第 57 卷 第 1 期 2008 年 1 月
1000-3290/2008/57(01)/0037-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.57,No.1,January,2008

一类改进的混沌迭代加密算法*

徐淑奖† 王继志

(山东省计算中心,济南 250014)

(2007 年 4 月 15 日收到;2007 年 4 月 30 日收到修改稿)

指出了最近提出的一类混沌迭代分组密码算法的缺陷,通过选择明文攻击可以恢复出置换后的明文.算法中二进制序列的产生只依赖于密钥,而与明文无关,从而使算法容易造成信息泄露并遭受攻击.基于此,给出了一种可以抵御选择明文攻击的安全性更高的算法.

关键词:混沌,混沌密码,攻击,安全性

PACC:0545

1. 引 言

近年来出现了一系列的混沌加密算法,然而大多数算法都存在着安全性缺陷.最近,Liao 等[1] 和 Cao 等[2] 分别提出来一种基于迭代混沌映射的分组密码算法.这两种算法的加密原理是类似的,都是先将明文块做一个依赖于密钥的置换,然后根据传统的混沌加密技术用迭代混沌映射产生的二进制序列来掩盖置换后的明文块.所不同的是前者[1] 是基于 Logistic 映射的,并且明文是按照 8 个字节分块的;而后者[2] 是基于时滞混沌神经网络的,明文是按照 4 个字节分块的,而且添加了一个从两个混沌轨道中选择用来生成二进制序列轨道的开关,并对用来掩盖置换后的明文块的二进制序列也做了一个置换.我们将这两种混沌加密算法统称为一类迭代混沌加密算法,该类算法可以看作是文献[3—6]的改进算法[1].

在 19 世纪 Kerchoffs 写下了现代密码学的原理.其中的一个原理提到加密体系的安全性并不依赖于加密方法本身,而是依赖于所使用的密钥[7].因而在分析密码系统时,通常假设密码分析者熟悉密码系统的设计和工作原理,也就是说,除了密钥之外,密码分析者知道密码系统任何知识.传统的密码分析方法按照从难到易的顺序排列如下[7]:

1)唯密文攻击:攻击者拥有用同一种加密算法加密的一些密文,在这种条件下破译出全部或部分明文,或者破解出全部或部分密钥.

2)已知明文攻击:攻击者通过密文的固定格式或其他方式知道了几段密文所对应的明文,从而破译出全部或部分明文或密钥.

3)选择明文攻击:密码分析者不但拥有一些密文和密文所对应的明文,而且能够随意的选择加密的明文,以破译出全部或部分明文或密钥.这种情况可视为攻击者暂时获得了加密机的使用权或通过间谍引诱选择明文.

4)选择密文攻击:密码分析者不但拥有一些明文和明文所对应的密文,而且能够随意的选择密文,以破译出密钥.这种情况可视为攻击者暂时获得了解密机的使用权或通过间谍引诱选择密文.

本文将指出该类算法存在的安全性缺陷,对于用该类算法加密的密文,可以用传统密码分析方法——选择明文攻击恢复出置换后的明文,这就造成了信息泄露,导致算法缺乏安全性;并且将给出具有更高安全性的改进算法.本文第二节给出了原算法的概述,第三节指出了原算法的安全性缺陷,第四节给出了改进的加密算法和实验结果,最后一节给出结论.

2. 算法概述

文献[1]和[2]的密码系统分别用到了 Logistic

* 山东省自然科学基金(批号:Y2006A27)资助的课题.

† E-mail:xushj@keylab.net

映射[1]

$$f(x) = \mu x(1-x), x \in [0,1], \quad (1)$$

和 Hopfiled 神经网络映射[8,9]

$$\begin{pmatrix} \frac{\mathrm{d}x_1(t)}{\mathrm{d}t} \\ \frac{\mathrm{d}x_2(t)}{\mathrm{d}t} \end{pmatrix} = -C\begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix} + A\begin{pmatrix} \tanh(x_1(t)) \\ \tanh(x_2(t)) \end{pmatrix} + B\begin{pmatrix} \tanh(x_1(t-\tau(t))) \\ \tanh(x_2(t-\tau(t))) \end{pmatrix}, \quad (2)$$

其中 μ, A, B 为参数，C 为二阶单位矩阵，$\tau(t) = 1 + 0.1\sin(t)$. 这是两个具有遍历性等优良特性的混沌映射. 该类加密算法用到了文献[10]中所提出的生成随机序列的算法之一来产生独立同分布的二进制随机序列. 将 x 的值写成二进制的形式，即

$$x = 0.b_1(x)b_2(x)\cdots b_i(x)\cdots, \quad x \in [0,1], b_i \in \{0,1\}. \quad (3)$$

如果 $x \in [a,b]$，可以做一个线性变换 $\frac{x-b}{a-b}$ 将其映射到区间[0,1]上. 第 i 比特 $b_i(x)$ 可表示为

$$b_i(x) = \sum_{r=1}^{2^i-1}(-1)^{r-1}\Theta_{r/2^i}(x), \quad (4)$$

其中 $\Theta_t(x)$ 是一个极限函数

$$\Theta_t(x) = \begin{cases} 0, & x < t, \\ 1, & x \geqslant t. \end{cases} \quad (5)$$

由此可以得到一个二进制随机序列 $B_i^n = b_i(\tau^n(x))|_{n=0}^{\infty}$（其中 n 是该序列的长度，$\tau^n(x)$ 是混沌映射的第 n 次迭代的函数值）.

首先定义一个从 8 比特的消息块到混沌映射象空间的不同区域（256 个点）的映射. 为了防止瞬时效应，预先迭代混沌映射 N_0 次.（神经网络映射(2)可用四阶 Runge-Kutta 法求解，取步长 $h = 0.01$. 假设 $x_1(t), x_2(t)$ 是该映射的两个混沌轨道，第 i 次迭代结果是 $x_{1i} = x_1(ih), x_{2i} = x_2(ih)$.）下面以文献[1]的密码系统为例来说明加密算法.

1）取迭代的初始点为第 N_0 次迭代的函数值，即

$$\omega = \tau^{N_0}(x_0).$$

2）将消息串 m 分成若干长度为 l 字节的子消息块（$l = 8$）：

$$m = \underbrace{p_0, p_1, \cdots, p_{l-1}}_{m_0}, \underbrace{p_l, \cdots, p_{2l-1}}_{m_1}, p_{2l}, \cdots. \quad (6)$$

其中 l 字节的明文串 $p_{lj}, p_{lj+1}, \cdots, p_{(l+1)j-1}$ 组成一个 $8l$ 比特的子消息块 $P_j = p_{lj}, p_{lj+1}, \cdots, p_{(l+1)j-1}$.

3）由上面所述的产生二进制序列的方法，在(3)式中取 $i = 3$，可以生成二进制序列 $A_j = B_i^1 B_i^2 \cdots B_i^{8l}$，$A_j^1 = B_i^{8l+1} B_i^{8l+2} \cdots B_i^{8l+\log_2 8l}$. 用 D_j 表示 A_j^1 的十进制数值，并在本轮加密后迭代混沌映射 D_j 次.

4）将 P_j 循环左移 D_j 比特，P_j 做置换变换后的序列记为 P_j'.

5）对序列 P_j' 和 A_j 做异或运算

$$C_j = P_j' \oplus A_j, \quad (7)$$

其中 $\oplus$ 是异或运算符号. 于是得到了消息块 P_j 所对应的密文 C_j，将 C_j 按照 8 比特分开来可以得到明文 $p_{lj}, p_{lj+1}, \cdots, p_{(l+1)j-1}$ 所对应的密文 $c_{lj}, c_{lj+1}, \cdots, c_{(l+1)j-1}$.

6）如果所有的明文块都已经被加密过，那么加密过程完毕. 否则，令 $\omega = \tau^{8l+\log_2 8l}(\omega)$，转到第 2）步进入下一轮加密.

解密过程和加密过程几乎一样，只需要将(7)替换为

$$P_j' = C_j \oplus A_j, \quad (8)$$

就可以得到置换后的消息块 P_j'. 根据 D_j 的值做一个逆置换变换，并将其按照字节分开来便可以恢复出相应的明文.

文献[2]的密码系统的算法与上述算法类似，不同之处是：第 1）步中的初值记为 $x_0 = x_1(N_0 h)$. 第 2）步中 $l = 4$. 第 3）步中还需要生成一个用作选择开关的二进制序列 $A_j^2 = B_i^{8l+\log_2 8l+1}$，且该算法在(3)式中取 $i = 4$. 第 4）步同时对序列 A_j 做了一个循环右移动 D_j 比特的置换，记置换后的序列为 A_j'. 在第 4）步和第 5）步之间加了一步用来选择迭代轨道的转换开关，若 $A_j^2 = 0$，下一轮加密中第 3）步将用轨道 $x_1(t)$ 来生成二进制序列；若 $A_j^2 = 1$，下一轮加密中第 3）步将用轨道 $x_2(t)$ 来生成二进制序列. 第 5）步做异或运算的是 P_j' 和 A_j'. 第 6）步中的初值取为 $x_0 = x_{A_j^2+1}((8l + \log_2 8l + 1)h)$. 相应的解密过程也需要做类似的修改.

3. 原算法的缺陷

对于给定密文串 C，本节将借助于选择明文攻击来恢复出置换后的明文并指出原算法的缺陷. 该类算法类似于同步流加密算法，在每一轮加密过程中，其状态转移函数与输入的明文符号无关，这就导致了算法容易遭受选择明文攻击.

我们仍然以文献[1]的密码系统为例来说明这一类加密算法的缺陷.具体分析步骤如下：

1)选择一个全为零的明文串 P^*，P^* 的长度与给定的密文串 C 相同.并根据原算法第 2)步将明文串 P^* 和给定的密文串 C 按照 l 字节分块.

2)用原算法将明文串 P^* 加密,可以得到对应的密文串 C^*，其中 C_j^* 是明文块 P_j^* 所对应的密文块.

3)根据原算法第 4)步,对明文块 P_j^* 做循环左移 D_j 比特的置换变换.事实上,全为零的消息块 P_j^* 置换后所得到的消息块 $P_j^{*'}$ 仍是一个 l 字节的全为零的消息块.

4)由原算法第 5)步中的(7)式,在第 j 轮加密过程中 $C_j^* = P_j^{*'} \oplus A_j$.根据上一步，$P_j^{*'}$ 是一个全为零的消息块,因此，C_j^* 和 A_j 是相同的,即 $C_j^* = A_j$.

5)根据原算法解密过程中的(8)式,可得到与给定的密文块 C_j 相对应的置换后的明文块 P'_j，

$$P'_j = C_j \oplus C_j^* . \tag{9}$$

对于文献[2]的密码系统,在上述过程中只须将 A_j 换成置换后的序列 A'_j,即可以得到同样的结果.

根据原算法可知，P'_j 是明文块 P_j 做置换变换后的字符串.据我们所知,仅仅对密文块做一个置换,是远远不能满足安全性要求的.这样容易造成部分明文信息的泄露，由于 P_j 和 P'_j 都是 l 字节的字符串,那么由原算法的解密过程可知最多经过 $8l-1$ 次循环移位可以恢复出一个明文块.因此,原算法存在着安全性缺陷,这是由于该类算法中迭代混沌映射产生二进制序列的机理造成的.原算法第 3)步中,通过迭代混沌映射产生的二进制序列仅仅与密钥有关,而不依赖于明文.由于产生二进制比特流的状态转移函数与输入的明文符号无关,所以对于任何明文串,第 j 轮加密过程中所涉及到的二进制序列 A_j，$A_j^1(D_j)$(包括文献[2]算法中的 A_j^2)都是固定的.这一点没有很好的满足分组密码算法设计的两个基本原则——扩散和混乱的要求.扩散要求将单个明文或密钥位的影响尽可能扩大到更多的密文中去,不仅将统计关系隐藏起来,也使密码分析者寻求明文冗余度增加了难度;而混乱要求掩盖密文统计特性与明文统计特性的关系,以挫败通过研究密文获取冗余度和统计模式的企图.在原算法中,每一个明文比特只能影响到它所在的明文块加密后的 $8l$ 个比特的密文块,而与其他的密文块无关.也就是说,每个密文比特最多只受到相应的 $8l$ 个比特明文块的影响,而与其他的明文块无关.由于传输的无误性,对于任何明文串,该类算法的第 j 轮加密过程中所产生的比特流相同,这就给选择明文攻击造成了可乘之机.

4. 改进算法

由上一节可知,迭代混沌映射产生的二进制序列仅与密钥有关,而不依赖于明文的机制容易造成信息泄露和导致算法遭受攻击.基于这一缺陷,本节提出一种改进的算法,以避免这一弱点并获得更高的安全性.

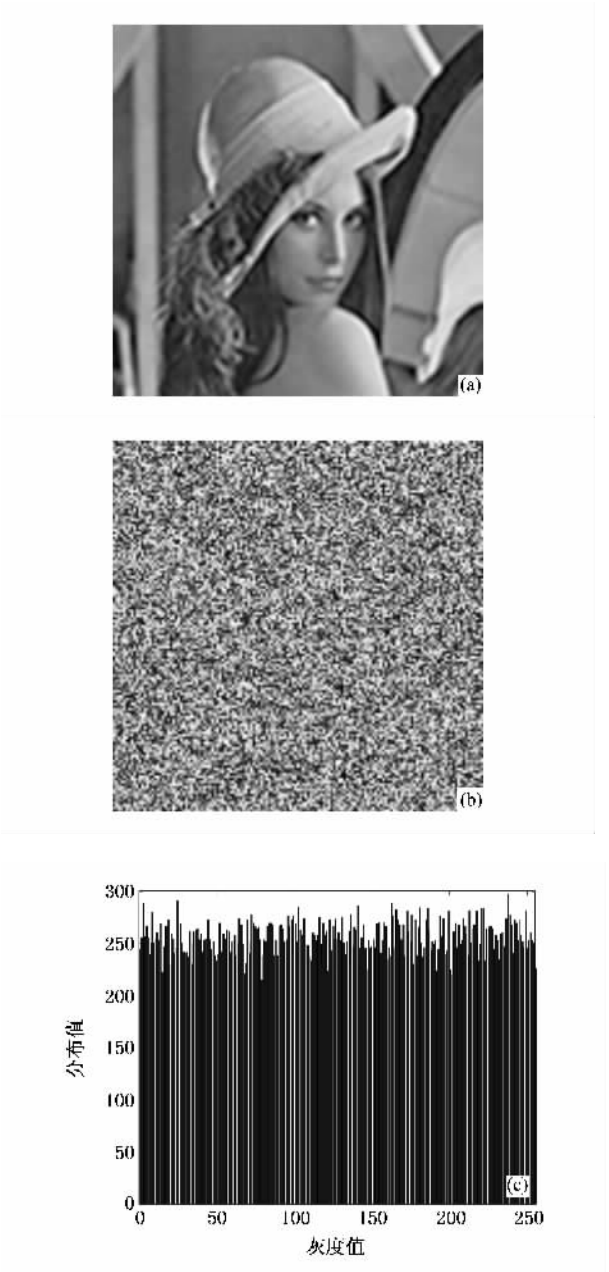

图 1　实验结果　(a)明文;(b)密文;(c)密文灰度值柱状分布图

为了避免上述缺陷,我们需要改变明文、密钥、二进制序列产生机理三者之间的关系,使得二进制序列的生成过程与明文相关,将单个明文比特的影响扩散到更多的密文比特当中去,以获得更好的扩散与混乱效果.事实上,只需要改变第 j 轮加密过程中的整数 D_j,使得 D_j 与明文相关.这样,对于不同的明文串 D_j 也不同.由于 D_j 不同,第 j 轮加密过程中迭代混沌映射的次数就会改变,从而导致了下一轮的二进制序列也会发生变化,这样不但避免了选择明文攻击,而且使得每一个明文比特可以影响到更多的密文比特.在上一节原算法的第 3)步中,令二进制序列 A_j^1 的十进制数值为 D_j',并取

$$D_j = D_j' + \sum_{k=1}^{l-1} p_{lj+k} \mod 8l, \qquad (10)$$

其中 p_{lj+k}($k = 0,2,\cdots,l-1$)是明文块 P_j 每一个字节的值.另外,为了避免生日攻击,在原算法的第 2)步中取 $l = 16$,即将明文按照 16 字节(128 比特)分块.需要指出的是 $a_j = D_j' + \sum_{k=0}^{l-1} p_{ij+k} \mod 256$ 为对应密文块的一部分.其他各步均不需要改变,当然解密过程也需要做相应的改变.

下面以文献[1]的算法为例,给出用改进的算法加密的实验结果.我们选取一张 256×256 的 BMP 格式的灰度图为明文,并取密钥为(x_0, μ) = (0.1777,3.9999995).如图 1 所示,图 1(a)是明文 Lena.bmp.图 1(b)是用改进的算法加密所得到的图像,可以看出加密后的图像是一张杂乱无章的、无任何明文信息的图片,因而满足了扩散和混乱的要求.图 1(c)是图 1(b)灰度值的柱状分布图,可以看出 0—255 各像素值都落在区间[200,300]之间,各像素值分布非常均匀,这表明了改进算法掩盖了所有的明文信息,并展现了很好的 0-1 自相关性和 0 互相关性.信息量 $H(m) = 7.99738$,这非常接近于理想状态的信息量 $H(m) = 8$.特别地,改进的算法对原算法的运行速度几乎没有影响.

5. 结 论

本文指出了一类迭代混沌加密算法存在着安全性缺陷,迭代混沌映射所产生的二进制序列仅与密钥相关,而不依赖于明文,导致了该算法容易遭受选择明文攻击.通过改变二进制序列的产生机理与密钥及明文的关系,使得每一个明文比特不但影响到本轮所得到的密文块,而且会影响到下一轮的密文块,本文给出一种改进的迭代加密算法,改进的加密算法不仅可以有效地防止选择明文攻击和生日攻击,而且具有更好的扩散与混乱等密码学特性.

[1] Xiang T, Liao X F, Tang G P, Chen Y, Wong K W 2006 *Phys. Lett.* A **349** 109

[2] Yu W W, Cao J D 2006 *Phys. Lett.* A **356** 333

[3] Baptista M S 1998 *Phys. Lett.* A **240** 50

[4] Wong W K, Lee L P, Wong K W 2001 *Comp. Phys. Commun.* **138** 234

[5] Wong K W 2002 *Phys. Lett.* A **298** 238

[6] Wong K W, Ho S W, Yung C K 2003 *Phys. Lett.* A **310** 67

[7] Stinson D R 1995 *Cryptography: Theory and Practice* (Boca Raton: CRC Press)

[8] Hopfild J J 1984 *Proc. Natl. Acad. Sci. USA* **81** 3088

[9] Lu H T 2002 *Phys. Lett.* A **298** 109

[10] Kohda T, Tsuneda A 1997 *IEEE Trans. Inform. Theory* **43** 104

An improved block cryptosystem based on iterating chaotic map *

Xu Shu-Jiang† Wang Ji-Zhi

(*Shandong Computer Science Center*, *Jinan* 250014, *China*)

(Received 15 April 2007; revised manuscript received 30 April 2007)

Abstract

Recently, a large number of chaotic cryptosystems have been proposed, yet many of them have the drawbacks of lack of robustness and security. In this paper, we point out the weakness of a very recent block cipher algorithm which is based on the chaotic map and give the improved scheme of it. We provide the chosen plaintext attack to recover the permuted plaintext string. It is shown that the generation mechanism of binary sequences which depends on the key but not on the plaintext facilitates leakage of information and is vulnerable to attacks. Based on such a fact, we give the improved scheme to achieve higher security.

Keywords: chaos, chaotic cryptosystems, attack, security

PACC: 0545

* Project supported by the Natural Science Foundation of Shandong Province, China (Grant No. Y2006A27).

† E-mail: xushj@keylab.net