一种图像加密算法的等效密钥攻击方案

郭建胜,张 锋
(解放军信息工程大学电子技术学院,河南郑州 450004)

摘 要: 本文分析了一个基于 3D 混沌 Baker 映射设计的图像加密方案的安全性,在已知图像的条件下,基于 3D 混沌 Baker 映射的仿射特性,通过求解三个线性无关的加密前后的图像像素灰度值点,获得了 3D 混沌 Baker 映射的全部等效密钥参数,再通过穷尽方法求出了加密算法的其余等效密钥.分析了攻击方法的计算复杂性,证明了该图像加密算法在已知图像攻击下是不安全的.

关键词: 密码分析; 等效密钥攻击算法; 仿射特性; 3D 混沌 Baker 映射; 图像加密; 混沌密码
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2010) 04-0781-05

An Equivalent Key Attack on an Image Cryptosystem

GUO Jian-sheng, ZHANG Feng
(*Electronic Technology Institute, Information Engineering University, Zhengzhou, Henan* 450004, *China*)

Abstract: This paper examines the security of an image cryptosystem based on 3D chaotic Baker map. With known image, based on the affinity of 3D chaotic Baker map, the equivalent key of Baker map can be found by three linearly independent plain-cipher image grey values. The other equivalent key can be found by exhaustive attack. We estimate the computational complexity of our attack and prove that this image cryptosystem is insecure under the known image attack.

Key words: cryptanalysis; equivalent key attack algorithm; affinity; 3D chaotic Baker map; image encryption; chaotic cipher

1 基于 3D 混沌 Baker 映射图像加密算法描述

毛耀宾,陈关荣等[1]将二维 Baker 映射[2]推广为三维 Baker 映射,并给出了三维 Baker 映射的一般形式.假设单位立方体被分为 $k \times t$ 块,$[W_{i-1}, W_i] \times [H_{j-1}, H_j] \times [0,1)$, $i = 1, \cdots, k$, $j = 1, \cdots, t$,且 $W_0 = 0$, $W_i = w_1 + \cdots + w_i$, $w_1 + \cdots + w_k = 1$; $H_0 = 0$, $H_j = h_1 + \cdots + h_j$, $h_1 + \cdots + h_t = 1$, w_i 与 h_j 表示相应小块的长度和宽度.结构如图 1 所示.对任意 $(x, y, z) \in [W_{i-1}, W_i] \times [H_{j-1}, H_j] \times [0,1)$,三维 Baker 映射表示为

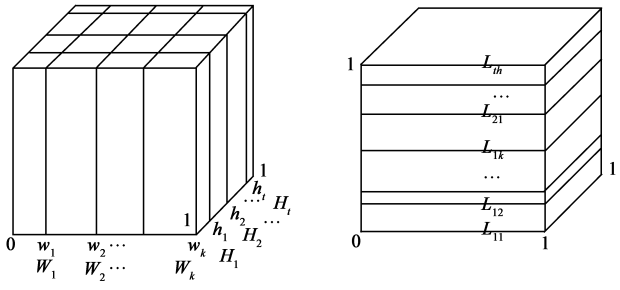

图1 推广的三维Baker映射

$$B_3(x, y, z) = \left(\frac{1}{w_i}(x - W_i), \frac{1}{h_j}(y - H_j), w_i h_j z + L_{ij}\right)$$

这里 $L_{ij} = W_i \times h_j + H_j$.

上述连续三维 Baker 映射被离散化,而且可用于任意的立方块.不失一般性,我们假设立方块为 $W \times H \times L$,被分割为 $k \times t$ 块. $W_0 = 0$, $W_i = w_1 + \cdots + w_i$, $W = w_1 + \cdots + w_k$; $H_0 = 0$, $H_j = h_1 + \cdots + h_j$, $H = h_1 + \cdots + h_t$.对立方块中的任意点 (m, n, l),三维离散 Baker 映射表示为

$$S = (H_{j-1} \times W + W_{i-1}) \times L + w_i \times h_j \times l + (n - H_{j-1}) \times w_i + (m - W_{i-1}) \quad (1)$$

$$(m', n', l') = B_{3D}(m, n, l) = \left((S \bmod (W \times H)) \bmod W, \left\lfloor \frac{S \bmod (W \times H)}{W} \right\rfloor, \left\lfloor \frac{S}{W \times H} \right\rfloor\right) \quad (2)$$

具体结构如图 2 所示.

基于上述三维离散 Baker 映射,毛耀宾,陈关荣等设计了一个用于图像加密的密码算法,该加密算法由以下五部分组成.

收稿日期:2007-03-06;修回日期:2009-12-22
基金项目:国家自然科学基金(No.60503012);河南省杰出青年基金(No.0312001800)

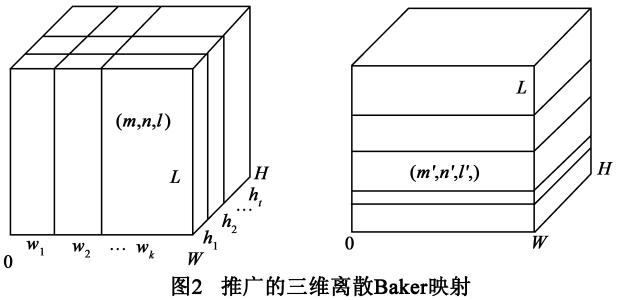

图2 推广的三维离散Baker映射

(1)密钥生成.选择一个 128 比特序列的密钥,将其分成 6 组 $k_1, k_2, k_3, k_4, k_5, k_6$,其中 k_1, k_2, k_3, k_4 为 24 比特,k_5, k_6 为 16 比特.并且将 k_1, k_2, k_3 看作(0,1)区间上的实数,k_4, k_5, k_6 为整数.

(2)将二维图像转变为三维图像.假设该图像长为 W 个像素,高为 H 个像素,共计 $W \times H$.将图像的所有像素组成 $M \times N \times L$ 的立方体,由于总的像素并未改变,显然满足 $M \times N \times L = W \times H$,下面给出 M, N, L 求解算法:

(a)设 $T = W \times H$,分解 T 有 $T = p_1 \times p_2 \times \cdots \times p_n \times 1$;

(b)对$\{p_1, p_2, \cdots, p_n, 1\}$进行重新排列,然后将其分成三组来组成 M, N, L.进行重排时以 k_5 作为种子,k_6 作为迭代圈数.

(3)进行三维离散 Baker 映射变换.分别用 k_1 和 k_2 作为初始参数作相应的 logistic 映射 $x_{k+1} = 4x_k(1 - x_k)$,按照约定的迭代圈数和实数到整数的转换方式,分别选取两个序列$\{m_1, \cdots, m_k\}$和$\{n_1, \cdots, n_t\}$,并且满足 $M_0 = 0, M_i = m_1 + \cdots + m_i, M = m_1 + \cdots + m_k; N_0 = 0, N_j = n_1 + \cdots + n_j, N = n_1 + \cdots + n_t$.然后,对每个图像立方块进行三维离散 Baker 映射变换.

(4)扩散过程.设 $C(0) = k_4$,然后进行如下变换 $C(k) = \varphi(k) \oplus \{[I(k) + \varphi(k)] \bmod M\} \oplus C(k-1)$,$I(k)$ 为当前待处理像素灰度值,$C(k-1)$是前一个处理过的像素灰度值,$C(k)$是当前处理过的像素灰度值,M 为灰度阶(对于一个 256 灰度的图像,$M = 256$).设 $x(0) = k_3$,作为初始值计算混沌 logistic 映射 $x(k+1) = 4x(k)[1 - x(k)]$,如果得到的值在(0.2,0.8)区间之内,用适当的采样和缩放比例将其数字化,得到的数值即为 $\varphi(k)$;否则,重复此步骤直到所得数值在(0.2,0.8)区间之内.

(5)将三维图像转换为二维图像.三维的立方块按序排列,将其转换为二维图像后输出作为密文图像.

上述图像加密算法如图 3 所示.算法没有明确给出对图像中各点像素进行变换的先后顺序,按照程序实现的习惯,在下面的分析中假设是按照字典排序方式来依次进行变换的.算法第三步和第四步可以只做一次,也可以迭代多次,但作者没有具体给出迭代次数.多次迭代时,每次迭代使用的密钥是使用相同的 128*bit* 初始密钥,还是使用不同的 128bit 初始密钥也没有说明,针对这些情况,下面的分析中将分别进行分析,给出相应的攻击算法.算法第二步中将二维的图像转变为三维时,如何利用$\{p_1, p_2, \cdots, p_n, 1\}$和 k_5、k_6 求解 M, N, L,算法没有交代清楚,但是,无论使用什么方式对我们的分析都没有影响.在使用混沌 logistic 映射 $x(k+1) = 4x(k)[1 - x(k)]$生成 $\varphi(k)$时,0.5 是一个“坏点”,会使循环陷入固定点 0.遇到此情况,作者要采取一点小措施来解决该问题,但采取的具体方法没有说明.另外,通过什么样的采样和缩放比例将得到的区间(0.2,0.8)内的值数字化来产生 $\varphi(k)$也没有说明.

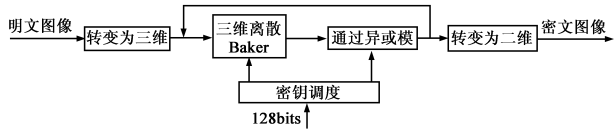

图3 基于三维离散Baker映射的图像加密算法

2 对图像加密算法的分析

下面首先对图像加密算法中的第二、三步进行分析.

定理 1 设明文图像被转化为 $W \times H \times L$ 的立体图像,被分割为 $k \times t$ 块,即有 $W_0 = 0, W_i = w_1 + w_2 + \cdots + w_i, W = w_1 + w_2 + \cdots + w_k; H_0 = 0, H_j = h_1 + h_2 + \cdots + h_j, H = h_1 + h_2 + \cdots + h_t$.对立方块中的任意点$(m, n, l)$,其三维离散 Baker 变换后的值为$(m', n', l')$,则有

$$S = W \times H \times l' + W \times n' + m'$$

以及

$$m = (S - (H_{j-1} \times W + W_{i-1}) \times L) \bmod w_i + W_{i-1},$$
$$n = \lfloor [S - (H_{j-1} \times W + W_{i-1}) \times L] / w_i \rfloor \bmod h_j + H_{j-1},$$
$$l = \lfloor \lfloor [S - (H_{j-1} \times W + W_{i-1}) \times L] / w_i \rfloor / h_j \rfloor.$$

证明 由式(2)显然有 $S = W \times H \times l' + W \times n' + m'$.根据 W_{i-1}和 w_i 的定义可知 $m - W_{i-1} < w_i$,再由式(1)有

$$m - W_{i-1} = (S - (H_{j-1} \times W + W_{i-1}) \times L) \bmod w_i \tag{3}$$

即 $m = (S - (H_{j-1} \times W + W_{i-1}) \times L) \bmod w_i + W_{i-1}$.

同样由式(1)有

$$(h_j \times l + n - H_{j-1}) \times w_i = S - (H_{j-1} \times W + W_{i-1}) \times L + m - W_{i-1}$$

又由式(3)知

$$n - H_{j-1} = \lfloor [S - (H_{j-1} \times W + W_{i-1}) \times L] / w_i \rfloor - (h_j \times l)$$

根据 H_{i-1}和 h_i 的定义可知 $n - H_{i-1} < h_i$,从而

$$n = \lfloor [S - (H_{j-1} \times W + W_{i-1}) \times L] / w_i \rfloor \bmod h_j + H_{j-1}$$

同理可证

$$l = \lfloor \lfloor [S - (H_{j-1} \times W + W_{i-1}) \times L] / w_i \rfloor / h_j \rfloor$$

图像加密算法中第二、三步的密钥因素为 W、H、L 以及诸 w_i、h_j,如果知道了这些值,三维离散 Baker 映射就被确定下来.如果知道了明文坐标(m, n, l)对应的三维离散 Baker 变换后的值(m', n', l'),根据定理 1 可知,$S = W \times H \times l' + W \times n' + m'$及

$$m = (S - (H_{j-1} \times W + W_{i-1}) \times L) \bmod w_i + W_{i-1},$$

可有

$$m = (W \times H \times l' + W \times n' + m' - (H_{j-1} \times W + W_{i-1}) \times L) \bmod w_i + W_{i-1}$$

当 $i = 1, j = 1$ 时,有 $H_0 = 0, W_0 = 0$,带入上式得到

$$m = (W \times H \times l' + W \times n' + m') \bmod w_1$$

如果获得了 w_1 的值就可通过解方程组的方式求得 W、H,而 $W \times H \times L$ 已知,进而求得 L.求出 W、H、L 的值后,再根据定理 1 中的结果,利用它们之间的相互递推关系就可以得其余诸 w_i、h_j.而 $w_1 \in [1, W \times H \times L]$,最坏情况下对其进行穷尽.

下面对图像加密算法的第四步进行分析.算法的第四步利用变换 $C(k) = \varphi(k) \oplus \{[I(k) + \varphi(k)] \bmod M\} \oplus C(k-1)$对图像的各点像素进行变换,其密钥因素素为 $C(0) = k_4$ 和设 logistic 映射 $x(k+1) = 4x(k)[1 - x(k)]$的初始值 $x(0) = k_3$,显然 k_4 的最大可能取值量为灰度阶 M.

3　对图像加密算法的等效密钥攻击

下面在已知一份加密前后的图像的条件下,对上述图像加密算法实施攻击,我们假设在加密过程中按照明文像素位置的字典序对像素依次变换,具体所使用的顺序并不影响分析过程.

首先对第三、四步只迭代一次时算法进行攻击.根据密钥生成算法可知,生成密钥参数 L_i 和 S 只与 k_3 和 k_4 有关.先把已知的二维密文图像转换为三维密文图像,然后对 k_3 和 k_4 进行穷举,利用密钥生成算法产生密钥参数 L_i 和 S,利用第四步变换的逆变换

$$I(k) = \{\varphi(k) \oplus C(k) \oplus C(k-1) + M - \varphi(k)\} \bmod M$$

对三维密文图像进行解密,解密后的图像我们称为三维混乱密文图像.由加密算法可知,三维混乱密文图像就是三维明文图像经过三维离散 Baker 映射变换后的图像.

首先穷尽 w_1 的值,然后对三维明文图像的像素位置(m, n, l)变换后的位置(m', n', l')进行穷举,由于三维离散 Baker 映射变换只改变像素灰度位置,并不改变其灰度值,因此(m', n', l')只取三维混乱密文图像中和三维明文图像中点(m, n, l)灰度值相同的点,设三维混乱密文图像中这样的点的个数为 M'.利用定理 1 中的结论 $m = (W \times H \times l' + W \times n' + m') \bmod w_1$,由于该线性方程为一同余方程,需要取满足$(m, w_1) = 1$ 的点,以保证解的唯一性.建立关于 W、H 的线性方程

$$W \times H \times l' + W \times n' + m' = yw_1 + m$$

这里 y 也为一未知量,当找到三个线性无关的点及其对应的三维离散 Baker 变换后的点$(m_1, n_1, l_1) \rightarrow (m'_1, n'_1, l'_1)$、$(m_2, n_2, l_2) \rightarrow (m'_2, n'_2, l'_2)$和$(m_3, n_3, l_3) \rightarrow (m'_3, n'_3, l'_3)$,就可解方程组求得 W、H 的值,而 $W \times H \times L$ 已知,进而求得 L.求出 W、H、L 的值后,再根据定理 1 中的结果,利用 w_i、h_j 之间的相互递推关系就可以得其余诸 w_i、h_j.设原始图像的大小为 $N_1 \times N_2$.

算法 1:

for$(k_3 = 0; k_3 < 2^{24}; k_3 ++)$
{*for*$(k_4 = 0; k_4 < M; k_4 ++)$
{$L_i = k_3$ 和 $S = k_4$;利用第四步变换的逆变换
$I(k) = \{\varphi(k) \oplus C(k) \oplus C(k-1) + M - \varphi(k)\} \bmod M$
对三维密文图像进行解密;
for$(w_1 = 1; w_1 < N_1 \times N_2; w_1 ++)$
{查找$(m_1, n_1, l_1) \rightarrow (m'_1, n'_1, l'_1)$,$(m_2, n_2, l_2) \rightarrow (m'_2, n'_2, l'_2)$和$(m_3, n_3, l_3) \rightarrow (m'_3, n'_3, l'_3)$;
解线性方程组

$$\begin{cases} W \times H \times l'_1 + W \times n'_1 + m'_1 = yw_1 + m_1 \\ W \times H \times l'_2 + W \times n'_2 + m'_2 = yw_1 + m_2; \\ W \times H \times l'_3 + W \times n'_3 + m'_3 = yw_1 + m_3 \end{cases}$$

$L = (N_1 \times N_2)/(W \times H)$;
for$(i = 2; i < t; i ++)$
for$(j = 1; j < k; j ++)$
{$m = (S - (H_{j-1} \times W + W_{i-1}) \times L) \bmod w_i + W_{i-1}$;
$n = \lfloor [S - (H_{j-1} \times W + W_{i-1}) \times L] / w_i \rfloor \bmod h_j + H_{j-1}$;
$l = \lfloor \lfloor [S - (H_{j-1} \times W + W_{i-1}) \times L] / w_i \rfloor / h_j \rfloor$;
$S = W \times H \times l' + W \times n' + m'$;
解上面四个联立方程求出诸 w_i、h_j;}
进一步利用已知的明文图像和密文图像验证所求得的密钥;若正确,输出密钥;flag = 1;反之,
flag = 0; continue;}
if(flag == 1) break;}
if(flag == 1) break;}

由加密算法所使用变换的性质,攻击算法总可以找到密钥的等效密钥,在攻击算法中,k_3 和 k_4 的穷尽量最坏情况下为 $2^{24}M$ 次,找到三对对应坐标$(m_1, n_1, l_1) \rightarrow (m'_1, n'_1, l'_1)$、$(m_2, n_2, l_2) \rightarrow (m'_2, n'_2, l'_2)$和$(m_3, n_3, l_3) \rightarrow (m'_3, n'_3, l'_3)$,设 M_s 为所有 M' 的最大值,最坏情况下要计算 $3M_s$ 次,w_1 的最大穷尽量为 $N_1 \times N_2$,事实上的 w_1 值应远小于该数值.故整个算法在最坏情况下需要计算 $3 \times 2^{24} M_s (N_1 \times N_2)$次,因此,攻击

算法得到加密算法的等效密钥的计算复杂性为 $O(2^{24} M_s(N_1 \times N_2))$.

下面对第三、四步迭代多次时的算法进行攻击.加密算法的第三步和第四步多次迭代时,每次迭代使用的密钥参数可以由相同的 128bit 初始密钥通过密钥生成算法生成,也可以由不同的 128bit 初始密钥通过密钥生成算法生成.此时算法结构成为 S-P 迭代结构类型,算法 1 无法对其进行攻击.三维离散 Baker 映射的密钥因素为 W、H、L 以及诸 w_i、h_j,诸可通过穷尽 k_1 和 k_2 得到,最大穷尽量为 2^{48}.利用得到的 w_i、h_j 以及 $L=(N_1 \times N_2)/(W \times H)$进而可以求出 W、H、L.算法第四步中,各密钥参数是利用 k_3 和 k_4 由密钥生成算法产生,一次迭代中该步密钥的最大穷尽量为 $2^{24}M$.多次迭代时,利用穷尽攻击[3,4]对算法进行攻击.当每次迭代使用的密钥参数由相同的 128bit 初始密钥通过密钥生成算法生成时,整个算法的最大穷尽量为 $2^{72}M$.当每次迭代使用的密钥参数由不相同的 128bit 初始密钥通过密钥生成算法生成时,若设此时迭代的圈数为 r,则整个算法的最大穷尽量为 $2^{72r}M^r$.分别给出相应的分析算法如下,算法 2 给出了多次迭代并且各迭代圈使用相同密钥时的攻击算法,算法 3 给出了多次迭代并且各迭代圈使用不同密钥时的攻击算法.

算法 2:

for($k_1=0; k_1<2^{24}; k_1$ ++)
{ *for*($k_2=0; k_2<2^{24}; k_2$ ++)
{ *for*($k_3=0; k_3<2^{24}; k_3$ ++)
{ *for*($k_4=0; k_4<M; k_4$ ++)
{ $L_i=k_3$ 和 $S=k_4$;
利用第四步变换的逆变换
$I(k)=\{\varphi(k)\oplus C(k)\oplus C(k-1)+M-\varphi(k)\}$ mod$M$
对三维密文图像进行解密;分别用 k_1 和 k_2 作为初始参数作相应的 logistic 映射 $x_{k+1}=4x_k(1-x_k)$,求出 W、H、L 以及诸 w_i、h_j;利用第三步三维离散 Baker 映射的逆变换对三维三维混乱密文图像进行进一步解密,获得明文图像;验证解密后的图像和明文图像是否一致,若验证通过,输出密钥,flag = 1,break;反之,
flag = 0;continue;}
if(flag == 1) break;}
if(flag == 1) break;}
if(flag == 1) break;}

算法 3:

对各迭代圈的所有密钥进行循环嵌套穷尽;
(各迭代圈中 $k_1, k_2, k_3 \in [0, 2^{24}-1]$, $k_4 \in [0, M-1]$)
{---{利用 k_1, k_2 作为初始参数作相应的 logistic 映射 $x_{k+1}=4x_k(1-x_k)$,求出 W、H、L 以及诸 w_i、h_j; $L_i=k_3$ 和 $S=k_4$;利用所得密钥对三维密文图像进行解密;验证解密后的图像和明文图像是否一致,若验证通过,输出密钥,flag = 1,break;反之,flag = 0;continue;} if(flag == 1) break;---}

4 攻击算法的有效性分析

通过上述分析可知,算法 1 得到加密算法的等效密钥的计算复杂性为 $O(2^{24}M_s(N_1 \times N_2))$.同样以对一个 512×512 个像素点的图像加密为例,图像的灰度 $M=2^{16}$, $N_1 \times N_2 = 2^{18}$,即使 $M_s = 2^{16}$(这显然不可能的,根据原始明文图像得到的立方块不会只有一种灰度).此时攻击算法的最大计算量为 $3 \times 2^{24} \times 2^{16} \times 2^{18} = 3 \times 2^{58} < 2^{60}$,远远小于加密算法密钥空间中的密钥量 2^{128}.与著名的数据加密标准(DES)算法相比,其有效密钥量为 2^{56},但在穷尽攻击下已经被破译,因此在现有的计算能力下可以完成对算法的破译.

在图像加密算法第三、四步迭代多次时,通过分析算法 2 可知当每次迭代使用的密钥参数由相同的 128bit 初始密钥通过密钥生成算法生成时,如果原始图像的大小为 $N_1 \times N_2$,整个算法的最大穷尽量为 $2^{72}M$.当每次迭代使用的密钥参数由不相同的 128bit 初始密钥通过密钥生成算法生成时,若设此时迭代的圈数为 r,则通过分析算法 3 知整个算法的最大穷尽量为 $2^{72r}M^r$.同样以对一个 512×512 个像素点的图像加密为例,图像的灰度 $M=2^{16}$,当每次迭代使用的密钥参数由相同的 128bit 初始密钥通过密钥生成算法生成时,整个算法的最大穷尽量为 $2^{72}M = 2^{72} \times 2^{16} = 2^{88}$.远远小于加密算法密钥空间中的密钥量 2^{128}.目前替代 DES 的高级加密标准(AES)算法的密钥量为 2^{128},这是公认的安全计算量,因此在现有的计算能力下此时加密算法安全性值得怀疑.当每次迭代使用的密钥参数由不相同的 128bit 初始密钥通过密钥生成算法生成时,整个算法的最大穷尽量为 $2^{72r}M^r = 2^{88r}$,依然远小于加密算法密钥空间中的密钥量 2^{128r}.同样在实际使用环境中,为了便于密钥的协同等因素,一般不会在不同的迭代圈使用独立不同的随机密钥,无论是 DES 算法还是 AES 算法都说明了这一点.即使这样使用,文献[1]所设计的加密算法的有效密钥量也远不能达到预期的目标.

文献[1]中所设计的图像加密算法之所以不安全,是因为算法所使用混沌变换密钥参数在模运算下有等效密钥存在,以及三维离散 Baker 映射在一定条件下转化为线性变换,能够不通过穷尽初始密钥参数求解其秘密参数,上述算法弱点可以通过改变密钥结合方式的方法来克服.

5 结束语

本文证明了“A Novel Fast Image Encryption Scheme Based on 3D Chaotic Baker Maps”一文基于 3D 混沌 Baker 映射的图像加密算法的不安全性.通过分析加密算法所使用环节的特性,给出了算法的信息泄漏规律,并设计实现了不同情况下针对算法的已知图像攻击算法,可以求出加密算法的等效密钥,并分析了攻击算法的计算复杂性.分析结果证明了算法的不安全性,同时也给出了改进方法.本文的结果再一次说明,在将一种变换用于密码领域时,必须对其进行细致的分析,并设法克服其自身的弱点[5~7],只有这样才可能使设计出的加密算法经得起密码分析的考验.

参考文献:

[1] Mao Yao-bin, Chen Guan-rong, Lian Shi-guo. A novel fast image encryption scheme based on 3D chaotic Baker maps[J]. International Journal of Bifurcation and Chaos, 2003, 13(6): 859 – 876.

[2] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps[J]. International Journal of Bifurcation and Chaos, 1998, 8(6): 1259 – 1284.

[3] 李树钧,牟轩沁,纪震,等.一类混沌流密码的分析[J].电子与信息学报,2003,25(4):473 – 479.
Li Shu-jun, Mou Xuan-qin, Ji Zhen, et al. Cryptanalysis of a class of chaotic stream ciphers[J]. Journal of Electronics & Information Technology, 2003, 25(4): 473 – 479. (in Chinese)

[4] 周红,俞军,凌燮亭.混沌前馈型流密码的设计[J].电子学报,1998,26(1):98 – 101.
Zhou Hong, Yu Jun, Ling Xie-ting. Theoretical design of chaotic feed forward stream cipher[J]. Acta Electronic Sinica, 1998, 26(1): 98 – 101. (in Chinese)

[5] Frey D R. Chaotic digital encoding: an approach to secure communication[J]. IEEE Trans on CAS, 1993, 40(10): 660 – 666.

[6] Douglas R. Stinson 著,冯登国译.密码学原理与实践[M].北京:电子工业出版社,2003. 21 – 26.
Douglas R. Stinson. Cryptography theory and practice[M]. Beijin: House of Electronics Industry, 2003. 21 – 26. (in Chinese)

[7] 马在光,丘水生.基于广义猫映射的一种图像加密系统[J].通信学报,2003,24(2):51 – 57.
Ma Zai-guang, Qiu Shui-sheng. An image cryptosystem based on general cat map[J]. Journal on Communications, 2003, 24(2): 51 – 57. (in Chinese)

作者简介:

郭建胜　男,1972 年 4 月出生于河南沁阳,1997 年在河南大学数学专业获学士学位,2000 年和 2004 年在解放军信息工程大学电子技术学院获密码学硕士和博士学位,现为解放军信息工程大学副教授,主要研究方向是密码学和信息安全. E-mail: gjians@sina.com.

张　锋　男,1976 年 7 月出生于浙江湖州,解放军信息工程大学电子技术学院硕士生,主要研究方向是信息安全.