第32卷 第23期
Vol.32 No.23

计 算 机 工 程
Computer Engineering

2006年12月
December 2006

·安全技术·
文章编号：1000—3428(2006)23—0168—03 文献标识码：A 中图分类号：TP309.7

基于一维离散混沌映射的图像加密算法分析

李 力，朱从旭，陈志刚
(中南大学信息科学与工程学院，长沙 410083)

摘 要：指出文献[1]设计的加密算法中的替代变换算法不能抵抗已知明文攻击，由极少的明密文对就可求出密钥；且置换变换算法没有提供足够的密钥空间。据此提出了一种对该算法的攻击方案，并用实例对该加密算法进行攻击，证明攻击方案完全有效。同时，也提出了对该算法的改进建议。

关键词：混沌序列；序列密码；图像加密；SP 网络

Image Encryption Algorithm Cryptanalysis Based on One-dimensional Discrete Chaotic Map

LI Li, ZHU Congxu, CHEN Zhigang
(School of Information Science & Engineering, Central South University, Changsha 410083)

【**Abstract**】This paper points out that the substitute encryption algorithm proposed in reference1 cannot resist known-plaintext attack. The analyses show that the key of this cipher can be found with very few known plaintext-cipher pairs; and the permutation algorithm is only provided with very small key space. So an attack scheme is proposed, and the example of the attack scheme successfully brokes the encryption algorithm. A proposal for improvement algorithm is proposed, too.

【**Key words**】Chaotic sequences; Sequence cipher; Image encryption; SP network

基于迭代的混沌映射产生的伪随机序列有以下特性：(1)长周期。理论上伪随机序列没有重复值，但受计算机数据精度的限制，其周期要远小于计算机所能表示数据的个数。(2)初值敏感性。初始值的微小改变，经过一定次数的迭代后产生的序列值会完全不同。(3)系统参数敏感性。混沌系统参数的微小改变，经过若干次数的迭代后产生的序列与原序列完全不同。(4)序列的产生速度快。(5)遍历性。对值域中的任意值，都能在序列中找到与之无限接近的序列数。(6)不可预测性。只能对序列值短期预测，长期预测不可能。将混沌映射的这些特点应用于加密解密，产生的密码算法比现有的加密算法实现方便，加解密速度快，安全性高，使得近年来混沌密码的研究成为密码研究领域的一个热点[1~4]。近年来，很多学者提出了不同的混沌密码方案。有些算法有很高的安全性，但有些加密方案尚不够安全。

文献[1]提出了一种基于一维离散混沌映射的加密解密算法，具有简单快速、非线性、初始值敏感等特性。但本文指出这种算法存在一定的安全漏洞，在已知明文攻击下，很容易被攻破。

1 基于随机密钥及类标准映射的图像加密算法简介

该算法的结构类似于Feistel网络结构中的SP网络结构，分为替代变换和置换变换两部分，用于加密图像，图像为N×N的矩阵，I(i,j)为图像(i，j)点的像素值，L为图像的灰度级数。先对像素值I(i，j)进行替代变换，再对位置点(i，j)进行置换变换，迭代r轮后进行加解密[1]。

其中替代变换算法如下：

$$I'(i,j)=I(i,j)+K(i,j) \mod L \quad (1)$$

$$X_n=\sin^2(\theta\pi\eta^n) \quad n=1,2,3,\ldots,N^2 \quad (2)$$

$$\theta=\frac{1}{\pi}\sin^{-1}(\sqrt{x_0}) \quad (3)$$

$$Y_n=\frac{2}{\pi}\sin^{-1}(\sqrt{x_n}) \quad n=1,2,3,\ldots,N^2 \quad (4)$$

$$K(i,j)=round((L-1)Y_n) \quad n=1,2,3,\ldots,N^2 \quad (5)$$

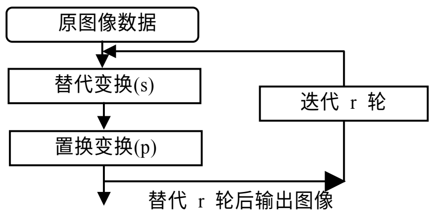

图1 原加密算法流程

加密过程，首先由混沌映射式(2)产生一个伪随机序列X_n，经过式(4)处理为一致分布的混沌序列，再经过式(5)转化为整数赋值给K(i,j)，最后由式(1)将像素值替代。其中，η>1且不大，密钥为(X_0,η)。

置换变换算法如下：

$$S1(i,j)=i+\varphi(j) \mod N \quad (6)$$

$$S2(i,j)=j+\phi(S1) \mod N \quad (7)$$

$$\varphi(x)=x+round(N*K_{1,n}) \mod N \quad n=1,2,3,\ldots,r \quad (8)$$

$$\phi(x)=x+round(N*K_{2,n}) \mod N \quad n=1,2,3,\ldots,r \quad (9)$$

$$K_{1,n}=\sin^2(b\arcsin(\sqrt{K_{1,n-1}})) \quad (10)$$

基金项目：湖南省自然科学基金资助项目(03JJY4054)

作者简介：李 力(1974－)，男，讲师、硕士生，主研方向：混沌密码学，信息安全；朱从旭，副教授；陈志刚，教授、博导

收稿日期：2006-03-03 **E-mail**：lili62_cn@163.com

$$K_{2,n}=a^{K_{2,n-1}} \bmod 1 \tag{11}$$

置换变换将像素从位置点(i，j)移位到(S1，S2)，r 为迭代的轮数，密钥为($k_{1,0}$,$k_{2,0}$,a,b)。算法流程如图 1 所示。

2 对该算法的分析

首先，分析该算法的置换变换，将置换变换中的式(8)和式(9)分别代入式(6)和式(7)，得

$$S1(i,j)=i+j+K_{1,1} \quad \bmod\ N \tag{12}$$

$$S2(i,j)=2*j+i+K_{1,1}+K_{2,1} \bmod\ N \tag{13}$$

由此可见，每一轮后，新位置点的一维顺序m_i都可以表示成i, j 和$k_{i,j}$的固定函数：

$$\begin{aligned}m_i&=((p(i,j)+q(K_{n1,n2})) \bmod N)\cdot N\\&+(p'(i,j)+q'(K_{n1,n2})) \bmod N\end{aligned} \tag{14}$$

其中p，p'为只含i,j变量的表达式且modN的函数，q，q'为只含$k_{n1,n2}$变量且modN的函数。

由式(14)可知迭代r轮后，新位置点的位置由q($k_{n1,n2}$)与q'($k_{n1,n2}$)确定，q($k_{n1,n2}$)与q'($k_{n1,n2}$)所有的不同值只有N×N个，即新位置点的不同种类也只有N×N个，而不是随机变换应有（N×N）!个。N×N是很小的一个数，使用穷举方法，几分钟就可找到正确的新位置点的位置。该算法的置换变换所提供的密钥空间太小，不能保证数据的安全性。

再分析替代变换算法，在算法中，该文作者使用了称之为“完全不可预测”的离散混沌映射式(2)，该文以及文献[4]认为该序列的下一个值不能由序列的以前值预测，并举例：η＝3/2，x_n，x_{n+1}可表示为

$$X_n=1-t^2 \tag{15}$$

$$X_{n+1}=\frac{1}{2}(1+t)(1-2t)^2 \tag{16}$$

-1<t<1，若想从X_n计算X_{n+1}则有两种可能：

$$X_{n+1}=\frac{1}{2}(1\pm(1-4X_n)\sqrt{1-X_n}) \tag{17}$$

因此从当前值不能预测下一个值。但该例只能证明当密码攻击者掌握的序列值不够多时，无法预测序列值。而当密码攻击者掌握的序列值足够多时完全可以求得式(2)中的θ与η。比如该例中，若密码攻击者知道从第 n 项开始的若干个序列值，则由式(2)知：

$$\theta\pi\eta^n=k\pi\pm\sin^{-1}(\sqrt{X_n}) \quad k\in Z^+ \tag{18}$$

由于$\theta\pi\eta^n$为一有限值，则式(18)的解集的个数有限，再由式(17)知对式(18)的解集，x_{n+1}有两种可能，则加入x_{n+1}的方程，解集的个数成倍减小，继续加入序列值，可以求出唯一的θ与η值(见表 1)。更糟糕的是，当密码攻击者掌握了序列的前 3 个点时，由于θ<1/2，η不大，则仅 3 个点就可求出θ与η(由于图像文件的格式标志处于文件头，这部分的明文容易猜出)。可见使用该一维离散混沌映射的替代算法也不安全。

又由式(1)知，由明密文对可推知k(i, j)，再由式(5)知，y_n约等于k(i, j)/(L-1)(当 L 很大时，比如对于L=2^{32}+1，并且数据使用单精度，则二者没有误差；而当L比较小时，可求密钥的前若干数位的值[6])，又由式(4)可求得x_n。由此可知由明密文对可推算出该一维离散混沌映射值(见式(19))。

$$\sum_{i=1}^{r-1}Y_i=\frac{I(i,j)-I'(i,j)+kL}{L-1} \quad k<r,k\in Z^+ \tag{19}$$

将式(2)和式(4)代入式(19)得

$$\begin{aligned}&\sum_{i=1}^{r}\frac{2}{\pi}\sin^{-1}(\sqrt{\sin^2(\theta\pi\eta^{m_i})})\\&=\frac{I(i,j)-I'(i,j)+kL}{L-1} \quad k<r,k\in Z^+\end{aligned} \tag{20}$$

其中m_i为该点在i轮时的顺序。式(20)可化简为式(21)。

表 1 方程解集的变化(η＝1.5，θ 为未知数)

序列点	方程 θ 的解集(K<=4)	解集的个数
X1=0.975 528 2	0.3 0.366 666 7 1.633 333 1.7 2.966 667 3.033 33 4.3 4.366 67	8
X2=0.726 995 3	0.3 1.633 333 2.966 667 4.3	4
X3=1.541 331e-3	0.3 2.966 667	2
X4=0.99 653 42	0.3	1

$$\begin{aligned}&\sum_{i=1}^{r}(-1)^{\mathrm{int}(2\theta\eta^{m_i})}(2\theta\eta^{m_i}-\mathrm{int}(2\theta\eta^{m_i})+\\&\frac{1}{2}(1-(-1)^{\mathrm{int}(2\theta\eta^{m_i})})=\frac{I(i,j)-I'(i,j)+kL}{L-1}\end{aligned} \tag{21}$$

int()为求整函数。将式(14)展开：

$$\begin{aligned}&m_i=p(i,j)\cdot N+p'(i,j)+q(K_{n1,n2})\cdot N+\\&q'(K_{n1,n2}) \quad or \quad m_i=p(i,j)\cdot N+p'(i,j)+\\&q(K_{n1,n2})\cdot N+q'(K_{n1,n2})-N^2 \quad or\\&m_i=p(i,j)\cdot N+p'(i,j)+q(K_{n1,n2})\cdot N+\\&q'(K_{n1,n2})-N \quad or \quad m_i=p(i,j)\cdot N+p'(i,j)+\\&q(K_{n1,n2})\cdot N+q'(K_{n1,n2})-N^2-N\end{aligned} \tag{22}$$

设q($k_{n1,n2}$)×N+q' ($k_{n1,n2}$)为T_i，则每一轮的顺序可由一个变量决定点的位置。

综合以上分析，对该加密算法可提出完整的已知明文攻击方法：

(1)对已知明文穷举 N×N 种密文位置，获得明密文对。

(2)每一个明密文对，推算出式(20)的右边的值(设为a_i)。

(3)每一个明密文对，对应一个方程，由所有的明密文对列出如式(21)的方程组。该方程组有 r+1 个未知数，则需要有 r+1 个明密文对，由于式(10)和式(11)的关系，未知数的个数不会随 r 的变化而增加，理想的情况下仅需 6 个方程就可求出任意 r 轮的密钥。

(4)使用牛顿迭代法或其它方法解此非线性方程组，求出T_i和θ，η。

(5)用解得的密钥解密图像，直到得到正确图像为止(见图 2)。

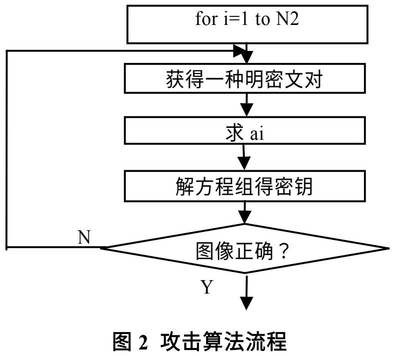

图 2 攻击算法流程

3 攻击实例

设r=2，θ=0.223 456 7，η=1.001 432，t_1=1($k_{1,1}$=0，$k_{2,1}$=1)，N=256，L=2^{32}+1，并且数据使用单精度，将图像pepper加密，如图 3(a)所示。已知图像点(0,0)，点(0,1)，点(1,0)的像素值，穷举 65 536 种密文位置后，由其中一种正确的明密文对推算出a_1=1.107 688 8,a_2=1.548 374 6,a_3=1.978 115 1 (a_1，a_2，a_3还可能等于 0.107 688 8，0.548 374 6，0.978 115 1 但获得的解不能解密图像)。列出的方程组如下：

$$
\begin{cases}
(-1)^{\mathrm{int}(2\theta\eta)}(2\theta\eta-\mathrm{int}(2\theta\eta))+ \\
(-1)^{\mathrm{int}(2\theta\eta^{t_1+1})}(2\theta\eta^{t_i+1}-\mathrm{int}(2\theta\eta^{t_1+1}))+ \\
\frac{1}{2}(2-(-1)^{\mathrm{int}(2\theta\eta)}-(-1)^{\mathrm{int}(2\theta\eta^{t_1+1})})=a_1 \\
(-1)^{\mathrm{int}(2\theta\eta^2)}(2\theta\eta^2-\mathrm{int}(2\theta\eta^2))+ \\
(-1)^{\mathrm{int}(2\theta\eta^{t_1+258})}(2\theta\eta^{t_i+258}-\mathrm{int}(2\theta\eta^{t_1+258}))+ \\
\frac{1}{2}(2-(-1)^{\mathrm{int}(2\theta\eta^2)}-(-1)^{\mathrm{int}(2\theta\eta^{t_1+258})})=a_2 \\
(-1)^{\mathrm{int}(2\theta\eta^6)}(2\theta\eta^6-\mathrm{int}(2\theta\eta^6))+ \\
(-1)^{\mathrm{int}(2\theta\eta^{t_1+257})}(2\theta\eta^{t_1+257}-\mathrm{int}(2\theta\eta^{t_1+257}))+ \\
\frac{1}{2}(2-(-1)^{\mathrm{int}(2\theta\eta^6)}-(-1)^{\mathrm{int}(2\theta\eta^{t_1+257})})=a_3
\end{cases}
\tag{23}
$$

使用牛顿迭代法，θ初值为 0.22，η初值为 1.001，t_1初值为 0，int(x)的导数为 0。求得结果为θ＝0.223 456 7，η＝1.025 432，t_1＝1，破译的结果如图 3(b)所示。结果完全正确，说明算法分析的攻击方法有效。

(a) 加密图像　　(b) 破译图像

图 3 加密图像与破译图像

4 建议改进方案

原算法的安全漏洞：(1)替代算法的混沌加密不能抵御已知明文攻击；(2)替换算法的混沌替换只提供了很小的密钥空间，不能抵抗穷举攻击。本文建议修改其替代变换算法和置换变换算法，首先使用分段线性映射式(24)经过多次迭代前馈的一维离散混沌算法[7]来代替式(2)的算法。

$$
X_{n+1}=\begin{cases} X_n/p, & 0\le X_n<p \\ (X_n-p)/(0.5-p), & p\le X_n<0.5 \\ F(1-X_n), & X_n\ge 0.5 \end{cases}
\tag{24}
$$

使用式(24)时，采用多次迭代进行前馈，即$X_{n+1}=F^m(x_n)$，迭代的次数m如果大于数据的实现精度，则可抵御已知明文攻击。事实上，即使攻击者知道多个经过m次迭代的混沌序列值，由于X_{n+1}与X_n之间可能的分段种类有 4^m种，比穷举密钥的次数还多，又任意X_{n+1}与X_n之间的分段都不同，lyapunov指数也求不出来，因此已知明文攻击无效。其次本文建议将置换算法进行如下修改：每轮迭代替换之前，由式(11)产生一个不同的混沌序列数，将其作为式(10)的初始值，由式(10)产生N^2个混沌序列数，将这N^2个不相等的混沌序列数由小到大排序，序列的原顺序与排序后顺序形成的一对一映射作为置换变换。新的置换变换的种类有$(N^2)!$个，穷举攻击完全无效。经过如上修改，该加密算法的安全性得到很大提高。

5 结论

通过已知明文攻击，对比于差分密码分析方法攻击DES需 2^{47}个明文[5]，而本文分析的算法只需要很少的已知明文密文对（如理想情况下只要 3 组）就能攻破原加密算法，说明该算法存在一定的安全漏洞。该文作者为该算法设置了 6 个实数的密钥，实际只提供了很小的密钥空间，没有起到应有的加密效果。本文建议修改其替代变换算法和置换变换算法，改进后的方案将大大提高该算法的安全性。

参考文献

1 李昌刚, 韩正之, 张浩然. 一种基于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): 465-410.

2 朱从旭, 陈志刚. 一种基于组合外密钥和明文的离散混沌密码算法[J]. 计算机工程与应用, 2004, 40(24): 91-93.

3 Alvarez G, Montoya F, Romera M. Keystream Cryptanalysis of A Chaotic Cryptographic Method[J]. Computer Physics Communications, 2004, 156(2): 205-207.

4 Jorge A G. Absoultely Unpredictable Chaotic Sequence[J]. International Journal of Bifurnation and Chos, 1999, 9(6): 1121-1135.

5 冯登国. 分组密码的分析和设计[M]. 北京: 清华大学出版社, 2000.

6 金晨辉. 一个基于混沌的分组密码算法的分析[J]. 中国工程科学, 2001, 3(6): 75-80.

7 周　红, 俞　军, 凌燮亭. 混沌前馈型流密码设计[J]. 电子学报, 1998, 26(1): 98-101.

8 Goce J, Ljupco K. Analysis of Some Rencently Proposed Chaos-based Encryption Algorithms[J]. Physics Letter A, 2001, 291(6): 381-384.

（上接第 158 页）

表 2 3 种算法实现 $GF(2^{83})$ 的比较+

算法	Les(个)	时间(μs)	反向时间(μs)	说明
1	999	13.50	2.96	未用桶移
2	650	3.10	2.42	
3	683	2.44	1.89	

在 Cantor 的论文中，113 位的求逆器平均需要 396 个周期，频率可以达到 96MHz，而使用的逻辑单元有 1 631 个。本文中采用改进的算法也实现了 113 位的求逆器，使用的逻辑单元仅有 910 个，频率可以达 100MHz，平均计算周期仅 300 个。Cantor 的数据表明，他在移位时使用了桶式移位器。然而，即使这样，4 个μs 左右的周期与本文相比也是较慢的。

4 总结

HECC 应用需要大量快速的模块，有限域求逆是其中非常重要的一个模块。优化的 MAIA 算法可以有效地利用随机数相邻两位为 0 的概率较大的这个特点，使用并行结构加速有限域的求逆运算。同时，优化的 MAIA 算法改进了以往算法，将 deg_*u* 和 deg_*v* 分开考虑的缺陷，省去了求 deg_*v* 的模块，节约了大量的芯片资源。进一步的研究可以考虑加大并行度，例如可以连续判断低 4 位的情况。另外，在硬件的实现上，如何使流程更合理，从而加大数据的吞吐量也是值得进一步研究的问题。总之，本文提出的算法，较以往的算法无论在速度上还是在面积上都有改进。相信这种改进的算法可以在今后的 HECC 实现中得到大量的应用。

参考文献

1 Hankerson D, Hernandez J L, Menezes A. Software Implementation of Elliptic Curve Cryptography over Binary Fields[C]. Proc. of the 2nd International Workshop on Cryptographic Hardware and Embedded Systems, Berlin, 2000: 1-24.

2 Clancy T. Analysis of FPGA-based Hyperelliptic Curve Cryptosystems[D]. Urbana-Champaign, Illinois: University of Illinois, 2002.

3 Chang H K, Soonhak K, Jong J K, et al. A New Arithmetic Unit in GF(2M) for Reconfigurable Hardware Implementation[M]. Berlin Heidelberg: Springer-Verlag, 2003.

4 张方国. 超椭圆曲线密码体制的研究[D]. 西安: 西安电子科技大学, 2001.