文章编号:1671-8860(2010)05-0546-04　　文献标志码:A

对一种混沌图像密码的选择明文攻击

刘　婷[1]　闵乐泉[1,2]

(1　北京科技大学信息工程学院,北京市海淀区学院路 30 号,100083)
(2　北京科技大学应用科学学院,北京市海淀区学院路 30 号,100083)

摘　要:对基于广义猫映射和加法模运算的混沌密码进行了安全性分析,指出了该密码设计上的几处瑕疵。在选择明文攻击下,该密码系统在 1 轮加密时不够安全,仅选择 3 幅明文图像就可破译。讨论了该密码在多轮加密时待解决的问题以及可能采取的改进措施。

关键词:混沌图像密码;密码分析;Kerckhoffs 准则;选择明文攻击
中图法分类号:TP309

计算机网络技术的快速发展增加了对快速安全的图像加密方法的需求。由于混沌系统具有密码学的很多基本性质,如非周期性、对初值的敏感性、遍历性和长期不可预测性,因此,基于混沌的图像密码算法的研究受到广泛关注[1-5]。对一些混沌图像密码系统的安全性分析表明,它们能够抵抗统计分析[1-5]、密钥敏感性分析[1,3-5]、像素相关性分析[1,3,5]和差分攻击[3]等。而部分系统不能抵抗其他的一些攻击[6-9],如已知明文攻击[7]和选择明文攻击[8]等。

安全的混沌密码系统必须能够抵抗现代密码学分析方法的攻击。现代密码学通常假设密码分析者知道密码系统的设计和工作原理[10],即秘密全寓于密钥中(Kerckhoffs 准则)。本文在 Kerckhoffs 准则下,从选择明文攻击出发分析了该算法的安全性。

1　基于广义猫映射的图像密码算法

文献[1]设计的图像密码算法由两部分组成,分别对应着置乱过程和扩散过程。该图像加密算法描述如下:① 生成密钥;② 置乱过程;③ 扩散过程;④ 若满足迭代轮数要求,则输出密文图像;否则,根据安全需要重复步骤①～③。

上述算法存在如下问题:

1) 没有给出对图像的各个像素进行置乱和扩散的先后顺序,这对本文的分析没有影响。不妨假设该算法按照行优先的顺序对图像像素进行置乱和扩散。

2) 没有给出具体的迭代轮数。本文主要分析 1 轮图像的加密过程,重构它的置乱密钥和扩散密钥,以此为例论述该类图像加密系统的安全性问题。

3) 在加密图像时,扩散部分进行了两次扩散操作。在第二次扩散过程中,对 q_0 的取值作了如下说明:取前一次扩散过程产生的密文的第 N 行第 N 列像素灰度值。但是对 p_{N^2+1} 如何取值没有说明。如果 p_{N^2+1} 也从第一次扩散产生的密文图像中选取,将导致接收者无从解密。因为接收者除了知道密钥之外,从公共信道上接收的只有经过两次扩散过程之后的密文图像,并没有第一次扩散之后产生的密文。这样对于接收者来说,用于解密第二次扩散过程所需要的 p_{N^2+1} 和 q_0 是未知的,因此接收者无法解密。为了解决这个问题,在每轮加密过程中增加两个扩散密钥 g_i 和 h_i,用于每轮的第二次扩散加密,其中,g_i、h_i 取[0,L)上的整数。在步骤① 中,增加产生密钥 g_i、h_i;在步骤②中,增加把扩散密钥 g_i、h_i 分别赋给第二次扩散过程中的 p_{N^2+1}、q_0。密码分析时,本文也把恢复密钥 g_i、h_i 作为任务。

4) 没有说明如何生成置乱密钥和扩散密钥,以保证加密系统的安全性。

收稿日期:2010-03-15。
项目来源:国家自然科学基金资助项目(60674059,60773120)。

2　选择明文攻击

对基于广义猫映射和加法模运算的密码系统的安全性分析依赖于两个事实:① 如果明文图像由相同的像素灰度值组成,则 Arnold 置乱变换实际上没有起到作用。分析者可以选择具有相同像素灰度值的明文图像分析扩散过程。② 如果明文图像的像素灰度值均为零,那么扩散过程起到的作用亦不大,分析者可以联合两幅只有一个非零像素的明文图像分析 Arnold 置乱过程。注意,置乱过程与扩散过程能够通过选择特殊的明文图像分开来分析,因为它们是相互独立的。

2.1　对扩散过程的分析

定理 1[11]　设 $N\geqslant 1$,$\Delta=ad-bc$,$\gcd(\Delta,N)=1$,那么,二元一次同余方程组为:

$$\begin{cases} ax+by=e(\mathrm{mod}N) \\ cx+dy=f(\mathrm{mod}N) \end{cases} \tag{1}$$

对模 N 有惟一解:

$$\begin{cases} x=\Delta^{-1}(de-bf)(\mathrm{mod}N) \\ y=\Delta^{-1}(af-ce)(\mathrm{mod}N) \end{cases} \tag{2}$$

其中,$\Delta^{-1}\Delta=1(\mathrm{mod}N)$。

置乱过程只是改变了图像像素的位置,并没有改变像素灰度值。若分析者输入一幅像素值全为零的明文图像 P_1,则置乱后的图像 P_2 与置乱前的图像 P_1 完全相同。至此,安全性仅依赖于扩散过程。

假设图像密码系统处理的图像 $N=256$,$L=256$,扩散密钥 $b_1=65$,$e_1=123$,$g_1=237$,$h_1=189$(该密钥不为分析者所知),输入像素全为零的明文图像 P_1,输出对应的密文图像为 Q_1。利用 P_1 和 Q_1 可以重构扩散密钥。详细过程如下:

1) 第一次扩散过程。由 P_1、P_2 均为零矩阵知,$p_i=0(i=1,2,\cdots,N^2)$,而且 $p_{N^2+1}=b_1$,$q_0=e_1$,根据式(2)得到 $q_1=e_1$,$q_2=e_1$,$\cdots$,$q_{N^2-1}=e_1$,$q_{N^2}=(b_1+e_1)\mathrm{mod}256$,即为第一次扩散后的密文图像$Q_1'$。

2) 第二次扩散过程。图像 Q_1' 作为第二次扩散过程的输入,则 $p_1=e_1$,$p_2=e_1$,$\cdots$,$p_{N^2-1}=e_1$,$p_{N^2}=(b_1+e_1)\mathrm{mod}256$。而 $p_{N^2+1}=g_1$,$q_0=h_1$,根据式(2)可以得到 $q_1=(2e_1+h_1)\mathrm{mod}256$,$q_2=(4e_1+h_1)\mathrm{mod}256$,$\cdots$,$q_{N^2-1}=(b_1-2e_1+h_1)\mathrm{mod}256$,$q_{N^2}=(2b_1-e_1+g_1+h_1)\mathrm{mod}256$,即为第二次扩散后的密文图像 Q_1。

明文图像 P_1 的 1 轮加密过程如图 1 所示。图 1 (a)为像素灰度值全为零的明文图像 P_1;图 1(b)为经过 Arnold 变换置乱后的图像 P_2;图 1(c)为扩散密钥 $b_1=65$、$e_1=123$ 时,经过第一次扩散加密后的图像 Q_1';图 1(d)为扩散密钥 $g_1=237$、$h_1=189$ 时,经过第二次扩散加密后的图像 Q_1。

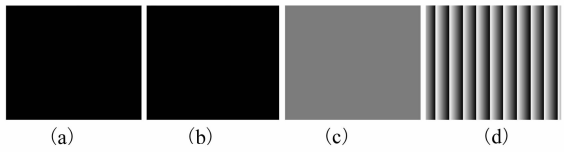


图 1　像素值均为零的明文图像的 1 轮加密过程

Fig. 1　One-round Encryption Process for Black Plain-image

由于 Q_1 是加密系统的输出图像,为分析者已知,故只需选取图像 Q_1 第一行的前两个像素值 179、169 和第 N 行的最后两个像素值 8、177,就可以求解下列两个方程组:

$$\begin{cases} 2e_1+h_1=179\mathrm{mod}256 \\ 4e_1+h_1=169\mathrm{mod}256 \end{cases} \tag{3}$$

$$\begin{cases} b_1-2e_1+h_1=8\mathrm{mod}256 \\ 2b_1-e_1+g_1+h_1=177\mathrm{mod}256 \end{cases} \tag{4}$$

方程组(3)在 $Z/(256)$ 上有两组解,分别将其代入方程组(4),由定理 1 得到两组扩散密钥为 $b_1^{(1)}=65$,$e_1^{(1)}=123$,$g_1^{(1)}=237$,$h_1^{(1)}=189$ 和 $b_1^{(2)}=65$,$e_1^{(2)}=251$,$g_1^{(2)}=109$,$h_1^{(2)}=189$。

对于一个密码系统,设 K 是密钥空间,SP 是明文空间,SQ 是密文空间,E 是加密函数,E^{-1} 是解密函数。若存在密钥 k_1,$k_2\in K(k_1\neq k_2)$,对于任意的明文 $P\in$SP,均有 $E_{k_1}(P)=E_{k_2}(P)$ 成立,则 k_1、k_2 是这个密码系统的等效密钥。

命题　$b_1^{(1)}=65$,$e_1^{(1)}=123$,$g_1^{(1)}=237$,$h_1^{(1)}=189$ 和 $b_1^{(2)}=65$,$e_1^{(2)}=251$,$g_1^{(2)}=109$,$h_1^{(2)}=189$ 是扩散操作的等效密钥。

2.2　对置乱过程的分析

定义　设矩阵 $\boldsymbol{A}$ 是整数集 Z 上的二维变换,矩阵 $\boldsymbol{B}$ 是 $Z/(N)$ 上的二维变换,其中 N 是正整数。如果对于任意的 $(x_0,y_0)\in Z/(N)\times Z/(N)$,均有下式成立:

$$\boldsymbol{A}\begin{bmatrix} x_0 \\ y_0 \end{bmatrix}\mathrm{mod}N=\boldsymbol{B}\begin{bmatrix} x_0 \\ y_0 \end{bmatrix}\mathrm{mod}N$$

则称 $\boldsymbol{B}$ 是 $\boldsymbol{A}$ 在 $Z/(N)$ 上的等效变换。

定理 2　$\boldsymbol{B}$ 是 $\boldsymbol{A}$ 在 $Z/(N)$ 上的等效变换的充要条件是 $(\boldsymbol{A}-\boldsymbol{B})\equiv\boldsymbol{0}\mathrm{mod}N$。

向图像加密系统输入一幅明文图像,输出即为密文图像,则该明文图像经置乱变换之后的图像可以通过上节得到的扩散密钥解密密文图像获

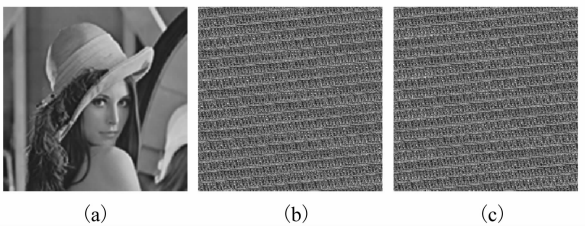
得。若输入的明文图像只有一个非零像素,其他像素灰度值均为零,则这个非零像素经置乱变换之后的位置就可以通过解密扩散过程得知,从而确定置乱变换的参数。

对于 $N=256$、$L=256$ 的图像,假设置乱密钥为 $u_1=57$,$v_1=119$(该密钥不为分析者所知),扩散密钥为 $b_1=65$,$e_1=123$,$d_1=237$,$c_1=189$(已由3.1节分析得到,由于两组扩散密钥为等效密钥,任取其中一组即可)。分析者分别输入只在(1,0)位置有一个非零像素的明文图像 $P_1^{(1)}$ 和只在(0,1)位置有一个非零像素的明文图像 $P_1^{(2)}$,输出对应的密文图像为 $Q_1^{(1)}$ 和 $Q_1^{(2)}$。用扩散密钥分别对密文图像 $Q_1^{(1)}$ 和 $Q_1^{(2)}$ 进行扩散解密操作,得到置乱变换后的图像 $P_2^{(1)}$ 和 $P_2^{(2)}$,则 $P_2^{(1)}$ 和 $P_2^{(2)}$ 中非零像素的位置(x_1,y_1)和(x_2,y_2)通过查找容易确定。

由上述两组图像在置乱变换前后非零像素对应的位置,定义广义 Arnold 变换矩阵 $\boldsymbol{A}$ 的等效变换为 $\boldsymbol{A}_1=\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}$,其中 $a_{11},a_{12},a_{21},a_{22}\in Z/(N)$。

由实验得知,图像 $P_2^{(1)}$ 和 $P_2^{(2)}$ 中非零像素的位置(x_1,y_1)和(x_2,y_2)分别为(1,119)和(57,128),因此 $a_{11}=1$,$a_{12}=57$,$a_{21}=119$,$a_{22}=128$。由定理2知,必然有$(\boldsymbol{A}-\boldsymbol{A}_1)\equiv\boldsymbol{0}\bmod 256$ 成立。等效变换 $\boldsymbol{A}_1$ 中的57和119就是置乱密钥。

同时,也可以通过置乱图像来验证,经过广义Arnold变换,$\boldsymbol{A}$ 的图像与经过等效变换 $\boldsymbol{A}_1$ 的图像完全相同,如图2所示。图2(a)是明文Lenna图像;图2(b)是经过广义Arnold变换 $\boldsymbol{A}$ 置乱之后的密文图像,其中 $u=57$,$v=119$;图2(c)是经过等效变换 $\boldsymbol{A}_1$ 置乱之后的密文图像。通过像素灰度值求差计算,图2(b)和图2(c)完全相同。



(a) (b) (c)

图2 Lenna图像的置乱变换

Fig. 2 Scrambling Transformation for Lenna Image

3 结 语

由前面的分析得知,在加密轮数为1时,通过一幅像素灰度值全为零的图像 P_1,只在(1,0)位置有一个非零像素的图像 $P_1^{(1)}$ 和只在(0,1)位置有一个非零像素的图像 $P_1^{(2)}$,这3幅明文图像能够获得置乱密钥和扩散密钥。不能抵抗选择明文攻击的原因在于,该密码系统的置换过程和扩散过程相互独立。若采用增加加密轮数的方法来提高安全性,具体轮数的选择需要严格证明,以平衡加密速度与安全性之间的矛盾。对多轮加密系统,若每轮使用不同的密钥,这相当于一次一密密码。一次一密的密码系统绝对安全,但是必须攻克密钥管理和密钥分配等问题。目前,这些问题阻碍了一次一密密码在实际安全通信中的应用[12]。

此外,还可以使得密钥流依赖于明文或密文,而无需改变密钥。这样设计的加密系统类似于分组密码的CBC模式(cipher-block chaining)或PCBC模式(propagating cipher-block chaining)。这种解决方案比一次一密模式更加实用,因为它们具备足够的安全性,并能够应用于实际[12]。通过改变加密流程的模式,可以增强类似文献[1]中混沌图像加密系统的安全性。

参 考 文 献

[1] 石熙,张伟. 基于广义猫映射和加法模运算的快速图像加密系统[J]. 计算机科学,2008,35(6):91-291

[2] 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

[3] Chen G R, Mao Y B, Chui C K. A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps[J]. Chaos, Solitons and Fractals, 2004, 21: 749-761

[4] Guan Z H, Huang F J, Guan W J. Chaos-based Image Encryption Algorithm[J]. Physics Letter A, 2005, 346: 153-157

[5] Gao T G, Chen Z Q. A New Image Encryption Algorithm Based on Hyper-chaos [J]. Physics Letter A, 2008, 372: 394-400

[6] Lvarez G, Montoya F, Romera M, et al. Keystream Cryptanalysis of a Chaotic Cryptographic Method [J]. Computer Physics Communications, 2004, 156:205-207

[7] 郭建胜,金晨辉. 对基于广义猫映射的一个图像加密系统的已知图像攻击[J]. 通信学报,2005,26(2):131-135

[8] Wang K, Pei W J, Zou L H, et al. On the Security of 3D Cat Map Based Symmetric Image Encryption Scheme [J]. Physics Letters A, 2005, 343: 432-

439
[9] Xiao D, Liao X F, Wei P C. Analysis and Improvement of a Chaos-based Image Encryption Algorithm [J]. Chaos, Soliton and Fractals, 2009, 40(5): 2 191-2 199
[10] 冯登国. 密码分析学[M]. 北京: 清华大学出版社, 2000
[11] 潘承洞, 潘承彪. 初等数论[M]. 北京: 北京大学出版社, 1992:176-177
[12] Rhouma R, Belghith S. Cryptanalysis of a New Image Encryption Algorithm Based on Hyper-chaos [J]. Physics Letter A, 2008, 372: 5 973-5 978

第一作者简介:刘婷,博士生,研究方向为信息安全与保密通信。
E-mail:tingliu1984@163.com

Chosen-plaintext Attack on a Chaotic Image Cipher

LIU Ting[1]　*MIN Lequan*[1,2]
(1 School of Information Engineering, University of Science and Technology Beijing, 30 Xueyuan Road, Haidian District, Beijing 100083, China)
(2 School of Applied Science, University of Science and Technology Beijing, 30 Xueyuan Road, Haidian District, Beijing 100083, China)

Abstract: The security of the chaotic cryptosystem based on general cat map and additive modular arithmetic is studied. Several weaknesses of the cipher are pointed out. By choosing three plaintexts, the one-round cryptosystem can be broken. The problems to be solved in the cryptosystem and possible improved methods are discussed.
Key words: chaotic image cipher; cryptanalysis; Kerckhoffs principle; chosen-plaintext attack

About the first author: LIU Ting, Ph.D candidate, majors in information security, secure communication.
E-mail: tingliu1984@163.com

(上接第 515 页)

A QoS Based Fault-Tolerant Topology Control Algorithm for Ad Hoc Network

WANG Dong[1]　*LI Fa*[1]　*LI Xiaohong*[1]
(1 School of Computer and Communication, Hunan University, 252 South Lushan Road, Changsha 410082, China)

Abstract: A fault-tolerant topology control algorithm of QoS guarantee, referred to as the AIFT, is proposed. The new algorithm generates K connected topology, and optimizes interference furthest. The simulation results show that AIFT decreases interference and improves the capacity of network.
Key words: ad hoc networks; fault-tolerant topology control; QoS

About the first author: WANG Dong, professor, Ph.D, majors in network test and performance evaluation, wireless communications and mobile computing, etc.
E-mail: wangd@hnu.cn