1 000，可知所有的 T 值都在假设检验区间中。因此，这些混沌序列是近似独立的。

2.3　基于混沌序列的压缩感知测量矩阵

根据 2.2 节可知，2D CML 模型在一定的条件下产生的混沌序列是拟服从独立同分布的，根据约束等距特性[15]，可将这些混沌序列应用于图像的并行压缩感知中。压缩感知测量矩阵的构建算法如下。

1) 初始化 2D CML 模型，取 $R=L=8$，$N=64$，$\mu=4$ 和 $\varepsilon=0.1$，生成长度为 $1\ 000+NMd$ 的混沌序列，舍弃混沌序列的前 1 000 个点来消除混沌初值的影响。

2) 以 $d=60$ 的距离对长度为 NMd 的混沌序列进行采样，可生成混沌序列 Z。

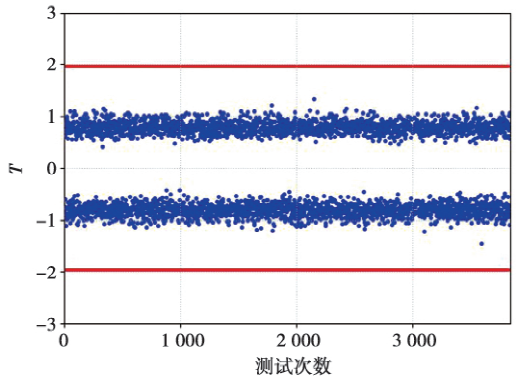

图 1　独立性假设检验

Fig.1　Independence hypothesis experiment

3) 利用 $w=1-2z$ 将混沌序列 Z 从 (0,1) 转换为 (−1,1) 的混沌序列 W。

4) 对混沌序列 W 以逐列的形式构建测量矩阵 $\boldsymbol{\Phi}_{N\times M}$，表示为

$$\boldsymbol{\Phi}_{N\times M} = \sqrt{\frac{2}{M}}\begin{pmatrix} w_0 & w_M & \cdots & w_{MN-M} \\ w_1 & w_{M+1} & \cdots & w_{MN-M+1} \\ \vdots & \vdots & & \vdots \\ w_{M-1} & w_{2M-1} & \cdots & w_{MN-1} \end{pmatrix} \tag{9}$$

(9) 式中，$\sqrt{\frac{2}{M}}$ 用于平衡采样前后的能量。

3　压缩感知框架下图像加密方案

在并行压缩感知框架下，基于 2D CML 模型的图像加密方案主要分为压缩感知的采样过程和采样图像的多轮扩散过程，主要流程如图 2，加密过程中基于 2D CML 的混沌测量矩阵和混沌序列采用不同的初始值，即不同的密钥。

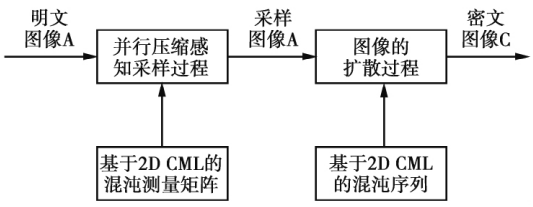

图 2　加密过程框架图

Fig.2　Frame diagram of the encrypted processing

3.1　原始图像的采样

原始图像如图 3，它的大小是 512 像素×512 像素。在采样过程中，根据(5)式的并行压缩框架和 2.3 节的压缩测量矩阵 $\boldsymbol{\Phi}_{N\times M}$ 实现对原始图像的并行压缩采样，采样结果如图 4。对比图 3 和图 4，经过并行压缩采样的图像已经变得很混乱。

图 3 原始图像

Fig.3 Original image

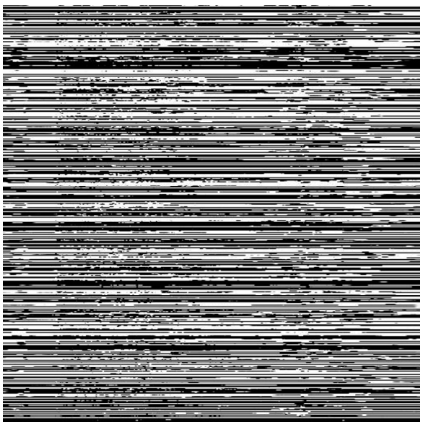

图 4 采样图像

Fig.4 Sampled image

3.2 图像的扩散过程

经过并行压缩后,实现了对原始图像的每一列进行采样。原始图像每一列的信息都保留在压缩后的对应的每一列种。所以,我们对压缩采样后的图像进行处理和多轮扩散操作,过程如下。

1) 将采样图像 B 的每一个测量值通过(10)式转换在(0,255)区间

$$P_i = round\left[\frac{255 \times (B_i - B_{\min})}{B_{\max} - B_{\min}}\right] \tag{10}$$

(10)式中: $round\lfloor . \rfloor$ 表示四舍五入取整函数; $B_{\min}$ 和 $B_{\max}$ 分别表示 $\boldsymbol{\Phi}_{N\times M}$ 中的最大值和最小值; $B_i(B_i \in \boldsymbol{B}_{M\times M})$ 是采样图像 B 的矩阵 $\boldsymbol{B}_{M\times M}$ 中的采样值。

2) 将 $P_i \in (0,255)$ 转变成为 8 位的二进制形式 Q_i,对 Q_i 进行如下处理可得到 Q_i',表示为

$$Q_i = b_1b_2b_3b_4b_5b_6b_7b_8 \tag{11}$$

$$Q_i' = (b_1 \oplus b_8)(b_2 \oplus b_7)(b_3 \oplus b_6) \cdot (b_4 \oplus b_5)b_5b_6b_7b_8 \tag{12}$$

3) 在 2D CML 中,取 $R = L = 8$, $N = 64$, $\mu = 4$ 和 $\varepsilon = 0.1$,对原始图像中的灰度值 G 按照(13)式和(14)式得到新的 ε',迭代混沌模型 1 000 次,为了消除初值的影响,舍弃前 1 000 次。继续迭代模型,对于每次迭代的值 x_n,转变成 64 位的二进制形式,取第 54—62 位作为密钥流 K。

$$sum = \sum_{a=1}^{W}\sum_{b=1}^{N} G_{ab} \tag{13}$$

$$\varepsilon' = \varepsilon + sum/256^2 \tag{14}$$

4) 然后对 Q_i' 依照(15)式进行多轮扩散操作。

$$Q_*'(m) = Q'(m) \oplus K(m) \oplus Q_*'(m-1) \tag{15}$$

(15)式中, $Q'(m)$, $Q_*'(m-1)$, $Q_*'(m)$, $K(m)$ 分别表示对采样图像 Q_i' 的当前操作,当前密文,下一次输出密文和加密密钥。

5) 对加密后的 $Q_*'(m)$ 图像依照(16)式变换,得到最后密文图像如图 5。

$$\overline{Q_*'} = \frac{Q_*' \times (B_{\max} - B_{\min})}{255} + B_{\min} \tag{16}$$

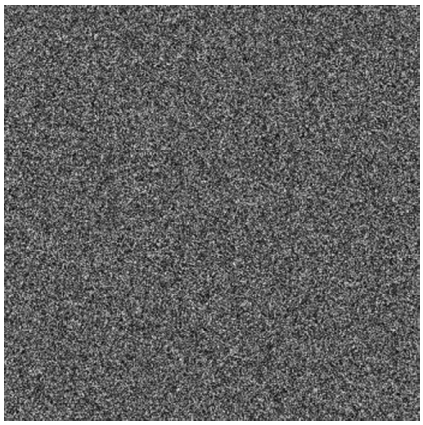

图 5 加密图像($\varepsilon = 0.1$)

Fig.5 Encryptedimage ($\varepsilon = 0.1$)

3.3 图像的解密过程

图像的解密过程就是加密的逆过程,对于 3.1 节和 3.2 节逆向操作,可得解密后图像如图 6。具体解密过程执行(17)—(22)式。

$$Q_*' = \frac{255(\overline{Q_*'} - B_{\min})}{(B_{\max} - B_{\min})} \tag{17}$$

$$Q'(m) = Q_*'(m) \oplus K(m) \oplus Q_*'(m-1) \tag{18}$$

$$Q'(m) = b'_1b'_2b'_3b'_4b_5b_6b_7b_8 \tag{19}$$

$$Q(m) = (b'_1 \oplus b_8)(b'_2 \oplus b_7)(b'_3 \oplus b_6) \cdot$$

$$(b'_4 \oplus b_5)\, b_5 b_6 b_7 b_8 \tag{20}$$

$$B_i = \frac{P_i \times (B_{\max} - B_{\min})}{255} + B_{\min} \tag{21}$$

$$\overline{s_i} = \operatorname{argmin} \| s_i \|_1 \tag{22}$$

通过压缩感知重构得到明文图像的稀疏矩阵后，就可以解得原始明文的图像。

图 6　恢复后的图像

Fig.6　Restored image

4　图像加密方案的性能分析

4.1　密钥分析

为了抵抗暴力破解的要求，通过设置 $\varepsilon = 0.1$ 和 $\varepsilon = 0.099\ 999\ 999\ 9$ 来分析密钥的敏感性，图 5 是 $\varepsilon = 0.1$ 的加密后的图像，图 7 是 $\varepsilon = 0.099\ 999\ 999\ 9$ 的加密图像。比较图 5 和图 7 相同位置像素的差异性，差异图像如图 8。2 种情况下加密后图像的差异程度达到 99.67%。这表明设计的图像加密方案具有较好的密钥敏感性。

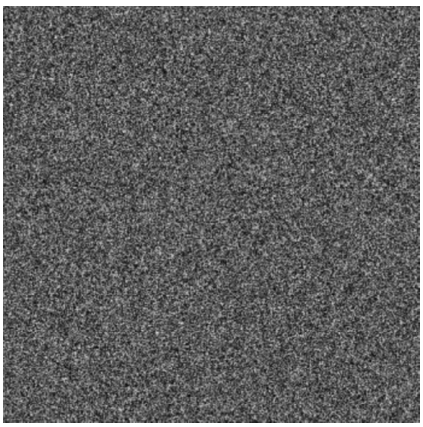

图 7　加密图像($\varepsilon = 0.099\ 999\ 999\ 9$)

Fig.7　Encryptedimage ($\varepsilon = 0.099\ 999\ 999\ 9$)

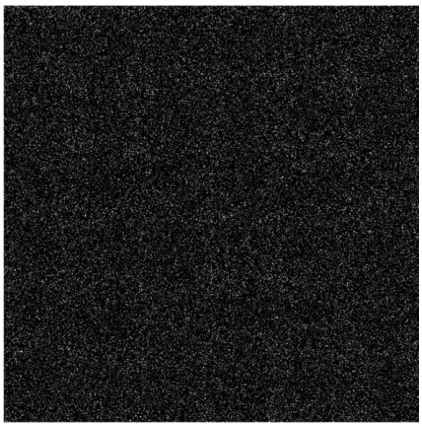

图 8　差异图像

Fig.8　Difference image

4.2　统计分析

对于原始图像和加密图像，从图像灰度值的统计直方图和各个方向的相关系数 2 个方面来对比分析加密方案的性能。原始图像的灰度值直方图如图 9，分布明显不均匀，灰度值集中分布区域明显，图像的灰度值信息直观暴露较多。经过加密后的图像灰度值分布如图 10，灰度值分布较均匀，能够很好地隐藏原始图像的灰度值的信息。

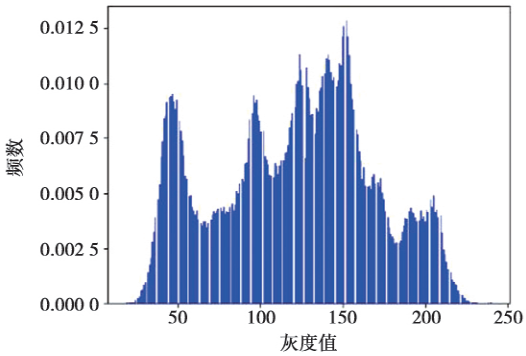

图 9　原始图像的灰度值直方图

Fig.9　Gray value histogram of the original image

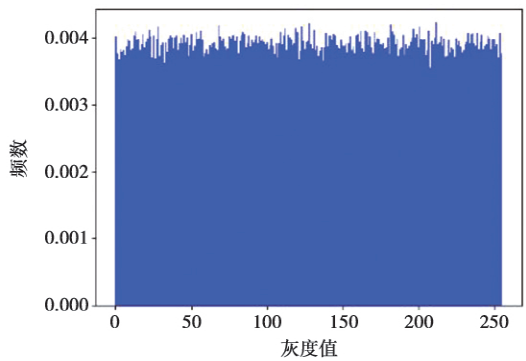

图 10　加密图像的灰度值直方图

Fig.10　Gray value histogram of the encrypted image

原始图像中像素点在各个方向(水平、垂直和对角相邻像素)的相关性非常大。使用(17)式和(18)式来计算它们相关性。计算过程如下:从原始图像和加密后的图像各抽取 1 000 组水平、垂直和对角相邻的像素,按照(23)式和(24)式计算它们的相关性。计算结果如图 11—图 16 和表 1,原始图像的各个方向的相关性分别是 0.983 5,0.986 2 和 0.965 8。加密图像的各个方向的相关性分别是 0.006 41,0.006 26 和−0.009 41,加密图像的相关性数值几乎可以忽略。同时,和文献[23-28]对比分析,表明所设计的加密算法具有较好的抵抗统计攻击的性能。

$$cov(x,y) = E\{(x - E(x))(y - E(y))\} \quad (23)$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (24)$$

(23)—(24)式中:x 和 y 为图像中相邻像素的灰度值;设 P 是像素对的个数,$E(x) = (\sum_{i=1}^{P} x_i)/P$;$D(x) = \{\sum_{i=1}^{P} (x_i - E(x))^2\}/P$。

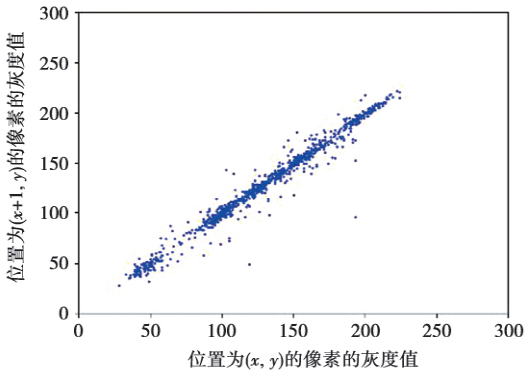

图 11 原始图像的水平相关性

Fig.11 Horizontal correlation of the original image

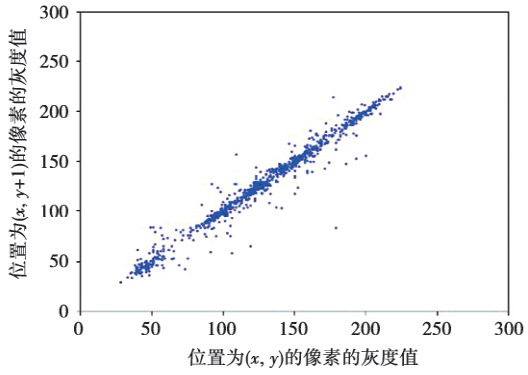

图 12 原始图像的垂直相关性

Fig.12 Verticalcorrelation of the original image

表 1 原始图像和密文图像中相邻点的相关系数

Tab.1 Correlation coefficients of adjacent points in the original image and encrypted image

算法	方向	原始图像	密文图像
本文	水平相邻	0.983 5	0.002 4
	垂直相邻	0.986 2	0.006 2
	对象相邻	0.965 8	−0.003 4
文献[23]	水平相邻	0.959 1	0.002 8
	垂直相邻	0.934 1	−0.002 3
	对象相邻	0.903 1	0.004 8
文献[24]	水平相邻	0.983 5	0.003 6
	垂直相邻	0.986 2	−0.004 4
	对象相邻	0.965 8	−0.004 0
文献[25]	水平相邻	0.924 8	−0.004 2
	垂直相邻	0.960 6	0.008 1
	对象相邻	0.901 7	0.001 3
文献[26]	水平相邻	0.969 2	−0.006 7
	垂直相邻	0.969 9	−0.001 5
	对象相邻	0.910 4	−0.002 6
文献[27]	水平相邻	0.975 0	0.006 2
	垂直相邻	0.971 4	−0.010 7
	对象相邻	0.950 1	0.005 2
文献[28]	水平相邻	0.989 7	−0.003 9
	垂直相邻	0.978 7	0.003 1
	对象相邻	0.968 1	−0.007 3

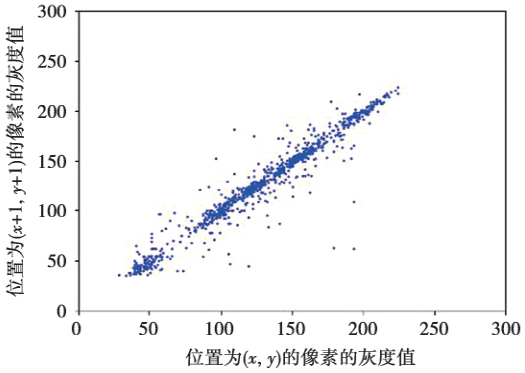

图 13 原始图像的对角相关性

Fig.13 Diagonal correlation of the original image

4.3 信息熵

图像的信息熵是反映图像中的平均信息量的多少,使用(25)式计算信息熵,它的最大混乱状态下的理想值是 8。通过计算得到原始图像和加密图像的信息熵分别是 7.429 5 和 7.999 2。本文图像加密方案的信息熵计算值和其他文献[23-28]的比较如表 2。

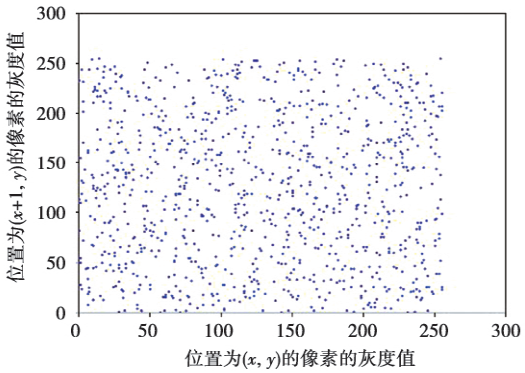

图 14　加密图像的水平相关性

Fig.14　Horizontal correlation of the encrypted image

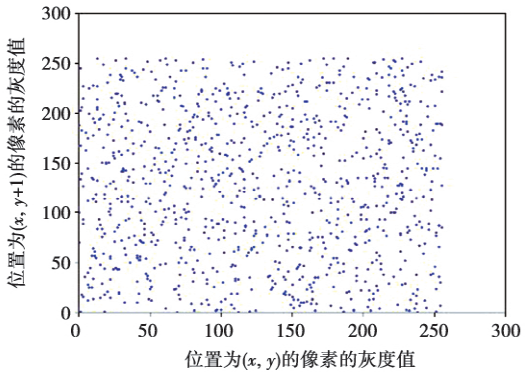

图 15　加密图像的垂直相关性

Fig.15　Vertical correlation of the encrypted image

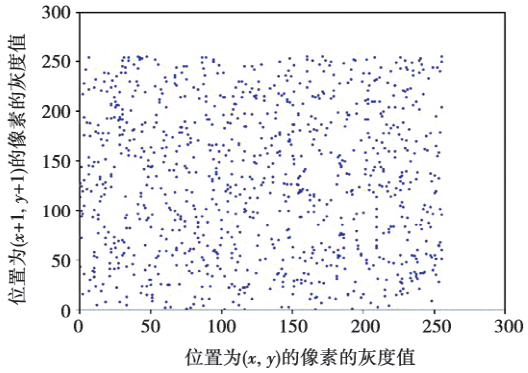

图 16　加密图像的对角相关性

Fig.16　Diagonal correlation of the encrypted image

表 2　信息熵

Tab.2　Information entropy

算法	信息熵 H
本文	7.999 2
文献 [23]	7.997 6
文献 [24]	7.997 5
文献 [25]	7.997 3
文献 [26]	7.997 2
文献 [27]	7.997 0
文献 [28]	7.998 6

可以得到本文加密后图像的信息熵更接近 8.0,表明图像灰度分布聚集特征较好,能够有效抵御攻击。

$$H = \sum_{i=0}^{n} p(a_i)\ \mathrm{lb}^{p(a_i)} \tag{25}$$

(25) 式中: a_i 是图像的灰度值; $p(a_i)$ 是灰度值 a_i 的像素所占的比例。

4.4　差分攻击

在对图像进行差分攻击时,敌手通常是对明文图像细小的调整,然后在比较原始密文 C_1 和微小调整后明文的密文 C_2 的差别进行攻击。一般用像素变化率(number of pixels change rate,NPCR)和归一化平均变化强度(unified average changing in tensity,UACI)这 2 个指标进行衡量,计算式为

$$NPCR = \frac{1}{M \times N} \times \sum_{i=1}^{M} \sum_{j=1}^{N} \boldsymbol{D}(i,j) \times 100\% \tag{26}$$

$$UACI = \frac{1}{M \times N} \times \left[\sum_{i=1}^{M} \sum_{j=1}^{N} \frac{| \boldsymbol{C}_1^{(i,j)} - \boldsymbol{C}_2^{(i,j)} |}{255} \right] \times 100\% \tag{27}$$

(26)—(27) 式中: C_1 和 C_2 的原始图像之间仅有一个像素的灰度值不一样,当 $\boldsymbol{C}_1^{(i,j)} = \boldsymbol{C}_2^{(i,j)}$ 时, $\boldsymbol{D}(i,j) = 0$; 否则, $\boldsymbol{D}(i,j) = 1$。NPCR 和 UACI 的理想值分别是 0.996 和 0.334。随机选择 10 个点,调节灰度值,计算出本文和文献 [23-28] 的 NPCR 和 UACI 的值。如表 3,本文算法是比较接近理想值,能够很好地抵抗差分攻击。

表 3　NPCR 和 UACI

Tab.3　NPCR and UACI

算法	*NPCR*	*UACI*
本文	0.996 0	0.335 3
文献 [23]	0.995 7	0.334 2
文献 [24]	0.999 5	0.335 3
文献 [25]	0.996 2	0.335 5
文献 [26]	0.995 0	0.333 8
文献 [27]	0.998 7	0.333 6
文献 [28]	0.995 6	0.334 3

5　结束语

通过独立性假设检验,表明 2D CML 模型产生的混沌序列拟满足独立同分布,将混沌序列应用于产生测量矩阵。在并行压缩感知框架下,对原始图像进行压缩采样,对采样图像进行预处理和多轮扩散得到加密后的图像。对加密图像进行密钥敏感

性、统计、信息熵和差分攻击的实验分析和其他算法的比对，得出本文设计的基于 2D CML 模型的图像压缩加密方案具有很好的加密性能。

参考文献:

[1] WOIF A, SWIFT J B, SWINNEY H L, et al. Determining Lyapounov exponents from a time series [J]. Physica D Nonlinear Phenomena, 1985, 16(3): 285-317.

[2] 李丕. 高维非线性系统的加密算法与混沌同步研究 [D].大连: 大连理工大学,2018.
LI P. Research on encryption algorithm and chaos synchronization of high dimensional nonlinear system [D]. Dalian: Dalian University of Technology, 2018.

[3] JAKIMOSKI G, KOCAREV L. Chaos and cryptography: block encryption ciphers based on chaotic maps [J]. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 2001, 48(2): 163-169.

[4] YANG T WU C W, CHUA L O. Crypto-graphy based on chaotic systems [J]. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 1997, 44(5): 469-472.

[5] LIAN S G, SUN J S, WANG Z Q. A block cipher based on a suitable use of the chaotic standard map [J].Chaos, Solitons and Fractals, 2005, 26(1): 117-129.

[6] CANDE S E, TAO T. Near-optimal signal recovery from random projections: universal encoding strategies [J]. IEEE Transactions on Information Theory, 2006, 52(12): 5406-5425.

[7] ORSDEMI R A, ALTUN H O, SHARMA G, et al. On the security and robustness of encryption via compressed sensing [C] //Military Communications Conference. New York: IEEE, 2008: 1-7.

[8] HUANG X L, YE G D, CHAI H J, et al. Compression and encryption for remote sensing image using chaotic system [J]. Security and Communication Networks, 2015, 8(18): 3659-3666.

[9] ZHANG Y S, WANG K W, XIAO D,et al. Embedding cryptographic features in compressive sensing [J]. Neurocomputing, 2016(205): 472-480.

[10] ZHOU N R LI H L, WANG D, et al. Image compression and encryption scheme based on 2D compressive sensing and fractional mellin transform [J]. Optics Communications, 2015(343): 10-21.

[11] RAWAT N, KIM B, MUNIRAJ I, et al. Compressive sensing based robust multispectral double-image encryption [J]. Applied Optics, 2015, 54(7): 1782-1793.

[12] CAMBARERI V, MANGIA M, PARESCHI F, et al. On known-plaintext attacks to a compressed sensing-based encryption: a quantitative analysis [J]. IEEE Transactions on Information Forensics and Security, 2015, 10(10): 2182-2195.

[13] RACHLIN Y, BARON D. The secrecy of compressed sensing measurements [C] //46th Annual Allerton Conference on Communication, Control, and Computing. New York: IEEE, 2008: 813-817.

[14] 胡国强. 压缩感知理论在图像信息保护中的应用研究 [D].重庆: 重庆大学, 2017.
HU G Q. The application research of compressed sensing theory in image information protection [D]. Chongqing: Chongqing University, 2017.

[15] HUANG R, RHEE K H, UCHIDA S. A parallel image encryption method based on compressive sensing [J]. Multimedia Tools and Applications, 2014, 72(1): 71-93.

[16] ZHANG L Y, WONG K W, ZHANG Y S, et al. Bi-level protected compressive sampling [J]. IEEE Transactions on Multimedia, 2016, 18(9): 1720-1732.

[17] YU L, BARBOT J P, ZHENG G, et al. Compressive sensing with chaotic sequence [J]. IEEE Signal Processing Letters, 2010, 17(8): 731-734.

[18] GAN H P, LI Z, LI J, et al. Compressive sensing using chaotic sequence based on chebyshev map [J]. Nonlinear Dynamics, 2014, 78(4): 2429-2438.

[19] 石航,王丽丹. 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 [J].物理学报,2019,68(20):39-52.
SHI H, WANG L D. A multi-process image encryption scheme based on compressed sensing and multi dimensional chaotic system [J]. Acta Physica Sinica, 2019, 68(20): 39-52.

[20] 田宝强,谢东.基于压缩感知和随机像素置换的多图像联合加密方案 [J].杭州师范大学学报,2020,19(2):208-214.
TIAN B Q, XIE D. Multi-image joint encryption scheme based on compressed sensing and random pixel replacement [J]. Journal of Hangzhou Normal University, 2020, 19(2): 208-214.

[21] LI Y Z, HUAN S S, XI Z. A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding [J]. Signal Processing, 2020(175): 107629.

[22] 王永,赵毅, GAO J,等.基于分段 Logistic 映射的二维耦合映像格子模型的密码学相关特性分析 [J].电子学报,2019,47(03):657-663.
WANG Y, ZHAO Y, GAO J, et al. Cryptographic feature

analysis on 2D coupled map lattices based on piece wise logistic map [J]. Chinese Journal of Electronics, 2019, 47(03): 657-663.

[23] 赵耿，李建新，马英杰，等.基于小波变换的抗退化混沌图像加密算法 [J].计算机应用与软件，2020，37(04)：290-296.
ZHAO G, LI J X, MA Y J, et al. Anti-degeneration chaotic image encryption algorithm based on wavelet transform [J]. Computer Applications and Software, 2020, 37(04): 290-296.

[24] 王磊，薛伟.基于时空混沌和小波变换的图像加密算法 [J].计算机工程与科学，2018，40(05)：856-862.
WANG L, XUE W. The image encryption algorithm based on spatiotemporal chaos and wavelet transform [J]. Computer Engineering and Science, 2018, 40(05): 856-862.

[25] 杨晓刚，范建卫，高宝文，等.基于小波变换和混沌映射的图像加密算法 [J].火控雷达技术，2016，45(01)：56-63，68.
YANG X G, FAN J W, GAO B W, et al. The image encryption algorithm based on wavelet transform and chaotic mapping [J]. Fire Control Radar Technology, 2016, 45(01): 56-63, 68.

[26] 罗玉玲，杜明辉.基于量子 Logistic 映射的小波域图像加密算法 [J].华南理工大学学报(自然科学版)，2013，41(06)：53-62.
LUO Y L, DU M H. The image encryption algorithm based on quantum logistic mapping in wavelet domain [J]. Journal of South China University of Technology(Natural Science Edition), 2013, 41(06): 53-62.

[27] WANG H, XIAO D, LI M, et al. A visually secure image encryption scheme based on parallel compressive sensing [J]. Signal Processing, 2019(155): 218-232.

[28] CHAI X L, WU H Y, ZHANG Y S, et al. Hiding cipher-images generated by 2D compressive sensing with a multiple-embedding strategy [J]. Signal Processing, 2020(171): 107525.

作者简介:

刘　卓(1987—)，女，河南驻马店人，硕士研究生，主要研究方向为信息安全、混沌密码等。E-mail: liuzhuo1987@outlook.com。

王　永(1977—)，男，四川自贡人，教授，博士，主要研究方向为信息安全、混沌密码等。E-mail: wangyong1@cqupt.edu.cn。

(编辑: 王敏琦)