文章编号:1001 - 9081(2008)02 - 0434 - 03

一种基于混合反馈的混沌图像加密算法

高 洁[1,2],袁家斌[2],徐 涛[2],齐艳珂[1]
(1. 郑州航空工业管理学院 计算机科学与应用系,郑州 450015; 2. 南京航空航天大学 信息科学与技术学院,南京 210016)
(gjlw0@hotmail.com)

摘 要:针对现有基于混沌分组密码的图像加密算法中,扩散函数扩散速度慢、需要多轮迭代才能抵抗差分攻击的缺点,提出了一种新的基于密文和输出混合反馈的混沌图像加密算法。该算法利用密文扰动混沌系统的初始值,既改善了数字混沌的退化,又能使扩散函数具有非常快的扩散速度。经过实验验证,该算法只需正反两轮迭代,就能达到较高的安全性和较快的加解密速度。

关键词:图像加密;混合反馈;混沌分组密码
中图分类号: TP309.7 **文献标志码**:A

New chaotic image encryption algorithm based on hybrid feedback

GAO Jie[1,2], YUAN Jia-bin[2], XU Tao[2], QI Yan-ke[1]
(1. *Department of Computer Science and Application, Zhengzhou Institute of Aeronautical Industry Management, Zhengzhou Henan* 450015, *China*; 2. *College of Information Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing Jiangsu* 210016, *China*)

Abstract: Aiming at the defects of diffusion function with lower diffusing speed and needing multiple round iteration to resist differential attack in the image encryption algorithm based on chaotic block cipher, a new chaotic image encryption algorithm based on output-cryptograph mixed feedback was proposed. It can improve the degradation of digital chaotic and diffusing speed of diffusion function through perturbating initial value of chaotic system with ciphertext. Experimental results show that the iterative algorithm only requires a positive iteration and an inverse iteration to achieve higher levels of security and faster encryption speed.

Key words: image encryption; hybrid feedback; chaotic block cipher

0 引言

混沌映射用于分组密码,实际上就是应用混沌的混迭特性来快速地置乱和扩散数据。一般地,在设计分组密码时利用置乱、替换、扩散等方法设计单轮加密变换 E,然后,通过对该加密变换 E 进行多轮迭代达到扩散和混淆明文的目的。图像置乱可分为图像像素位置置乱和对图像灰度值进行置乱,其中像素位置置乱的运算量比较大,要求对图像的所有像素点遍历,同时还要考虑地址之间的相关性。而像素灰度值加密易实现、运算量小、效果较好。所以像素灰度值加密算法更为普遍。在基于混沌的图像加密算法中,现有的很多灰度值混淆和扩散的方法[1-5]都是基于混沌分组密码系统中的一个环节,单独使用需要较大的迭代次数,扩散速度较慢。本文提出并实现了一种新的基于输出和密文混合反馈的混沌分组密码的图像加密算法,算法不需要置乱环节,利用混沌本身的混迭特性,采用输出和密文混合反馈的方法,既改善了数字混沌系统的退化,又能使扩散速度非常快,只需正反两轮迭代便能达到较高的安全性。

1 一维分段线性混沌映射

基于文献[6]的分析选择如下的一维分段线性混沌映射[7,8]:

$$x(k+1)=f(x(k),p)=\begin{cases}x(k)/p, & 0<x(k)<p\\ (x(k)-p)/(0.5-p), & p\leqslant x(k)<0.5\\ (1-p-x(k))/(0.5-p), & 0.5\leqslant x(k)<1-p\\ (1-x(k))/p, & 1-p\leqslant x(k)<1\end{cases}\tag{1}$$

其中,p 是控制参数,且满足 $0<p<0.5$。将其离散化到整数域,可得:

$$x(k+1)=F(x(k),p)=\begin{cases}\left\lfloor\dfrac{2^{n_0}\cdot x(k)}{p}\right\rfloor, & 0<x(k)<p\\ \left\lfloor\dfrac{2^{n_0}\cdot(x(k)-p)}{2^{n_0-1}-p}\right\rfloor, & p\leqslant x(k)<2^{n_0-1}\\ \left\lfloor\dfrac{2^{n_0}\cdot(2^{n_0}-x(k)-p)}{2^{n_0-1}-p}\right\rfloor, & 2^{n_0-1}\leqslant x(k)<2^{n_0}-p\\ \left\lfloor\dfrac{2^{n_0}\cdot(2^{n_0}-x(k))}{p}\right\rfloor, & 2^{n_0}-p\leqslant x(k)<2^{n_0}\end{cases}\tag{2}$$

其中,$\lfloor x\rfloor$ 是将 x 圆整到与 x 距离最近的整数,$x(k)$ 的变化范围是从 0 到 $2^{n_0}-1$,p 满足 $0<p<2^{n_0}-1$。考虑到现在的计算机通常是 32 位的,故 $n_0=32$。当 n_0 一定,产生的混沌序列与计算机的速度无关,这克服了连续混沌映射的缺点。但是,圆整化处理,是个有损过程,可能带来混沌特性的降质,如产生循环[9]。根据文献[6]的分析,采用同时扰动混沌系统的控制参数和变量的方法改善该数字化混沌退化问题。

收稿日期:2007 - 09 - 05;**修回日期**:2007 - 11 - 05。

作者简介:高洁(1978 -),女,河南新乡人,讲师,硕士研究生,主要研究方向:图像处理、信息安全、视频编码; 袁家斌(1968 -),男,江苏兴化人,副教授,主要研究方向:信息安全、网络技术; 徐涛(1962 -),男,重庆人,教授,主要研究方向:计算机视觉、图像处理、分布式计算;齐艳珂(1981 -),女,河南周口人,助教,硕士研究生,主要研究方向:网格、网络技术。

2　输出和密文混合反馈混沌分组密码设计

2.1　混沌密码系统设计

由于混沌系统是确定性的,混沌理论中一些工具可以用来辨别混沌系统,一旦密码分析者获得了足够的混沌轨道信息,就可能利用这些信息降低获得密码系统密钥的复杂度。输出和密文混合反馈混沌密码系统可以弥补上述缺陷,使密码分析者不能从密文,或者明文—密文对获得足够的混沌轨道来攻击密码系统。其结构如图 1 所示。

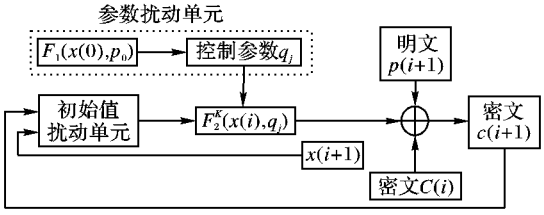


图 1　输出—密文混合反馈混沌分组密码

设图像像素矩阵为 $\boldsymbol{N} = m \times n$。图中 F_1,F_2 都是式(2)所示的同一个混沌映射,$x(0)$ 为 F_1 的初始值,p_0 为 F_1 的参数,q_j 为 F_2 的参数,$q(j) = \lfloor x(j)/2 \rfloor$,$x(j)$ 为 F_1 产生的混沌序列 $(j = 1,2,\cdots,N)$;$p(i+1)$ 为明文(图像的第 $i+1$ 个像素值),$i = 1,2,\cdots,N-1$;$c(i+1)$ 为密文(加密后图像的第 $i+1$ 个像素值),$x(i+1)$ 为混沌系统的输出值。

2.2　加密函数和解密函数

输出—密文混合反馈混沌分组密码以图像一个像素(8 bit)为单位,对每一个图像的像素进行逐位异或运算,其数学表达式如下:

加密:

$$c(i+1) = p(i+1) \oplus [F^K((c(i) + x(i)) \bmod (2^{n_0} - 1), q_j) \bmod 256] \oplus c(i) \tag{3}$$

解密:

$$p(i+1) = c(i+1) \oplus c(i) \oplus [F^K((c(i) + x(i)) \bmod (2^{n_0} - 1), q_j) \bmod 256] \tag{4}$$

2.3　加解密步骤

加密算法步骤如下:

步骤 1:密钥的产生。选择一个 192 bit 的序列作为密钥,将这 192 bit 分成 6 组,每组为 32 bit。将这 6 组比特流分别映射为 6 个整数:$k_1,k_2,\cdots,k_6$。

步骤 2:产生扰动系统参数的序列 $q_j(j = 1,2,\cdots,N)$。令 $x(0) = k_1$,$p_0 = k_2$,其中 $x(0)$ 为 F_1 的初始值,p_0 为 F_1 的参数。为了保持混沌序列 q_j 有较好的混沌特性,取 F_1 迭代 1 000 次以后的 N 个数除以 2 再取整得到的数作为 q_j 序列($q_1,q_2,\cdots,q_N$)。

步骤 3:选择初始向量。将明文图像像素矩阵变为 $1 \times N$ 的矩阵 $\boldsymbol{p}$。在 F_1 迭代产生的序列中任意选择(比如选择迭代 100 次)一个数作为初始向量 $\boldsymbol{X}$,将明文图像的第一个像素 $p(1)$ 与($\boldsymbol{X}$ mod 256)进行逐位异或运算得到 $c(1)$。

步骤 4:令 $x(1) = k_3$,$x(1)$ 为 F_2 的初始值。将 $x(1)$、$c(1)$、$p(i)$、$q(i)$ 代入式(3),对明文图像数据进行第一轮加密,得到第一轮加密后的图像数据。

步骤 5:令 $x(0) = k_4$,$p_0 = k_5$,$x(1) = k_6$,重复步骤 1 ~ 4,对图像数据进行第二轮加密,在第二轮加密中步骤 3 略有不同,为了使加密算法对明文非常敏感,第二轮迭代必须从最后一个像素开始,然后是倒数第二个像素,最后一直到第一个像素。

步骤 6:将两轮加密后的图像数据 $1 \times N$,变回到 $m \times n$ 的图像数据矩阵。

解密算法和加密算法相似,按式(4)进行。

3　安全性分析与实验结果

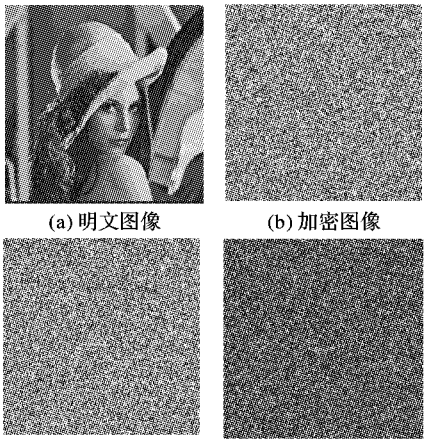
与其他图像加密方案相比,本算法具有高的安全性,能抵抗诸如已知明文攻击、统计分析、差分攻击等多种攻击,并具有大的密钥空间,更为重要的是,在具有高安全性的同时,该算法只需要两轮迭代,加解密速度也非常快。

1)密钥空间分析。

本加密方案为 192 bit 的加密,密钥空间达 $2^{192} \approx 10^{115}$。本方案采用的精度是 32 bit,如果采用 64 bit 精度,密钥空间可达。显然,对于如此大的密钥空间采用穷举搜索法进行攻击是不现实的。

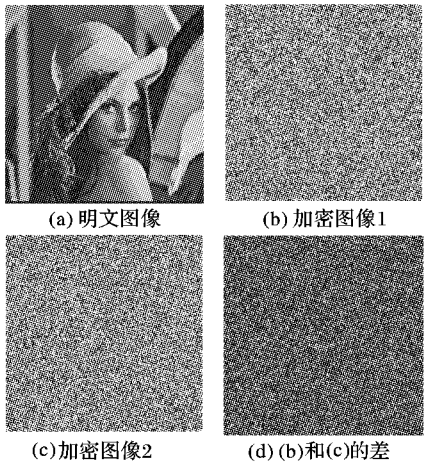
2)密钥敏感性测试。

(1)对密钥极其敏感,设加、解密密钥为:[123,456,789,369,258,147],对其中任一个子密钥,即使相差 1 都不能够正确解密。图 2 中图(c)是解密密钥为[122,456,789,369,258,147]的解密图像,图(d)为(b)和(c)两图之差值,有 99.61% 的像素都不相同。对另外五个子密钥的测试结果和对第一个密钥测试结果类似,这里就不给出图例。



(a) 明文图像　(b) 加密图像　(c) 错误密钥解密图像　(d) b和c两图的差

图 2　密钥敏感性测试一



(a) 明文图像　(b) 加密图像1　(c)加密图像2　(d) (b)和(c)的差

图 3　密钥敏感性测试二

(2)密钥有很小的改变所得到的加密图像有很大的差异,图 3(a)是使用密钥[123,456,789,369,258,147]的加密图像,(b)是使用密钥[122,456,789,369,258,147]的加密图像,(c)是两个密图之差,有 99.63% 的像素都不同。改变另外五个子密钥会得到相似的结果,这里就不给出图例。

3)差分攻击(明文敏感性测试)。

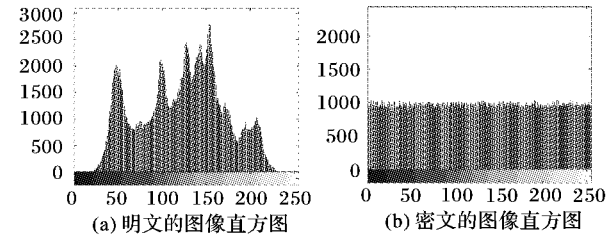
攻击者通常会通过改变图像中很小的一点，比如只改变一个像素，来观察加密后图像的变化情况，通过这种方式，攻击者可能破解加密图像。

实验中测试了将明文图像第一个像素138改为137后的密文之差：有99.59%的密文像素不同。改变明文图像任意像素的任一比特位都会得到相似结果。这使得已知明文攻击不可行。实验结果与图2、图3类似。

4)统计攻击

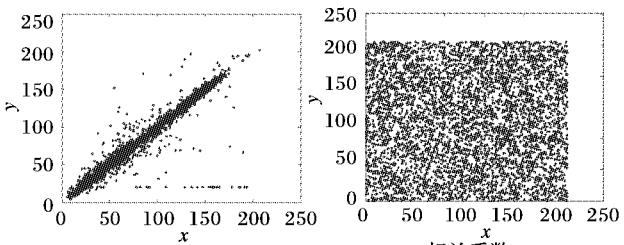
(1)加密图像的直方图

实验中选择了多幅大小为500×500的256级灰度图像，比较它们在加密前后的直方图。图4是其中的一个结果，可以看出，加密后图像的直方图与原始图像的直方图有很大不同，且非常均匀。



(a)明文的图像直方图 (b)密文的图像直方图

图4 500×500 Lena图像明文和密文的直方图



(a)相关系数0.9683 (b)相关系数0.0113

图5 明文图像和密文图像相邻两点相关性分析结果

(2)相邻像素的相关性

图像中相邻两个像素的相关性是很大的，为了破坏统计攻击，必须使相邻两个像素的相关性降低。实验中在加密图像和原始图像中各随机选择了20 000对相邻像素点对(包括水平、垂直和对角方向的相邻点)，记为(x_i, y_i)，其中x_i, y_i分别代表第i对像素的两个像素值。计算这20 000对像素灰度值之间的线性相关系数。以相邻两像素灰度值为x，y坐标，得到加密前后相邻两点的相关性分析结果如图5所示。

通过实验可以看出，加密前的图像像素之间具有强相关性，经过加密后这种相关性已经完全被破坏了。

4 结语

本文提出并实现了一种新的基于输出和密文混合反馈的混沌分组密码的图像加密算法。算法不需要置乱环节，利用混沌本身的混迭特性，采用输出和密文混合反馈的加密系统对图像进行加密，既改善了数字混沌的退化又能使扩散函数具有非常快的扩散速度。大量的实验研究证明，该算法实现简单，只需正反两轮迭代，就能达到高的安全性和较快的加解密速度，能够抵抗蛮力攻击、差分攻击、统计攻击等多种密码攻击。

参考文献：

[1] 茅耀斌. 基于混沌的图像加密与数字水印技术研究[D]. 南京：南京理工大学, 2003.

[2] FRIDRICH J. Symmetric ciphers based on two-dimensional chaotic maps[J]. Int. J. Bifurcation and Chaos, 1998, 8(6): 1259 - 1284.

[3] 廉士国. 多媒体快速加密算法研究[D]. 南京：南京理工大学, 2005.

[4] 廉士国, 王执铨. Standard映射及其三维扩展在多媒体加密中的应用[J]. 东南大学学报, 2003, 33(A): 90 - 94.

[5] MAO Y, CHEN G, CHUI C K. A symmetric image encryption scheme based on 3D chaotic Cat maps[J]. Chaos, Solitons Fractals, 2004, 21(1): 749 - 761.

[6] 李树钧. 数字化混沌密码的分析与设计[D]. 西安：西安交通大学, 2003.

[7] PAPADIMITRIOU S, BOUNTIS T, MAVROUDI S, *et al*. A Probabilistic symmetric encryption scheme for very fast secure communication based on chaotic systems of difference equations[J]. International Journal on Bifurcation & Chaos, 2001, 11(12): 3107 - 3115.

[8] XIAO D, LIAO X, DENG S. One - way hash function construction based on the chaotic map with changeable-parameter[J]. Chaos, Solitons and Fractals, 2005(24): 65 - 71.

[9] LI S, CHEN G, MOU X. On the dynamical degradation of digital piecewise linear chaotic maps[J]. International Journal of Bifurcation and Chaos, 2005, 15(10): 3119 - 3151.

[10] 王云峰. 基于混沌的密码算法及关键技术研究[D]. 浙江：浙江大学, 2006.

(上接第433页)

[2] BONEH D, BOYEN X. Efficient selective-ID identity based encryption without random oracles[C]// Advances in Cryptology-Eurocrypt 2004. German: Springer-Verlag, 2004: 223 - 238.

[3] BONEH D, BOYEN X. Secure identity based encryption without random oracles[C]// Advances in Cryptology-Crypto 2004. Germany: Springer-Verlag, 2004: 443 - 459.

[4] WATERS B. Efficient selective-ID identity based encryption without random oracles[C]// Proceedings of Eurocrypt 2004, LNCS 3027. Berlin: Springer-Verlag, 2004: 223 - 238.

[5] COCKS C. An identity based encryption scheme based on quadratic residues[C]// Cryptography and Coding. Germany: Springer-Verlag, 1999: 205 - 221.

[6] GENTRY D B C, HAMBURG M. Space-efficient identity based encryption without pairings[EB/OL]. [2007 - 02 - 15]. http://eprint.iacr.org/2007/177.pdf.

[7] BERKOVITS S. How to broadcast a secret[C]// International Conference on the Theory and Application of Cryptographic Techniques. Berlin: Springer Verlag, 1991: 535 - 541.

[8] FIAT A, NAOR M. Broadcast Encryption[C]// 13th Annual International Cryptology Conference. Berlin: Springer-Verlag, 1993: 480 - 491.

[9] NAOR D, NAOR M, LOTSPIECH J. Revocation and tracing schemes for stateless receivers[C]// 21th Annual International Cryptology Conference. Heidelberg: Springer, 2001: 41 - 62.

[10] HALEVY D, SHAMIR A. The LSD broadcast encryption scheme[C]// 22th Annual International Cryptology Conference. Heidelberg: Springer, 2002: 47 - 60.

[11] BONEH D, GENTRY C, BRENTWATERS. Collusion resistant broadcast encryption with short ciphertexts and private keys[C]// 25 Annual International Cryptology Conference. Heidelberg: Springer, 2005: 258 - 275.

[12] ATTAPADUNG N, FURUKAWA J, IMAI H. Forward-secure and searchable broadcast encryption with short ciphertexts and private keys[C]// ASIA Cryptology Conference 2006. 湖南：湖南文艺出版社, 2006: 161 - 177.

[13] SAKAI R, FURUKAWA J. Identity-based broadcast encryption[EB/OL]. [2007 - 02 - 15]. http://eprint.iacr.org/2007/217.pdf.