文章编号 1004-924X(2004)02-0200-06

一种基于混沌映射的图像加密算法

樊春霞, 姜长生
(南京航空航天大学 自动化学院, 江苏 南京 210016)

摘要:应用离散混沌序列易于生成,对初值敏感以及具有白噪声的统计特性,设计了一种"仿 Feistel 网络结构"的数字图像加密/解密算法。该算法的所有密钥都由不同的混沌动力系统产生,增加了破译难度。算法中的置换和替代操作,组成了具有良好密码特性的 SP 网络结构,置换也受密钥控制,增加了算法的复杂性。加密操作的输出结果依赖于密钥的强非线性耦合,增强了安全性。在"仿 Feistel 网络结构"的每次迭代操作中,都能够对所有的明文进行加密,提高了加密效率。最后,以 Matlab 中的图像 Pout 为例进行了仿真试验,结果表明,该算法具有良好的安全性和效率。

关 键 词:图像加密; 离散混沌系统; SP 网络
中图分类号:TP391.4 **文献标识码**:A

Image encryption based on discrete chaotic maps

FAN Chun-xia, JIANG Chang-sheng

(College of Automatic Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract: Discrete chaos is used to generate cipher systems because it is easy to create, sensitive to initial value and similar to white noise of statistical nature. A "quasi-Feistel network" algorithm is designed using discrete chaotic maps for image encryption/decryption. All secret keys of the algorithm are generated by different chaotic maps, and this improves difficulty of decryption. Permutation and substitution consist of SP networks with good cipher performance. Permutation is also controlled by cipher to improve algorithm complexity. Safety is enhanced by the output of encryption which strongly depends on nonlinear coupled secret keys. All of white text is encrypted during each iteration of "quasi-Feistel network", and this improves the encryption efficiency. Finally, a simulation test is conducted by taking the image Pout in Matlab as an example, and the simulation results show that the algorithm proposed possesses perfect safety and efficiency.

Key words: image encryption; discrete chaotic maps; SP network

1 引 言

近年来,由于通讯技术的飞速发展,越来越多的领域需要传送数字图像信号,如多媒体系统、宽带网、有线电视、电话会议系统等。这些图像数据很多是需要发送方和接收方进行保密通信的,因此信息的安全问题越来越重要。为了安全传送这些需要保密的信息,设计了很多加密方法。对于数字图像,有两种保护技术:一种是数字水印技

收稿日期:2003-12-16;**修订日期**:2004-02-24.
基金项目:国家自然科学基金项目(No. 60174045);航空第一集团资助项目(No. 01D52025)

术,通过在图像中嵌入数字信息,达到保护版权的目的。但是,这种保护方法不改变图像的可见性,不适合用来保护需要保密传输的图像。另一种技术就是图像加密技术,通过加密操作,改变图像的可见性,使原来的图像成为不可辨别的。随着通讯技术的发展,图像加密技术将会有越来越广泛的应用前景。

图像加密技术有 3 种思想方法:灰度值替代,像素位置变换以及二者的组合。灰度值替代是利用密钥改变源图像的灰度,可以逐点改变[1],也可以把源图像分成几块,逐块进行替代操作[2];像素位置变换是改变源图像中像素点的排列顺序,Fridrich 等利用混沌映射来改变像素位置[3];组合方法是加密过程中既有灰度值替代,又有像素位置的变换[4-5]。在所有的加密算法中,都需要一个随机数产生器。由于离散的混沌系统容易实现,比如可以用神经网络来实现[6-7],具有良好的统计特性,从而可以作为随机数发生器。混沌系统对参数和初始条件极其敏感,如果把系统的参数或初值作为密钥,混沌系统就成为一个具有优良密码特性的密码系统[8]。混沌系统在二维相平面内的不规则性使得混沌系统更适合用于图像加密。

本文应用离散混沌动力系统,针对图像数据的存储特点,设计了一种图像加密算法。这是一种把灰度值替代和像素位置变换相结合的方法。利用 Logistic 映射产生密码流,改变源图像的灰度值;利用指数混沌和正弦迭代混沌映射,借鉴密码学中的 Feistel 网络,构造置换方式,从而改变像素点的位置。Feistel 网络每操作一次,只能对一半的明文进行加密,从而效率较低。这里构造的置换方式仅进行一次置换操作,就能够对所有的明文进行加密,从而提高了加密效率。所有的密钥都由离散混沌映射产生,因此算法没有因为增加密钥设置而影响加密/解密的效率和速度。由于利用了混沌映射,增加了破译难度,提高了安全性。分析和仿真结果都表明,该算法能够有效地实现对数字图像数的加密/解密。

2 混沌系统

混沌现象是一种有界的内在的随机过程,具有时间遍历性,这种过程既非周期性,又不收敛。任意相近的两点经过若干次混沌迭代之后,都会呈现指数发散,所以很难预测混沌系统的初值和参数。另外,混沌轨道极其不规则,经过系统局部扩展、压缩、折叠之后,系统的输出类似于随机噪声。这些特点均使混沌映射很适用于设计密码系统。

首先考虑一类非常简单却被广泛研究的混沌映射 Logistic 映射:

$$x(k+1) = px(k)(1-x(k)), \quad (1)$$

其中,$0 \leq p \leq 4$ 为分岔参数,$x(k) \in (0,1)$ 是系统的状态变量。当 $3.569\,945\,6\cdots < p \leq 4$ 时,Logistic 映射工作于混沌状态。此时,由初值 $x(0)$ 在 Logistic 映射的作用下产生的序列 $\{x(k); k = 0,1,2,\cdots\}$ 是非周期,不收敛,对初值敏感的序列。当分岔参数 $p = 4$ 时,该序列的概率分布函数是

$$\rho(x) = \begin{cases} \dfrac{1}{\pi\sqrt{x(1-x)}} & 0 < x < 1 \\ 0 & else \end{cases}, \quad (2)$$

由式(2)可以看出,Logistic 映射不满足一致分布[9]。为了得到随机性更好的满足一致分布的随机序列,将式(1)做变换

$$y(n) = \frac{2}{\pi}\sin^{-1}(\sqrt{x(n)}), \quad n = 1,2,3,\cdots, \quad (3)$$

变量 y 的分布函数

$$F\{y \leq Y\} = F\{x \leq \sin^2(\frac{\pi Y}{2})\} = \int_0^{\sin^2(\frac{\pi Y}{2})} \rho(x)\,\mathrm{d}x = \int_0^{\sin^2(\frac{\pi Y}{2})} \frac{1}{\pi\sqrt{x(1-x)}}\,\mathrm{d}x = Y, \quad (4)$$

因此,变量 y 的概率分布函数为

$$\rho(Y) = \frac{\mathrm{d}F}{\mathrm{d}Y}\{y \leq Y\} = 1, \quad (5)$$

即式(3)在(0,1)区间满足一致分布。

指数混沌系统

$$x(n+1) = a^{x(n)} \bmod 1, \quad (6)$$

其中 $1 < a \in R$,系统初值 $x(0) \in R$,且 $0 < x(0) < 1$,mod 表示取余运算。该系统是一个混沌系统,其 Lyapunov 指数是 $\ln a > 0$。

正弦迭代混沌系统

$$x(n+1) = \sin^2(b\arcsin\sqrt{x(n)}), \quad (7)$$

其中,$1 < b \in R$,系统初值 $x(0) \in R$,且 $0 < x(0) < 1$。由式(7)产生的系统的 Lyapunov 指数是

$\ln b > 0$,因而是一个混沌系统。

如果以系统的初值和参数以及迭代次数为密钥来设计密码,混沌映射能够组成很好的密码系统。下面讨论混沌映射在数字图像加密中的应用。

3　置换设计

考虑一幅大小为 $M \times N$,具有 L 级灰度的图像。

置换能够有效打乱明文之间的统计特性,从而有效地抵御统计和预测分析。在现代密码系统中经常采用的 Feistel 网络是一种有效的置换方式。迭代形式的 Feistel 网络将一分组明文 (X_1, X_2) 变换为

$$X_1(n+1) = X_2(n)$$
$$X_2(n+1) = X_1(n) \oplus F(X_2(n), K), \quad (8)$$

其中,F 为非线性函数;K 为密钥;$\oplus$ 为异或操作符号;$n = 1,2,\ldots,16$ 为迭代轮数。这种网络结构的一个缺点就是每迭代一轮,只能对一半的明文进行加密,效率较低。

受 Feistel 网络的启发,设计了一种网络结构,每一次迭代都能够对所有的明文进行加密,提高了效率。不妨称这种结构为"仿 Feistel 网络":

$$i' = \mathrm{mod}(i + f(j, k_{1n}), M)$$
$$j' = \mathrm{mod}(j + g(i', k_{2n}), N), \quad (9)$$

其中,(i', j') 分别表示源图像 (i, j) 位置经过置换之后的位置;$M \times N$ 表示图像的大小;$f(\cdot,\cdot)$ 和 $g(\cdot,\cdot)$ 表示非线性函数,与密钥 k_1 和 k_2 相关;$i = 0,1,2,3,\ldots,M$,$j = 0,1,2,3,\ldots,N$,k_{1n} 和 k_{2n} 表示第 n 轮迭代的密钥。这里采用混沌动力系统设计密钥,使得非线性函数 f 和 g 对各自的自变量敏感,增强系统加密效果。选择指数混沌系统(6)产生密钥 k_1,正弦混沌迭代映射(7)产生密钥 k_2。为了提高密钥的不可预测性,混沌映射迭代 t 次之后,作为密钥,从而迭代次数也是子密钥之一。非线性函数 f 和 g 分别选择如下

$$f(j, k_{1n}) = j + \mathrm{mod}(\mathrm{round}(N \cdot k_{1n}), N)$$
$$g(i', k_{2n}) = i' + \mathrm{mod}(\mathrm{round}(M \cdot k_{2n}), M), \quad (10)$$

其中,round(·)表示四舍五入运算;mod(x, y) 表示取 x/y 的余数。分别选择系统(6)和(7)的参数 a 和 b,迭代初值 $k_1(0)$ 和 $k_2(0)$,迭代次数 t_1 和 t_2 作为置换部分的密钥

$$kp = (a, k_1(0), t_1, b, k_2(0), t_2), \quad (11)$$

可以看出,式(9)不是一个一一映射,其逆映射不存在,不可能对加密之后的图像进行解密运算。为此,需要计算行变换矩阵 TR 和列变换矩阵 TC,

$$\mathrm{TR}(i', j') = \frac{i + f(j, k_{1n})}{M}$$
$$\mathrm{TC}(i', j') = \frac{j + f(i', k_{2n})}{N}, \quad (12)$$

从而得到置换算法(9)的逆映射

$$j = j' - \mathrm{TC}(i', j') \cdot N - g(i', k_{2n})$$
$$i = i' + \mathrm{TR}(i', j') \cdot M - f(j, k_{1n}), \quad (13)$$

假设接收方已知图像的大小,因此可以根据密钥自行计算出变换矩阵 TR 和 TC。至此,应用离散混沌系统设计的置换操作已经完成。从算法中可以看出,利用混沌系统产生密钥,可使密码对初值和参数充分敏感,从而设计的"仿 Feistel 网络"充分依赖混沌系统参数,初值以及混沌序列的迭代次数。

4　像素灰度替代设计

替代是通过密钥来改变图像的灰度值,从而改变图像的可视性,实质上是在灰度空间的置换操作。假设 $I(i, j)$ 和 $I'(i, j)$ 分别表示源图像和替代之后 (i, j) 位置的灰度值,其中 $1 \le i \le M$,$1 \le j \le N$。要设计映射 $f: I(i, j) \to I'(i, j)$ 来完成灰度替代。

为了使替代操作后的灰度 $I'(i, j)$ 具有不可预测性,能够抵御破译攻击,采用混沌序列来完成替代操作:

$$I'(i, j) = I(i, j) + K(i, j) \bmod L, \quad (14)$$

其中,$K(i, j)$ 由混沌动力系统(3)产生,L 表示源图像的灰度等级。

为了将式(3)产生的序列映射到[0, $L-1$]区间的整数值,设计如下的映射:

$$z(n) = \mathrm{round}((L-1)\, y(n)), \quad n = 1,2,\ldots,T, \quad (15)$$

其中,$T > M \times N$。为了增加密文的安全性,不用混沌序列起始阶段来加密。从式(15)产生的一维序列中按照一定规律截取 $M \times N$ 个元素,组成 $M \times N$ 矩阵形式,并赋给 $K(i, j)$。所用的密钥为 ks

$= (x(0), t_3)$,其中 $x(0)$ 表示产生混沌序列的初值,t_3 表示在混沌序列中截取密码的初始位置。

相应的解密运算为

$$I(i,j) = I'(i,j) - K(i,j) \bmod L . \quad (16)$$

5 加密/解密算法

在第 2 部分和第 3 部分分别完成了置换和替代变换。这样的变换重复进行 n 次,能够实现很好的加密效果。整个算法过程如下:

加密过程:对源图像进行置换变换,同时保留变换过程中的变换阵,然后进行替代变换,重复进行 n 次。

解密过程:将接收到的图像进行替代变换的反变换,然后进行置换变换的逆变换,就得到了源图像,重复进行 n 次。

替代过程,相当于一个混淆过程,而置换过程相当于一个扩散过程,这样设计的算法构成了密码学中的 SP 结构。取 3 个不同的混沌结构来设计密钥,是为了增加破译难度。

6 算法分析

6.1 安全性分析

从算法的结构上看,整个算法由 2 部分组成:置换和替代。这与密码学中的 SP 网络结构相似,不同之处在于 SP 网络结构的置换部分不受密钥控制,而在上述算法中,置换部分也受密钥的控制,这增加了算法的复杂性。

从混沌动力学的角度来分析算法,由于混沌动力系统对初值和参数都很敏感,具有"差之毫厘,失之千里"的特性。离散混沌系统对于不同初值的输出结果以指数形式发散。本文所用的混沌映射的 Lyapunov 指数分别是:系统(3)的 Lyapunov 指数是 $\ln 2 > 0$;系统(6)和(7)的 Lyapunov 指数分别是 $\ln a > 0$ 和 $\ln b > 0$。这样,在置换和替代逆变换时,即使密钥有一个细小差别,解密结果都会与源图像相差很大。另外,混沌系统具有拓扑共轭性,初值和参数相差很小的时候,也会使误差很快地传递到整个吸引域相空间上,这也会增加非法攻击者的破译难度。迭代次数也作为密钥,那么不同的迭代次数产生不同的密码流,也增加了破译难度。

从一次一密的角度讲,加密者可以随意选择密钥,这有利于密码的安全性。

6.2 效率分析

算法中采用的都是迭代映射形式,适合计算机快速计算。加密图像之前,不需要对图像进行预处理,节省了时间。采用混沌映射产生密码流,简单快速且具有非线性,对系统初值,参数以及迭代次数具有敏感性。算法的置换设计,具有非线性强耦合特性,所以算法的迭代轮数不需要太多,就可以提高加密效率。

文中所采用的置换和替代部分都符合模块化设计,能够很方便的实现。

7 仿真实例

选择 Matlab 中的图像 Pout 为仿真对象,图像大小为 291 ×240,灰度等级 $L = 256$。密钥参数分别选择为 $kp = (5, 0.3, 1\,000, 3, 0.5, 800)$ 和 $ks = (0.5, 500)$。进行一轮迭代加密,其仿真结果如图 1～图 4 所示。加密 4 轮之后,所得图像如图 5。

图 1 源图像

Fig. 1 Source image

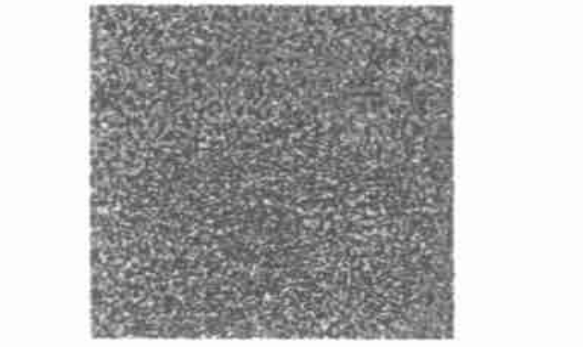

图 2 一次置换之后的图像

Fig. 2 Image after one time permutation

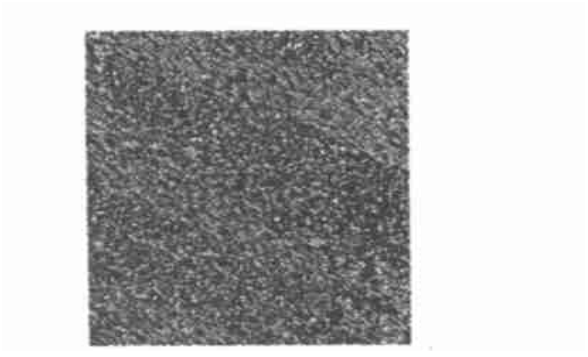

图 3　一次替换之后的图像

Fig. 3　Image after one time substitution

图 4　置换与替代操作各一次之后的解密图像

Fig. 4　Decryption image after one time permutation and substitution

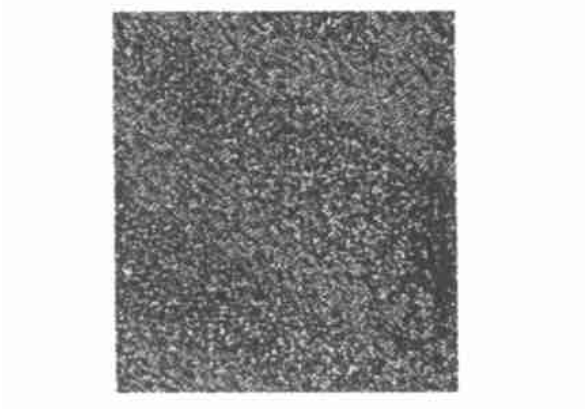

图 5　四轮加密之后的图像

Fig. 5　Image after four times' encryption

所示。如果解密密钥选择为 $kg = (0.500\ 1, 500)$, kp 与加密时相同,解密图像如图 6 所示。从仿真结果可以看出,混沌映射的初值的微小差别都会造成不能正确解密,这与上面的分析结果相一致。

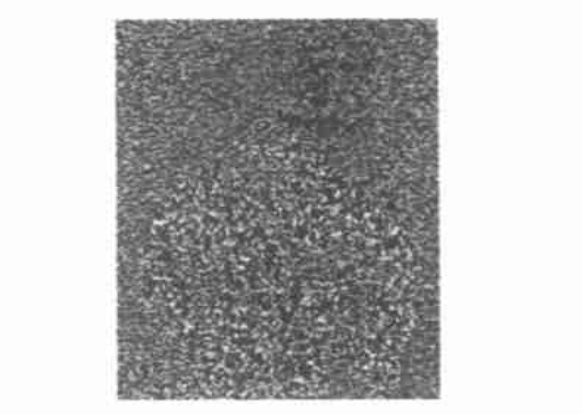

图 6　错误密钥解密图像

Fig. 6　Decryption image of wrong keys

8　结　论

提出了一种基于离散混沌映射的图像加密算法。借鉴 Feistel 网络结构,设计了一种"仿 Feistel 网络"结构,能够在每次迭代中对所有的明文进行加密,提高了加密效率。整个算法结构具有密码学中的 SP 结构,经过几次迭代之后能够对明文进行有效的混淆和扩散,而且在每次迭代过程中,混淆和扩散都依赖于密钥的强非线性耦合,增强了安全性。由于所有的密码流都是由混沌映射产生,所以置换和替代的输出结果都强烈依赖于密钥的选择,因而要求用户能够知道准确密钥,才能得到正确的解密结果,否则不可能得到有效的解密结果,该算法具有良好的安全性。另外,从理论上讲,算法的密钥空间很大,是无穷大,因此可以满足一次一密的密钥体制要求。

参考文献:

[1] 张晓华,刘芳,焦李成. 一种基于混沌序列的图像加密技术[J]. 中国图像图形学报, 2003,8A(4):374-378.
ZHANG X H, LIU F, JIAO L CH. An encryption arithmetic based on chaotic sequence[J]. *J Image and Graphics*, 2003,8A(4): 374-378. (in Chinese)

[2] NETO L G, SHENG Y L. Optical implementation of image encryption using random-phase encoding[J]. *Opt Eng*, 1996,35(9): 2459-2463.

[3] FRIDRICH J. Image encryption based on chaotic maps[C]. *IEEE Int Conf System*, Man and Cybernetics, Computational Cybernetics, Simulations, 1997,1117-1120.

[4] CHUANG T J, LIN J C. A new multi-resolution approach to still image encryption[J]. *Pattern Recognition*. 1999,9(3):431-436.

[5] 李昌刚,韩正之,张浩然. 一种随机密钥及"类标准映射"的图像加密算法[J]. 计算机学报,2003,26(4):465-470.
LI CH G, HAN ZH ZH, ZHANG H R. An image encryption algorithm based on random key and quasi-standard map[J]. *Chinese Journal of Computers*, 2003,26(4):465-470. (in Chinese)

[6] 石文效,荆涛,杨怀江. 混沌序列的神经网络实现[J]. 光学 精密工程,2000,8(3):231-233.
SHI W X, JING T, YANG H J. Chaos generation based on neural network[J]. *Optics and Precision Engineering*, 2000,8(3): 231-233. (in Chinese)

[7] 荆涛,宋健中,杨怀江,等. 基于复合混沌映射的神经网络模型[J]. 光学 精密工程, 1999,7(1):39-45.
JING T, SONG J ZH, YANG H J, *et al*. The model of neural network based on the compound chaotic map[J]. *Optics and Precision Engineering*, 1999,7(1): 39-45. (in Chinese)

[8] ZBIGNIEW K, JANUSZ S. Application of discrete chaotic dynamical systems in cryptography-DCC method [J]. *International Journal of Bifurcation and Chaos*, 2000,10(8):1867-1874.

[9] 陈式刚. 映像与混沌[M]. 北京: 国防工业出版社. 1992. 101-103.
CHEN SH G. *Map and chaos* [M]. Beijing: National Defence Industry Publishing House. 1992. 101-103. (in Chinese)

作者简介:樊春霞(1972 -),女,吉林梨树人,南京航空航天大学自动化学院博士研究生,主要研究方向为混沌系统应用。
E-mail:fcx@zjfc.edu.cn