第33卷 第20期 计 算 机 工 程 2007年10月
Vol.33 No.20 Computer Engineering October 2007
·安全技术· 文章编号：1000—3428(2007)20—0165—02 文献标识码：A 中图分类号：TN918

CH混沌序列图像加密算法分析

张 斌，金晨辉
(信息工程大学电子技术学院，郑州 450004)

摘 要：分析了一个基于混沌序列的图像加密算法的安全性，发现该加密算法本质上是一个移位密码且密钥空间太小，利用古典密码中对移位密码的分析方法得到混沌序列，进而给出了穷举参数求解其密钥的已知明文攻击方法。对于大小为 $M\times N$ 的明文图像，该攻击方法的计算复杂性为 $O(M+N)$。理论分析和实验结果均表明该图像加密算法是不安全的。

关键词：混沌密码；图像加密；密码分析；已知明文攻击

Analysis of CH Chaos Sequence-based Image Encryption Algorithm

ZHANG Bin, JIN Chen-hui
(Institute of Electronic Technology, University of Information Engineering, Zhengzhou 450004)

【Abstract】 The security of a chaos sequence-based image encryption and decryption algorithm is analyzed. The encryption algorithm is a shift cipher essentially and its key space is too small. The chaotic sequence is obtained by using the analysis method of shift cipher of classical cipher. A known plaintexts attack is proposed by exhaustive parameter search. For a $M\times N$ plain image, the computing complexity is $O(M+N)$. From the analysis in theory and experimental results, this image encryption algorithm is proved insecure.

【Key words】 chaotic cipher; image encryption; cryptanalysis; known plaintexts attack

混沌密码作为一类新型的密码技术，近年来得到了广泛的研究。混沌密码算法主要分为模拟混沌加密算法[1]和数字混沌加密算法[2~4]。数字混沌加密算法既包括序列密码算法[5~7]也包括分组密码算法[8]以及公钥密码算法[9]。目前，在数据加密、图像加密[10~11]和数字水印[12~14]等领域中出现了很多混沌密码算法。文献[11]提出了一个基于混沌序列的图像加密算法(CH图像加密算法)，它利用混沌映射产生混沌序列，由混沌序列决定图像像素点的位置置换从而实现对图像的加密。

已知明文攻击是假定攻击者除了已知加密体制，还能获得由同一密钥加密的若干明文及对应的密文，在此条件下求解密钥的攻击就是已知明文攻击。因此，对图像加密算法进行已知明文攻击时，攻击者除了已知图像加密算法，还可得到若干明文图像及在同一密钥加密下对应的密文图像。

1 基于混沌序列的图像加密算法介绍

基于混沌序列的图像加密算法采用混沌映射：

$$f(x)=\begin{cases}\lceil (m/a)x\rceil, 1\le x\le a\\ \lfloor m(m-x)/(m-a)\rfloor, a<x\le m\end{cases}$$

其中，$x,a\in\{1,2,\cdots,m\}$；$\lceil z\rceil$，$\lfloor z\rfloor$ 分别表示不小于 z 的最小整数和不大于 z 的最大整数。

定义 设 $F^1(x)=f(x)$，$F^n(x)=F(F^{n-1}(x))$，则称 $F^n(x)$ 为函数 $f(x)$ 的 n 次迭代函数。

基于混沌序列的图像加密算法的密钥包括混沌映射的初态x_0、参数a和迭代次数n，而混沌映射的参数m及原始图像的宽度M和长度N均为算法给定的参数。

基于混沌序列的图像加密算法包括3个步骤：

(1)用密钥 (x_0,a,n) 对函数 $F^n(x)$ 初始化，由 $x_{k+1}=F^n(x_k)$ 生成混沌序列 $x_0,x_1,\cdots,x_{M+N-1}$。

(2) $M\times N$ 大小的原始图像 $I_R=\{g_{i,j}:0\le i\le M-1,0\le j\le N-1\}$。其中，$g_{i,j}$ 为 (i,j) 点的灰度值。对于 $0\le i\le M-1$，将 I_R 第 i 行的像素点循环右移 x_i 位。得到的图像记为 $I_R'=\{g_{i,j}':0\le i\le M-1,0\le j\le N-1\}$，其中，$g_{i,j}'$ 为 (i,j) 点的灰度值。

(3)对于 $0\le j\le N-1$，将步骤(2)得到的图像 I_R' 的第 j 列的像素点循环下移 x_{M+j} 位，所得的图像 I_E 即为密文图像，记为 $I_E=\{g_{i,j}^e:0\le i\le M-1,0\le j\le N-1\}$，其中，$g_{i,j}^e$ 为 (i,j) 点的灰度值。

说明：文献[11]中指出若原始图像为256色，则 $m=256$。即 m 的取值为明文图像的颜色数。

2 图像加密算法的信息泄漏规律及已知明文攻击

基于混沌序列的图像加密算法本质上是利用密钥产生一个移位密码，对移位密码的分析在古典密码中已经解决。移位密码实际上对应于一个位置置换表，故该置换表就是密码算法的等效密钥。下面给出两个对该移位密码的分析方法。

方法 1 假设攻击者可以得到足够多的明文图像及对应的由同一密钥加密的密文图像。

不妨设攻击者可得到 t 组明密文图像。记 $A_{r,s}$ 是第 r 个密文图像中出现第 r 个明文图像中的第 s 个($0\le s\le M\times N-1$)像素灰度值的位置全体构成的集合，令 $A_s=\bigcap_{r=1}^{t}A_{r,s}$，则当 A_0，A_1，…，$A_{M\times N-1}$ 都是单点集合时，该移位密码对应的置换表

基金项目：河南省杰出青年科学基金资助项目(0312001800)
作者简介：张 斌(1982－)，男，硕士研究生，主研方向：密码学；金晨辉，教授、博士生导师
收稿日期：2006-10-26 **E-mail**：dzjszhangbin@126.com

就可确定。因此只要 t 足够大就可实现对该移位密码的破译。根据加密算法知，由位置置换表可解得混沌序列 $x_0, x_1, \cdots, x_{M+N-1}$。

方法 2 假设攻击者只能得到一幅明文图像及对应的密文图像。

在下面的讨论中，将 $M\times N$ 的图像视为灰度矩阵而不加区分，即 $\boldsymbol{I}=[g_{i,j}]_{M\times N}$，其中，$g_{i,j}$ 为 (i, j) 点的灰度值。记明文图像 I_R 的第 i 个 N 维行向量为 $\boldsymbol{\alpha}_i$；密文图像 I_E 的第 j 个 M 维列向量为 $\boldsymbol{\beta}_j$。

由加密算法知，明文图像 I_R 的第 i 行 $\boldsymbol{\alpha}_i$ 循环右移 x_i 位，不妨记为 $\boldsymbol{\alpha}_i'$，则 $\boldsymbol{\alpha}_i'$ 的 N 个像素灰度值一定从左到右依次出现在密文图像的 N 列中。由于 $x_M, x_{M+1}, \cdots, x_{M+N-1}$ 未知，因此 $\boldsymbol{\alpha}_i'$ 的 N 个像素灰度值具体位于密文图像的哪一行并不能确定。据此可以对 x_i 的 m 种可能取值 x_i' 依次检验。若 x_i' 穷举正确，则对明文图像第 i 行 $\boldsymbol{\alpha}_i$ 循环右移 x_i' 位后的 $\boldsymbol{\alpha}_i'$ 的 N 个像素灰度值一定从左到右依次出现在密文图像的 N 列中；若穷举错误，则对明文图像第 i 行 $\boldsymbol{\alpha}_i$ 循环右移 x_i' 位后的 $\boldsymbol{\alpha}_i'$ 的 N 个像素灰度值不一定从左到右依次出现在密文图像的 N 列中，以此为依据就可得到 x_i 的候选值。同理，对密文图像第 j 列 $\boldsymbol{\beta}_j$ 循环上移 x_{M+j}' 位与明文图像中 M 行像素灰度值对比可得到 x_{M+j} 的候选值。

算法 1

Step1 对于 $0\le i\le M-1$，攻击 x_i。对 x_i 的每个可能值 x_i'，将明文图像的第 i 行 $\boldsymbol{\alpha}_i$ 循环右移 x_i' 位得到 $\boldsymbol{\alpha}_i'$，若 $\boldsymbol{\alpha}_i'$ 的 N 个像素灰度值均从左到右依次出现在密文图像的 N 列中，则将 x_i' 作为 x_i 的候选值；否则对 x_i 的下一个可能值进行检验。

Step2 对于 $0\le j\le N-1$，攻击 x_{M+j}。对 x_{M+j} 的每个可能值 x_{M+j}'，将密文图像的第 j 列 $\boldsymbol{\beta}_j$ 循环上移 x_{M+j}' 位，不妨设为 $\boldsymbol{\beta}_j'$，若 $\boldsymbol{\beta}_j'$ 的 M 个像素灰度值从上到下依次出现在明文图像的 M 行中，则将 x_{M+j}' 作为 x_{M+j} 的候选值；否则对 x_{M+j} 的下一个可能值进行检验。

Step3 用 Step1 及 Step2 所产生的混沌序列的候选值加密明文图像，若得到的图像与密文图像一致，则输出混沌序列，算法结束；否则检验下一个可能的混沌序列。

说明：算法 1 穷举混沌状态 x_i 的每个可能值时，只需对上个可能值对应的 $\boldsymbol{\alpha}_i'$ 循环右移 1 位，并没有必要每次都对明文图像的 $\boldsymbol{\alpha}_i$ 循环右移 x_i' 位，从而避免重复运算。

定理 1 算法 1 得到混沌序列的成功率为 1，穷举复杂性为 $m(M+N)$。

证明 由于算法 1 的各步骤均不漏掉混沌序列的每个可能值，因此一定可以找出正确的混沌序列，即算法 1 的成功率为 1。

由于对 x_i 的 m 个可能值均依次检验，因此算法 1 的穷举复杂性为 $m(M+N)\in O(M+N)$。

至此，可以得到混沌序列 $x_0, x_1, \cdots, x_{M+N-1}$，即该图像加密算法的等效密钥。下面给出求解密钥 a 和 n 的方法。

算法 2

Step1 令 d=10。

Step2 对密钥 a 的每个可能值 a’，由 x_0 及 a’对混沌映射 $f(x)$ 初始化并进行迭代。若某次迭代后的函数值为 x_1，则将 a’及迭代次数 n’作为密钥 a 和 n 的候选值；若迭代次数大于 d 且函数值始终不等于 x_1，则检验 a 的下一个可能值。

Step3 若 Step2 没有产生密钥 a 和 n 的候选值，则令 d=d+10 并返回 Step2；否则执行 Step4。

Step4 用密钥 a 和 n 的候选值产生混沌序列，若该混沌序列与 $x_0, x_1, \cdots, x_{M+N-1}$ 一致，则判定该候选值为正确密钥，算法结束。若所有的候选值所产生的混沌序列均与 $x_0, x_1, \cdots, x_{M+N-1}$ 不一致，则令 d=d+10 并返回 Step2。

说明：算法 2 在实现时可建立一个大小为 m 的数组用于存储密钥 a 的每个可能值 a’对应的混沌迭代状态，这样当 Step4 执行 $d=d+10$ 并返回 Step2 后，在以 a’为参数进行迭代时仅需以对应数组中的混沌状态为起点，并没有必要以 x_0 为起点重复计算。

定理 2 算法 2 的成功率为 1，穷举复杂性为 $O(m)$。

证明 由于算法 2 对密钥 a 的所有可能值均进行穷举且对 n 由小到大依次穷举，因此一定可以求出密钥 a 和 n，即算法 2 的成功率为 1。

由于 n 是混沌映射的迭代次数，n 的大小决定了混沌序列产生的快慢，从而决定了图像加密算法的速率的快慢。事实上，现代保密通信中对加密算法的加密效率均有较高要求，因此 n 不可能很大。这里假设 n 的合理取值范围是 $1\le n\le 100$。此时，算法 2 的穷举复杂性为 $100m\in O(m)$。至此，已经求出了基于混沌序列的图像加密算法的全部密钥 (x_0, a, n)。

3 实验

本文做了一例攻击实验。图 1 为 512×512 的明文图像 Lena.bmp，取密钥 $x_0=35, a=94, n=6$，图 2 为密文图像。明文图像为 512×512 的 256 色灰度图，因此参数 $m=256$，$M=N=512$。

图 1 明文图像

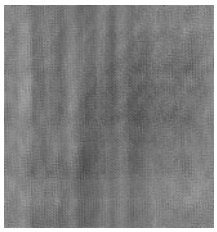

图 2 密文图像

利用算法 1 得到 $x_0, x_1, \cdots, x_4$ 均有 5 个候选值，x_{510}, x_{511} 均有 2 个候选值，混沌序列的其余 1 017 个值均只有 1 个候选值。利用 $x_{512}, x_{513}, \cdots, x_{1023}$ 对密文图像进行列变换得到图像 I_R'。用 x_0 的候选值分别对明文图像第 0 行做行变换并与 I_R' 的第 0 行比较就可得到 x_0 的正确值。利用同样的方法就能很快得到混沌序列。再利用算法 2 最终得到密钥 a 和 n 的正确值。在主频为 2.5GHz 的 Pentium 4 PC 机上，攻击算法所用时间不足 1min。

参考文献

1 Vaidya P G, Anand S. Cryptography Based on Chaotic Synchro-is ization: Round III[DB/OL]. (2005-07). http://eprint.iacr.org/2005/273.

2 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.

(下转第 169 页)