文章编号: 1006-4710(2012)02-0193-05

基于高维广义猫映射的图像加密算法

鲍芳, 李军, 李旭
(广东工业大学 自动化学院,广东 广州 510006)

摘要: 提出了一种四维广义猫映射,并构造了一种基于该映射的图像加密算法。将三维广义猫映射扩展至四维广义猫映射,通过将图像的像素坐标和灰度值作为广义猫映射的初始值,映射参数和迭代次数作为密钥实现图像加密。与常见的低维混沌猫映射加密算法相比,该算法具有更大的密钥空间及更高的加密速度,可作为加密系统的一个子模块用于常规网络或中高速无线传感器网络图像、数据块和视频的加密传输。

关键词: 图像加密; 混沌; 猫映射
中图分类号: TN914.2 **文献标志码:** A

Image Encryption Algorithm Based on High Dimensional Chaotic Cat Maps

BAO Fang, LI Jun, LI Xu
(College of Automation, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: A 4D dimensional extensive cat map and a novel fast image encryption algorithm based on the map are proposed in this paper. The 3D extensive cat map is extended to a 4D extensive cat map. The pixel coordinates and the grey values of images can be used as the initial conditions of the 4D extensive cat map, and the mapping parameters and the number of iteration can be used as the secret keys to achieve image encryption. In comparison with the usual low dimension chaotic cat map encryption algorithm, this algorithm is of higher security and faster encryption speed. It can be used as a sub-model in the encryption system, which can be served for encryption transmissions of images, data blocks and visual images in conventional networks as well as wireless sensor networks with the medium or high speed.

Key words: image encryption; chaos; cat map

信息获取能力和信息安全保障能力是二十一世纪一个国家综合国力的重要组成部分,密码技术在解决网络信息安全中发挥着重要的基础性作用。传统的对称和非对称密码对于语音、图像以及视频等大数据量和高冗余性的多媒体信息来说并不太合适。为解决多媒体信息的加密问题,近年来人们尝试利用混沌的拓扑传递性来快速地进行图像像素坐标的置乱及像素值的扩散变换。典型的混沌映射如Baker map、Cat map、Line map 等,利用图像的几何特征,对图像进行拉伸和折叠,密钥的微小变化经变换后扩散到密图中,由于映射的置换与扩散算法组合非常多,使密钥分析较为困难[1-3]。针对单一混沌映射的加密系统容易被破解的特点,有混沌加密系统复合使用多组低维映射以提高算法安全性[4-5]。例如文献[4]将三维广义猫映射加密算法中的像素扫描改进为随机方式,在扩散过程引入 Logistic 函数进行异或使得扩散过程更具有混沌敏感性。但这些方法是以增加计算量为代价,降低了图像加密算法的实时性。根据混沌动力学理论,高维广义猫映射混沌系统较二维或三维等低维猫映射具有更大的 Lyapunov 指数及更多的控制参数个数[6],这使得基于高维广义猫映射的图像加密算法具有更大的密钥空间,并且只需较少的加密轮数即可获得均匀分布的密文,进而可获得更高的加密速度和增加破解难度,在目前可查阅的参考文献中尚未见类似的报道。

1 从二维猫映射比较密码变换与混沌映射的关系

猫映射(Cat map)最早是由 Arnold 引入的[7],

收稿日期: 2011-12-03
基金项目: 国家自然科学基金资助项目(U0935002);广东省自然科学基金资助项目(9151009001000030)。
作者简介: 鲍芳(1967-),女,湖北钟祥人,副教授,博士,研究方向为网络化测控技术。E-mail:fainabao@126.com。

因为经常用一张猫脸的图进行演示而得名,其方程如下:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \pmod 1 \qquad (1)$$

式中,x_n, y_n 都是实数且满足 $0 < x_n, y_n < 1$ ($n = 0, 1, 2, \cdots$)。(x_n, y_n) 的相空间被限制在单位正方形 $[0,1] \times [0,1]$ 内,猫映射在此正方形内不断地进行线性的拉伸(乘以矩阵使 x_n、y_n 都变大),然后折叠(通过取模使 x_n、y_n 又折回单位正方形内),具有Shannon在其经典论文《保密通信理论》中指出的一个好的混合变换应具有的"在有限区域内进行反复折叠、拉伸变换的特性"[8]。

将原始的猫映射定义(1)式数字化,即 x_n, y_n ($n = 0, 1, 2, \cdots$) 均取正整数而非任意实数,得到如下二维广义猫映射:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \boldsymbol{C}_2 \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\mathrm{mod}\ N), \boldsymbol{C}_2 = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \qquad (2)$$

式中 a, b, N 为正整数。可以证明(2)的参数 a, b 以 N 为周期,故要求 $a, b \in N$。

若初始值 x_0, y_0 为正整数,则 x_n, y_n ($n = 0, 1, 2, \cdots$) 也均为正整数,数字化后的猫映射(2)仍然具有猫映射的拉伸和折叠的性质,故可通过将图像的像素坐标及灰度值作为(2)的初始值进行迭代来实现图像的加密。对于图像内原来相邻的两点如 (x_n, y_n) 和 (x_n, y_{n+1}),其像素坐标经广义猫映射迭代几次后不再相邻;具有均匀概率分布的猫映射还可以保证经过一定次数的灰度值迭代后,原加密图的灰度直方图由具有特定的统计规律改变为呈均匀分布,从而达到图像保密的目的。

2 从二维广义猫映射到高维广义猫映射的扩展

本节给出三维广义猫映射的定义并将其扩展至四维广义猫映射。基于三维到四维的扩展模式可以将广义猫映射扩展至更高维如八维,但由于篇幅限制及基于表述简介的原则,下面以四维广义猫映射为例说明如何将低维猫映射扩展至高维广义猫映射。

2.1 三维广义猫映射

文献[1]将二维广义猫映射(2)扩展为三维广义猫映射:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{pmatrix} = \boldsymbol{C}_3 \begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix} (\mathrm{mod}\ N), \boldsymbol{C}_3 = \begin{pmatrix} 1 + a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y a_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{pmatrix} \qquad (3)$$

其中 N 为正整数,$a_i, b_i (i = x, y, z) \in N$ 且为正整数。

2.2 四维广义猫映射

通过以下4个映射子变换可以实现从三维广义猫映射(3)到四维广义猫映射的扩展。

在 (x, y, z) 三维空间进行三维广义猫映射,同时令 $\gamma_{n+1} = \gamma_n$,由(3)可得:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \\ \gamma_{n+1} \end{pmatrix} = \boldsymbol{Q}_1 \begin{pmatrix} x_n \\ y_n \\ z_n \\ \gamma_n \end{pmatrix} (\mathrm{mod}\ N), \boldsymbol{Q}_1 = \begin{pmatrix} 1 + a_x a_z b_y & a_z & a_y + a_x a_z (a_y b_y + 1) & 0 \\ b_z + (a_z b_z + 1) a_x b_y & a_z b_z + 1 & b_z a_y + (a_z b_z + 1) a_x (a_y b_y + 1) & 0 \\ (a_x b_x + 1) b_y & b_x & (a_x b_x + 1)(a_y b_y + 1) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad (4)$$

在 (x, y, γ) 三维空间进行三维广义猫映射,同时令 $z_{n+1} = z_n$,由(3)可得:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \\ \gamma_{n+1} \end{pmatrix} = \boldsymbol{Q}_2 \begin{pmatrix} x_n \\ y_n \\ z_n \\ \gamma_n \end{pmatrix} (\mathrm{mod}\ N), \boldsymbol{Q}_2 = \begin{pmatrix} 1 + a_x a_\gamma b_y & a_\gamma & 0 & a_y + a_x a_\gamma (a_y b_y + 1) \\ b_\gamma + (a_\gamma b_\gamma + 1) a_x b_y & a_\gamma b_\gamma + 1 & 0 & b_\gamma a_y + (a_\gamma b_\gamma + 1) a_x (a_y b_y + 1) \\ 0 & 0 & 1 & 0 \\ (a_x b_x + 1) b_y & b_x & 0 & (a_x b_x + 1)(a_y b_y + 1) \end{pmatrix} \qquad (5)$$

在 (x, z, γ) 三维空间进行三维广义猫映射,同时令 $y_{n+1} = y_n$,由(3)可得:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \\ \gamma_{n+1} \end{pmatrix} = \boldsymbol{Q}_3 \begin{pmatrix} x_n \\ y_n \\ z_n \\ \gamma_n \end{pmatrix} (\mathrm{mod}\ N), \boldsymbol{Q}_3 = \begin{pmatrix} 1 + a_x a_\gamma b_z & 0 & a_\gamma & a_z + a_x a_\gamma (a_z b_z + 1) \\ 0 & 1 & 0 & 0 \\ b_\gamma + (a_\gamma b_\gamma + 1) a_x b_z & 0 & a_\gamma b_\gamma + 1 & b_\gamma a_z + (a_\gamma b_\gamma + 1) a_x (a_z b_z + 1) \\ (a_x b_x + 1) b_z & 0 & b_x & (a_x b_x + 1)(a_z b_z + 1) \end{pmatrix} \qquad (6)$$

在 (y, z, γ) 三维空间进行三维广义猫映射,同时令 $x_{n+1} = x_n$,由(3)可得:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \\ \gamma_{n+1} \end{pmatrix} = \boldsymbol{Q}_4 \begin{pmatrix} x_n \\ y_n \\ z_n \\ \gamma_n \end{pmatrix} (\mathrm{mod}\ N), \boldsymbol{Q}_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 + a_y a_\gamma b_z & a_\gamma & a_z + a_y a_\gamma (a_z b_z + 1) \\ 0 & b_\gamma + (a_\gamma b_\gamma + 1) a_y b_z & a_\gamma b_\gamma + 1 & b_\gamma a_z + (a_\gamma b_\gamma + 1) a_y (a_z b_z + 1) \\ 0 & (a_y b_y + 1) b_z & b_y & (a_y b_y + 1)(a_z b_z + 1) \end{pmatrix} \tag{7}$$

联立(4)~(7)可得四维广义猫映射为:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \\ \gamma_{n+1} \end{pmatrix} = \boldsymbol{C}_4 \begin{pmatrix} x_n \\ y_n \\ z_n \\ \gamma_n \end{pmatrix} (\mathrm{mod}\ N), \quad \boldsymbol{C}_4 = \boldsymbol{Q}_1 \boldsymbol{Q}_2 \boldsymbol{Q}_3 \boldsymbol{Q}_4 \tag{8}$$

为计算及表述简洁起见,可令各基本参数 $a_x = a_y = a_z = a_\gamma = b_x = b_y = b_z = b_\gamma = 1$,有:

$$\boldsymbol{C}_4 = \begin{pmatrix} 45 & 240 & 132 & 452 \\ 77 & 411 & 226 & 774 \\ 48 & 256 & 141 & 482 \\ 12 & 64 & 35 & 121 \end{pmatrix} \tag{9}$$

上述各维广义猫映射均为保面积的,即满足:

$$\det \boldsymbol{C}_2 = \det \boldsymbol{C}_3 = \det \boldsymbol{C}_4 = 1$$

2.3 三类广义猫映射的基本动力学特征

选择一个合适的基本混沌映射系统,可以减少加密复杂度及提高加密速度且不失去良好的安全加密性能。

根据混沌动力学理论,文献[9]从刻画动力系统对初始条件敏感性强弱程度的 Lyapunov 指数和混沌映射分布的均匀性两个方面出发,指出一个合适的混沌映射系统应该具有以下特征:1)大的 Lyapunov 指数。具有较大 Lyapunov 指数的混沌映射对初始值更敏感,也就越适合用于加密系统。2)均匀的概率分布。由于混沌映射的拓扑传递性,一个离散混沌映射的迭代轨迹会落在相空间的每一点的小邻域,但其分布并非一定均匀。具有均匀概率分布的混沌映射可以保证明文经过一定次数的迭代后获得均匀分布的密文,具有较强的抗统计攻击性能。例如针对 Logistic 映射的分布在区域(0,1)两端呈现奇异性,文献[10]给出了一种基于概率原理的变换方法,实现把 Logistic 映射产生的非均匀分布随机变量转化为均匀分布的随机变量,进而满足图像置乱需要。与 Logistic 映射相比,即使是二维猫映射也能保证明文只通过一轮的扩散变换就可获得较均匀分布的密文,这是由混沌系统自身的特性所决定。

由三类广义猫映射的定义式(2)、(3)及(8)可以计算出当各基本参数均取 1 时,各类猫映射的特征值及最大 Lyapunov 指数,如表 1 所示。由表 1 可以得到,四维广义猫映射的最大 Lyapunov 指数远大于二维或三维猫映射的最大 Lyapunov 指数,因此从动态系统对初始条件敏感性强弱程度而言,四维广义猫映射较低维的猫映射更适合加密系统。

表 1 三类广义猫映射的基本动力学特征比较

Tab. 1 Comparison among basic dynamic behaviors of different dimensional cat maps

广义猫映射类型	特征值	最大 Lyapunov 指数
二维	$\sigma_1 = 2.618, \sigma_2 = 0.382$	0.481
三维	$\sigma_1 = 7.184, \sigma_2 = 0.573, \sigma_3 = 0.243$	0.654
四维	$\sigma_1 = 717.269, \sigma_2 = 0.625, \sigma_3 = 0.080, \sigma_4 = 0.028$	1.644

3 基于四维广义猫映射的图像加密算法

置换和替代是加密技术的两个基本构造模块。由于对图像像素坐标进行的像素置乱不会改变图像的统计直方图,为了避免统计攻击,通常图像加密算法会引入图像像素值的扩散变换使密文的直方图变得比较均匀,并通过置乱变换与扩散变换的组合进行多轮的变换,以获得更好的加密效果。

3.1 图像扩散

欲将四维猫映射应用于图像扩散,可将原始图像分解成 2×2 的小方块,对每个方块中的四个像素值 $f(i,j)$,$f(i+1,j)$,$f(i,j+1)$ 及 $f(i+1,j+1)$ 运用如下变换:

$$\boldsymbol{X}' = \boldsymbol{C}_4 \boldsymbol{X} (\mathrm{mod}\ N) \tag{10}$$

式中 $\boldsymbol{X} = [f(i,j) \quad f(i,j+1) \quad f(i+1,j) \quad f(i+1,j+1)]^{\mathrm{T}}$ 为小方块中四个像素值组成的向量,$\boldsymbol{X}' = [f'(i,j) \quad f'(i,j+1) \quad f'(i+1,j) \quad f'(i+1,j+1)]^{\mathrm{T}}$ 为经扩散变换后的像素值向量。

3.2 加密算法

1) 设置加密密钥:加密轮数 k,猫映射的参数 $a_i, b_i (i = x,y,z,\gamma) \in N$;

2) 利用二维猫映射式(2)对图像像素的位置进行置乱变换;

3) 在每一次的置乱变换后根据式(10)进行基于四维猫映射的像素值扩散变换;

4) 转到步骤 2),将加密算法中的 2)、3)步循环做 k 轮。

3.3 解密算法

解密算法是加密算法的逆过程,具体过程如下:

1) 设置解密密钥:即解密轮数为 k,猫映射的参数 $a_i, b_i (i = x, y, z, \gamma) \in N$ 与加密时完全相同;

2) 进行一次像素值反扩散变换,即运用反扩散的公式:

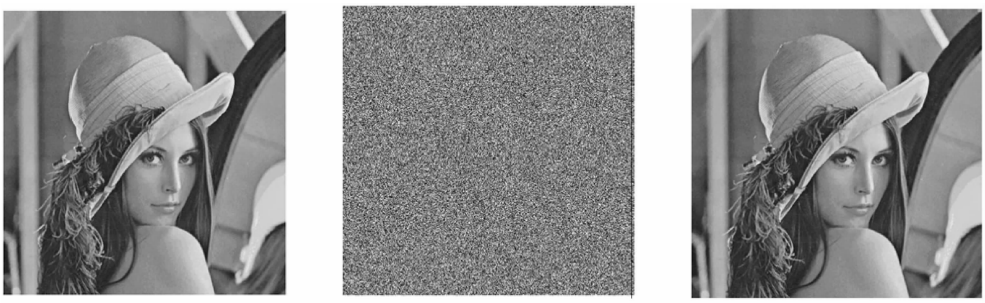
$$\boldsymbol{X}' = \boldsymbol{C}_4^{-1}\boldsymbol{X} (\bmod N),\ \boldsymbol{C}_4^{-1} = \begin{pmatrix} 37 & -16 & -8 & -4 \\ 5 & 3 & -8 & -6 \\ -8 & 0 & 7 & 2 \\ -4 & 0 & 3 & 3 \end{pmatrix} \quad (11)$$

3) 在一次反扩散变换后进行像素位置反置乱变换,即运用反置乱变换公式:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \boldsymbol{C}_2^{-1} \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\bmod N), \boldsymbol{C}_2^{-1} = \begin{pmatrix} ab+1 & -a \\ -b & 1 \end{pmatrix} \quad (12)$$

4) 转到步骤 2),将解密算法中的 2)、3) 步循环做 k 轮。

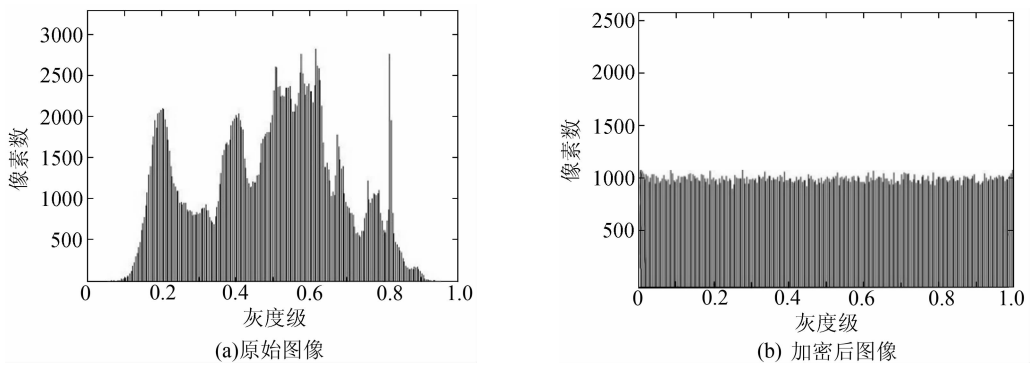
图 1 给出了对一幅 256 × 256 像素经典 Lena 图像的基于上述加解密算法的加、解密仿真计算结果($k = 3$)。图 2 给出了原始图像及加密后图像的灰度直方图。



(a) 原始图像 (b) 三轮加密后图像 (c) 解密后图像

图 1 一幅 256 × 256 像素图像的加、解密仿真计算结果

Fig. 1 Simulation results of encrypting and decrypting an image of 256 × 256 pixels



(a)原始图像 (b) 加密后图像

图 2 原始及各加密后图像的灰度直方图

Fig. 2 Histograms of the raw image and the encrypted images

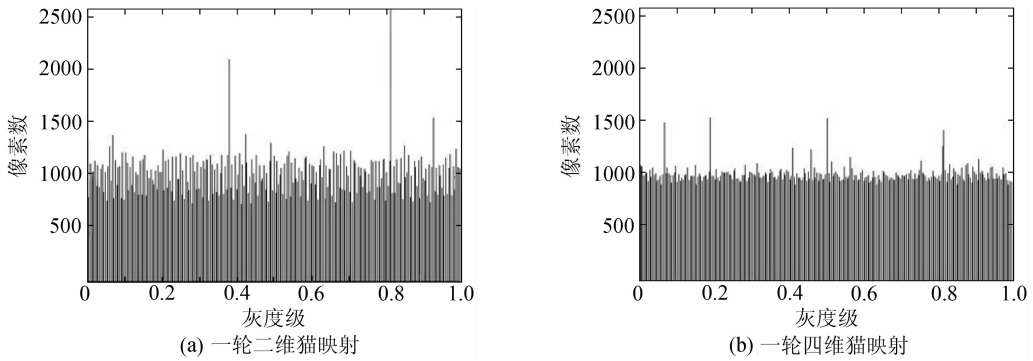
由图 2 可知,经三轮加密后的直方图(b)呈均匀分布,它掩盖了原始图像灰度直方图(a)的分布规律,用此方法加密后的密文对密钥的贡献很小。

3.4 加密算法速度与安全性分析

仅考虑单轮计算量时,基于低维和高维的广义猫映射图像加密算法速度无实质区别,两者所需计算时间均取决于原始图像像素的大小,但高维广义猫映射具有更大的 Lyapunov 指数,这使得基于高维广义猫映射的图像加密算法只需较少的加密轮数即可获得均匀分布的密文,进而可获得更高的加密速度。图 3 给出了原始图像经过一轮由(2)式描述的二维广义猫映射(a, b 均取 1)及一轮由(9)式描述的四维猫映射扩散变换后获得的图像灰度直方图。从图 3 可以看到,在相同加密轮数时四维猫映射加密算法较二维猫映射加密算法获得了更为均匀分布的密文,表明基于高维广义猫映射的图像加密算法只需较少的加密轮数即可获得均匀分布的密文。

Shannon 曾指出理论上不可破译的密码系统是“一次一密钥”系统,主要阐述了在加密过程中每一个密钥仅使用一次的设想[8]。尽管这种“一次一密钥”系统只是一种理想的极限情况,在实际应用中很难实现,但在密码学领域依然是密码算法设计者应遵从的一个指导思想。常见的基于单参数的混沌信号加密,其参数一般固定不变,不符合 Shannon 提出“一次一密钥”加密系统的设计理念,也是安全性能得不到保证的原因之一。例如文献[11]通过分析

证明了文献[1]设计的图像加密算法的有效密钥量达不到预期的目标,在已知图像攻击下是不安全的。如果将混沌系统中的某一组便于调节的参数视为密钥,每加密一次就改变这组参数一次,则符合“一次一密钥”的设计思想。本文提出的高维广义猫映射图像加密算法在单独应用时虽然较低维猫映射具有更大的密钥空间,其安全性能并无实质性改善,但可以作为加密系统的一个子模块用于对多帧图像分时并随机地共用某一组切换参数来实现图像或视频的加密。虽然由于不受限的图像帧数将远大于有限的可选切换参数的数量而不能真正实现对每一帧图像的“一次一密钥”加密,但与固定参数的混沌视频图像加密相比,其安全性能将得到很大的提高。



(a) 一轮二维猫映射 (b) 一轮四维猫映射

图 3 经猫映射图像灰度值扩散变换后的灰度直方图

Fig. 3 Histograms of the images with diffusing gray values by cat maps

4 结 语

本文根据混沌动力学理论首次构造了一种基于四维广义猫映射的图像加密算法,将三维广义猫映射扩展至四维广义猫映射,并可基于该扩展模式很容易地将广义猫映射扩展至更高维。对三类不同维数广义猫映射的基本动力学特征进行了比较。通过将图像的像素坐标和灰度值作为广义猫映射的初始值,映射参数和迭代次数作为密钥实现图像加密,该加密算法具有像素坐标置换及灰度值扩散等加密系统的基本要素。与常见的低维混沌猫映射相比,基于四维广义猫映射的图像加密算法具有更大的密钥空间及更高的加密速度,可以作为常规网络或中高速无线传感器网络的图像、数据块或视频加密系统的一个子模块,通过对多帧图像分时并随机地共用某一组切换参数来实现图像加密。

参考文献:

[1] Chen G R, Mao Y, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos Solitons & Fractals, 2004, 21(2):749-761.

[2] Masuda N, Jakimoski G, Aihara K, et al. Chaotic block ciphers: from theory to practical algorithms [J]. IEEE Transactions on Circuits and Systems - I: Regular Papers, 2006, 53(6): 1341-1352.

[3] 罗松江,丘水生. 基于时空混沌和 S 盒的彩色图像加密算法[J]. 电路与系统学报,2010,15(3):117-122.
Luo Songjiang, Qiu Shuisheng. Color image encryption algorithm based on spatiotemporal chaos and S-box [J]. Journal of Circuits and Systems, 2010,15(3):117-122.

[4] 张琼,沈民奋,翟懿奎. 基于三维混沌猫映射图像加密算法的改进[J]. 系统工程与电子技术,2007,29(9):1568-1572.
Zhang Qiong, Shen Minfen, Zhai Yikui. Improving image encryption method based on three-dimensional chaotic cat map[J]. Systems Engineering and Electronics, 2007,29(9):1568-1572.

[5] 张爱华,江中勤. 基于 Logistic 映射的混沌图像加密算法的改进[J]. 南京邮电大学学报,2009,29(4):69-73.
Zhang Aihua, Jiang Zhongqin. Improving for chaotic image encryption algorithm based on Logistic mapping[J]. Journal of Nanjing University of Posts and Telecommunication, 2009,29(4):69-73.

[6] 禹思敏. 混沌系统与混沌电路—原理、设计及其在通信中的应用[M]. 西安:西安电子科技大学出版社,2011.
Yu Simin. Chaotic systems and chaotic circuits: principle, design and its application in communications[M]. Xi'an: Xidian University Publishing House,2011.

[7] Arnold E A, Avez A. Ergodic problems of classical mechanics[M]. New Jersey: Benjamin, W A,1968.

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

[9] 陈关荣,汪小帆. 动力系统的混沌化—理论、方法和应用[M]. 上海:上海交通大学出版社,2006.

[10] 曹光辉,胡凯,佟维. 基于 Logistic 均匀分布图像置乱方法[J]. 物理学报,2011, 60(11):1-8.
Cao Guanghui, Hu Kai, Tong Wei. Image scrambling based on Logistic uniform distribution [J]. Acta Physica Sinica, 2011, 60(11):1-8.

[11] 郭建胜,张锋. 一种图像加密算法的等效密钥攻击方案[J]. 电子学报,2010,38(4):781-785.
Guo Jiansheng, Zhang Feng. An equivalent key attack on an image cryptosystem [J]. Acta Electronica Sinica, 2010,38(4):781-785.

(责任编辑 杨小丽)