文章编号:1001 - 9081(2010)07 - 1815 - 03

一种基于 Logistic 混沌序列的图像置乱算法的安全分析

肖　迪[1,2],赵秋乐[2]
(1. 重庆大学 计算机学院, 重庆 400044; 2 重庆大学 机械工程学院, 重庆 400044)
(dixiao@ cqu. edu. cn)

摘　要:分析最近由袁玲等人提出的一种基于 Logistic 混沌序列和位交换的图像置乱算法所存在的脆弱性,提出必须使得混沌密钥序列的产生过程与明文本身建立起联系的改进建议。通过提出的已知明文/选择明文攻击这两种方法,可以方便地获得该算法的等效密钥。理论分析和仿真实验证明:原算法存在安全隐患,易受攻击,有待加强安全性。

关键词:图像安全; 混沌加密; 已知明文攻击; 选择明文攻击
中图分类号: TP309. 7　　**文献标志码**:A

Cryptanalysis of an image scrambling algorithm based on Logistic chaotic sequence

XIAO Di[1,2], ZHAO Qiu-le[2]
(1. *College of Computer, Chongqing University, Chongqing* 400044, *China*;
2. *College of Mechanical Engineering, Chongqing University, Chongqing* 400044, *China*)

Abstract: Aiming to analyze the potential vulnerability of a recently proposed image scrambling algorithm based on Logistic chaotic sequence and bit exchange, this paper gave out the corresponding improving ideas and got rid of the flaw of the algorithm application. Through known-plaintext attack and chosen-plaintext attack, the equivalent keys of the algorithm could be easily recovered. Both theoretical analysis and computer simulation indicate that the proposed attacks can completely break this algorithm and cause damage.

Key words: image security; chaotic encryption; known-plaintext attack; chosen-plaintext attack

0　引言

作为数字媒体的一个极其重要的组成部分,数字图像的安全性研究得到了广泛的关注。由于传统的加密方法对图像并不是特别适应,因此将混沌引入图像安全领域是一个很有潜力的思路[1-10]。文献[10]中提出一种新的基于混沌序列和位交换的图像置乱算法。算法根据各像素点的位置,采用不同的 Logistic 混沌序列和像素值的二进制序列进行异或操作改变图像像素值,并利用图像本身的自相关性进行加密,可有效地实现图像置乱。然而,该算法在设计上存在安全漏洞,可通过已知明文/选择明文攻击获取等效密钥。本文将对此进行详细分析,并提出改进建议。

1　原算法简介

算法密钥包括:Logistic 映射的初值 x_0 和参数 μ 及决定舍弃序列前面若干项数的参数 t。

1.1　生成混沌密钥序列

根据选定的 Logistic 映射 $x_{k+1} = \mu x_k(1 - x_k)$ 的初值 x_0 和参数 μ,迭代生成一个混沌序列,二值化后得到一个二值混沌序列 s。再根据用户指定的密钥值 t,舍弃序列 s 的前 t 项,获得需要的混沌密钥序列 $s = \{s_{t+1}, s_{t+2}, \cdots, s_{t+M+N+L}\}$,其中,$M$ 和 N 为待加密图像的大小,L 为待加密图像中每个像素的位平面数。为方便起见,混沌密钥序列可简记为 $s = \{s_1, s_2, \cdots, s_{M+N+L}\}$。

1.2　根据像素点位置选取子序列并进行逐像素加密

原算法对图像的每个像素的处理是相互独立的。首先通过位分解使每个像素变为 L 位二进制数,并在序列 s 中,根据每个像素点 $C(m,n)$($m \in [1,M]$, $n \in [1,N]$)的位置选取子序列 $sp = \{s_{m+n+1}, s_{m+n+2}, \cdots, s_{m+n+L}\}$(注:此处的算法表述和原文稍有不同,但不影响对算法的分析结果)。然后,根据 $m + n$ 值的奇偶性分别进行处理:当值为奇数时,用 $C(m,n)$ 的二进制序列按位异或序列 sp,并交换高位和低位序列的位置;当值为偶数时,先交换高位和低位序列的位置,再与序列 sp 异或。以上的步骤对每个像素重复进行,最终完成对整个图像的加密。

2　安全分析

2.1　安全漏洞的根源

在原算法中,混沌密钥序列的产生仅依赖于算法的密钥(包括 Logistic 映射的初值 x_0 和参数 μ 以及决定舍弃序列项数的参数 t),而与明文没有任何关联。这样一来,只要这些密钥参数不发生改变,所获得的混沌密钥序列 $s = \{s_1, s_2, \cdots, s_{M+N+L}\}$ 也将不会发生变化。攻击者只要能以某种方式获得这个混沌密钥序列,就可以解密任何用这个密钥序列加密的密文,而不必去花费精力试图了解算法最初始密钥(x_0, μ, t)的细节,因此,可以称这个混沌密钥序列 $s = \{s_1, s_2, \cdots, s_{M+N+L}\}$ 为该算法的等效密钥。

收稿日期:2009 - 12 - 22;**修回日期**:2010 - 02 - 11。
基金项目:国家自然科学基金资助项目(60703035);教育部新世纪优秀人才支持计划资助项目(NCET-08-0603)。
作者简介:肖迪(1975 -),男,重庆人,副教授,博士生导师,博士,主要研究方向:混沌密码学、多媒体; 赵秋乐(1983 -),男,河北保定人,硕士研究生,主要研究方向:多媒体。

此外,在进行逐像素加密时,需要根据像素点 $C(m,n)$ 的位置来选取子序列 $sp = \{s_{m+n+1}, s_{m+n+2}, \cdots, s_{m+n+L}\}$,并决定异或与交换的处理顺序。在原算法里,像素点 $C(m,n)$ 的位置体现为像素点坐标值的和 $m+n$,由于图像中可能会有很多个像素点的坐标值的和相等,而且相邻像素点坐标值的和往往相近,造成根据 $m+n$ 所选取的子序列 $sp = \{s_{m+n+1}, s_{m+n+2}, \cdots, s_{m+n+L}\}$ 会发生局部甚至是全部的重用。如以下像素点 $C(0,10)$、$C(1,9)$、$C(2,8)$、$C(3,7)$、$C(4,6)$、$C(5,5)$、$C(6,4)$、$C(7,3)$、$C(8,2)$、$C(9,1)$ 和 $C(10,0)$,其像素点坐标值的和 $m+n$ 都是10。把像素点坐标值的和 $m+n$ 都是 a 的像素称为 a 族像素。显然,按照原算法,属于同一族的不同像素点,它们所选取的子序列 $sp = \{s_{m+n+1}, s_{m+n+2}, \cdots, s_{m+n+L}\}$ 将是相同的,而且异或与交换的处理顺序也是完全一样的。再比如两个相邻像素点 $C(0,10)$,$C(0,11)$,其坐标值的和分别为10和11,按照原算法,它们所选取的子序列将分别为 $sp_{10} = \{s_{11}, s_{12}, \cdots, s_{10+L}\}$ 和 $sp_{11} = \{s_{12}, s_{13}, \cdots, s_{11+L}\}$,显然,这两个子序列中有 $L-1$ 个元素被局部重用了。

以上这些安全漏洞的存在,造成了原算法对于已知明文/选择明文攻击的脆弱性。

2.2 已知明文攻击分析

已知明文攻击是指攻击者可以获得一些明文/密文对,通过这些明文/密文对,他可以分析出原算法的秘密参数[3-4]。对本算法而言,就是获得该算法的等效密钥——混沌密钥序列 $s = \{s_1, s_2, \cdots, s_{M+N+L}\}$。不失一般性,设待加密图像的大小 M、N 均为256,待加密图像中每个像素的位平面数 L 为8。

由于原算法中存在比较普遍的子序列局部或全部的重用现象,因此,实际上攻击者只需要获得一对尺寸为 256×256 的明文图/密文图中的65对明文像素/密文像素,即可完全恢复出该算法的等效密钥——混沌密钥序列 $s = \{s_1, s_2, \cdots, s_{520}\}$。上面已经提到,像素点坐标值的和 $m+n$ 都是 a 的像素称为 a 族像素。攻击者只需要获得2族、10族、18族、26族、…、506族和512族像素中的任意一个代表性的明文像素及其对应的密文像素,即可恢复出混沌密钥序列 $s = \{s_1, s_2, \cdots, s_{520}\}$(注:根据算法的描述,该混沌密钥序列的前2项 s_1, s_2 实际上不会用到,因此实际需要恢复的等效密钥序列是 $s = \{s_3, s_4, \cdots, s_{520}\}$,下同)。具体过程如下:当已知2族像素中的代表明文像素 $C(1,1)$ 及其对应的密文像素 $CC(1,1)$,根据原算法,像素 $C(1,1)$ 所选取的子序列 $sp_2 = \{s_3, s_4, \cdots, s_{10}\}$;由于2为偶数,因此,应该先交换像素 $C(1,1)$ 高位和低位序列的位置,再与序列 sp_2 异或,最终获得相对应的密文像素值 $CC(1,1)$。显然,当攻击者已知明文像素 $C(1,1)$ 及其对应的密文像素 $CC(1,1)$,他只需先交换像素 $C(1,1)$ 高位和低位序列的位置获得 $C'(1,1)$,然后利用逐位异或运算的性质即可恢复出混沌密钥子序列:$sp_2 = \text{bitxor}(C'(1,1), CC(1,1))$。同理,当已知10族像素中的代表明文像素 $C(5,5)$ 及其对应的密文像素 $CC(5,5)$,即可恢复出子序列 $sp_{10} = \{s_{11}, s_{12}, \cdots, s_{18}\}$;…;已知506族像素中的代表明文像素 $C(253,253)$ 及其对应的密文像素 $CC(253,253)$,即可恢复出子序列 $sp_{506} = \{s_{507}, s_{508}, \cdots, s_{514}\}$;已知512族像素中的代表明文像素 $C(256,256)$ 及其对应的密文像素 $CC(256,256)$,即可恢复出子序列 $sp_{512} = \{s_{513}, s_{514}, \cdots, s_{520}\}$。

2.3 选择明文攻击分析

选择明文攻击是指攻击者可以选择特定的明文,并获得其对应的密文,通过分析这些明文/密文对得出原算法的秘密参数[3-4]。对本算法而言,当待加密图像的大小 M、N 均为256,待加密图像中每个像素的位平面数 L 为8时,就是设法获得该算法的等效密钥:混沌密钥序列 $s = \{s_3, s_4, \cdots, s_{520}\}$。

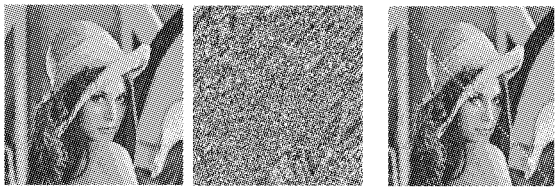
比上面的已知明文攻击更方便,攻击者只需选择一幅 256×256 的明文图像,并限定它的65个族像素中的代表像素值为0,即:$C(1,1)$、$C(5,5)$、$C(9,9)$、…、$C(256,256)$ 均为0,并获得其对应的65个密文像素值,即可很容易地获得对应的各个密钥子序列 $sp_2 = \{s_3, s_4, \cdots, s_{10}\}$、$sp_{10} = \{s_{11}, s_{12}, \cdots, s_{18}\}$、$sp_{18} = \{s_{19}, s_{20}, \cdots, s_{26}\}$、…、$sp_{506} = \{s_{507}, s_{508}, \cdots, s_{514}\}$、$sp_{512} = \{s_{513}, s_{514}, \cdots, s_{520}\}$。比如:当已知2族像素中的代表明文像素 $C(1,1)$ 及其对应的密文像素 $CC(1,1)$,根据原算法,$C(0,0)$ 的值为0,高位和低位序列的交换操作对其失效,故 $C'(1,1) = C(1,1) = 0$,且由于异或的性质,可以很快地恢复出对应的混沌密钥子序列:$sp_2 = \text{bitxor}(C'(1,1), CC(1,1)) = CC(1,1)$。同理,其他密钥子序列 $sp_{10}, sp_{18}, \cdots, sp_{506}, sp_{512}$ 也可很快地恢复出来。

3 仿真实验和改进建议

通过仿真实验演示如何成功地对原算法进行已知明文/选择明文攻击。算法密钥值取定为:Logistic 映射的初值 $x_0 = 0.232323$,参数 $\mu = 4$,舍弃序列前面的项数为 $t = 200$。根据原算法,迭代 Logistic 映射 $x_{k+1} = \mu x_k(1 - x_k)$ 生成一个混沌序列{0.7134,0.8178,0.5959,0.9632,0.1417,…,0.9722,0.1082,0.3860,0.9480,0.1972},二值化后得到一个二值混沌序列 s,舍弃序列 s 的前 $t = 200$ 项,获得真正参与加密的混沌密钥序列为 $s = \{s_3, s_4, \cdots, s_{520}\} = \{0,1,1,1,1,0,1,1,\cdots,1,0,1,1,0,1,1,0\}$。

3.1 已知明文攻击实例

设攻击者获得了如图1(a)、(b)所示的 256×256 的明文图及其对应的密文图。



(a) 已知明文 (b) 对应的密文 (c) 65个代表明文像素

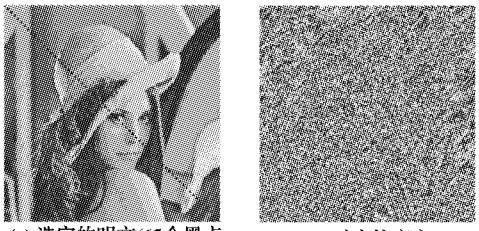
图1 已知明文攻击实例

上面已经提到,攻击者只需要获得2族、10族、18族、26族、…、506族、512族像素中的任意一个代表性的明文像素(如图1(c)所示中的白色点所代表的像素,共65个)及其对应的密文像素,即可恢复出混沌密钥序列 $s = \{s_3, s_4, \cdots, s_{520}\}$。具体过程如下:当已知2族像素中的代表明文像素 $C(1,1)$ 为 $162 = (10100010)_2$ 及其对应的密文像素 $CC(1,1)$ 为 $81 = (01010001)_2$,由于2为偶数,他只需先交换像素 $C(1,1)$ 高位和低位序列的位置获得 $C'(1,1) = (00101010)_2$,然后利用逐位异或运算的性质即可恢复出混沌密钥子序列:$sp_2 = \text{bitxor}(C'(1,1), CC(1,1)) = \{s_3, s_4, \cdots, s_{10}\} = 01111011$。同理,当已知10族像素中的代表明文像素 $C(5,5)$ 为 $163 = (10100011)_2$ 及其对应的密文像素 $CC(5,5)$ 为 $135 = (10000111)_2$,即可恢复出子序列 $sp_{10} = \{s_{11}, s_{12}, \cdots, s_{18}\} = 10111101$;…;已知506族像素中的代表明文像素 $C(253,253)$ 为 $57 = (00111001)_2$ 及其对应的密文像素 $CC(253,253)$ 为 $41 = (00101001)_2$,即可恢复出子序列 $sp_{506} = \{s_{507}, s_{508}, \cdots, s_{514}\} = 10111010$;已知512族像素中的代表明文像素

$C(256,256)$ 为 $105 = (01101001)_2$ 及其对应的密文像素 $CC(256,256)$ 为 $32 = (00100000)_2$，即可恢复出子序列 $sp_{512} = \{s_{513}, s_{514}, \cdots, s_{520}\} = 10110110$。将以上 56 个恢复出的子序列合并在一起，即可获得完整的等效混沌密钥序列 $s = \{s_3, s_4, \cdots, s_{520}\}$。

3.2 选择明文攻击实例

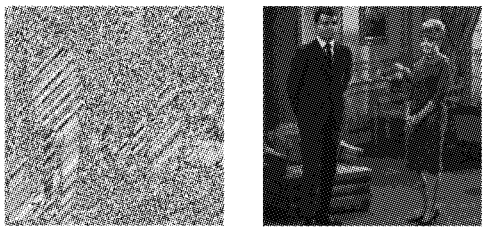
比上面的已知明文攻击更方便，攻击者只需选择一幅 256×256 的明文图像，并限定它的 65 个族像素中的代表像素值为 0(如图 2(a)所示中的黑色点所代表的像素，共 65 个)，即：$C(1,1)$、$C(5,5)$、$C(9,9)$、…、$C(256,256)$ 均为 0，并获得其对应的 65 个密文像素值 $CC(1,1) = 123 = (01111011)_2$，$CC(5,5) = 189 = (10111101)_2$，…，$CC(253,253) = 186 = (10111010)_2$，$CC(256,256) = 182 = (10110110)_2$，即可很快地恢复出对应的混沌密钥子序列：$sp_2 = \{s_3, s_4, \cdots, s_{10}\} = 01111011$，$sp_{10} = \{s_{11}, s_{12}, \cdots, s_{18}\} = 10111101$，…，$sp_{506} = \{s_{507}, s_{508}, \cdots, s_{514}\} = 10111010$，$sp_{512} = \{s_{513}, s_{514}, \cdots, s_{520}\} = 10110110$。将以上 56 个恢复出的子序列合并在一起，即可获得完整的混沌密钥序列 $s = \{s_3, s_4, \cdots, s_{520}\}$。



(a) 选定的明文(65个黑点代表明文像素值为0)　　(b) 对应的密文

图 2　选择明文攻击实例

当攻击者获得了完整的混沌密钥序列，他就可以解密任何用这个密钥序列加密的密文，而不必去花费精力试图了解算法最初始密钥(x_0, μ, t)的细节，如图 3 所示。



(a) 未知的密文图像　　(b) 恢复出的明文图像

图 3　利用密钥序列恢复出明文

3.3 改进建议

由上可见，攻击者得以实施等效密钥攻击的理论基础是原算法的第一个脆弱性根源，即混沌密钥序列的产生与明文没有任何关联。所以，算法改进的出发点应该是如何使得混沌密钥序列的产生过程与明文本身建立密切的联系。一种改进的思路是：先将明文图像中的各个像素值线性转化，然后调制到 Logistic 映射 $x_{k+1} = \mu x_k(1 - x_k)$ 的迭代过程中，通过改变每次迭代的参数值，生成一个与原明文图像密切相关的混沌序列，进而二值化后为混沌密钥序列 s。这样改进以后，不同的明文图像所对应的混沌密钥序列将会不同，攻击者也就无法再实施等效密钥攻击。

4 结语

本文运用已知明文/选择明文两种方法攻击了最近提出的一种基于 Logistic 混沌序列和位交换的图像置乱算法[10]，揭示了该算法隐藏的脆弱性。原算法可参照本文提出的改进建议加强安全性，排除应用过程中的安全隐患。

参考文献：

[1] 廖晓峰，肖迪，陈勇，等. 混沌密码学原理及其应用[M]. 北京：科学出版社，2009.

[2] FRIDRICH J. Symmetric ciphers based on two-dimensional chaotic maps[J]. International Journal of Bifurcation and Chaos, 1998, 8(6): 1259 - 1264.

[3] LIAN SHIGUO, SUN JINSHENG, WANG ZHIQUAN. Security analysis of a chaos-based image encryption algorithm[J]. Physics letters A, 2005, 351(2/3): 645 - 661.

[4] XIAO DI, LIAO XIAOFENG, WEI PENGCHENG. Analysis and improvement of a chaos-based image encryption algorithm[J]. Chaos, Solitons and Fractals, 2009, 40(5): 2191 - 2199.

[5] GAO HAOJIANG, ZHANG YISHENG, LIANG SHUYUN, *et al*. A new chaotic algorithm for image encryption[J]. Chaos, Solitons and Fractals, 2006, 29(2): 393 - 399.

[6] PAREEK N K, PATIDAR V, SUD K K. Image encryption using chaotic Logistic map[J]. Image Vision Computing, 2006, 24(9): 926 - 934.

[7] 张翌维，王育民，沈绪榜. 基于混沌映射的一种交替结构图像加密算法[J]. 中国科学: E 辑，2007, 37(2): 183 - 190.

[8] 袁益民，盛利元，尚芳. 基于 TD2ERCS 混沌系统的图像加密方法[J]. 计算机应用，2008, 28(4): 906 - 909.

[9] 高洁，袁家斌，徐涛，等. 一种基于混合反馈的混沌图像加密算法[J]. 计算机应用，2008, 28(2): 434 - 436.

[10] 袁玲，康宝生. 基于 Logistic 混沌序列和位交换的图像置乱算法[J]. 计算机应用，2009, 29(10): 2681 - 2683.

(上接第 1814 页)

在解密过程中，若初始值(密钥)发生极其细微的变化，解密后的图像则不能恢复到原图像，且与原图像差异巨大，依然是类似于噪声的均匀图像，完全不能获得原图像的几乎任何信息。

参考文献：

[1] 李昌刚，韩正之，张浩然. 图像加密技术综述[J]. 计算机研究与发展，2002, 39(10): 1317 - 1324.

[2] ZOU JIANCHENG, ZHONG WENQI, WARD R K. A novel digital image encryption method based on DES[C]// International Conference on Communication Systems and Applications. Anaheim, CA, USA: ACTA Press, 2005: 472.

[3] BEHNIA S, AKHSHANI A, MAHMODI H. A novel algorithm for image encryption based on mixture of chaotic maps[J]. Chaos, Solitons and Fractals, 2008, 35(2): 408 - 419.

[4] GAO TIEGANG, CHEN ZENGQIANG, DOMNGANG S. A new image encryption algorithm based on hyper-chaos[J]. Physics letters A, 2008, 372(4): 394 - 400.

[5] XU Q D, CHENG Z J, YOU H X. A new class of scrambling transformation and it application in the image information covering[J]. Science in China: Series E, 2000, 43(3): 304 - 312.

[6] PISARCHIK A N, ZANIN M. Image encryption with chaotically coupled chaotic maps[J]. Physica D, 2008, 237(20): 2638 - 2648.

[7] 陈帅，钟先信，石军峰，等. 基于离散数字混沌序列的图像加密[J]. 电子与信息学报，2007, 29(4): 898 - 903.

[8] 赵怀勋，王晓然，郑敏. 一种彩色图像的混沌解密算法[J]. 计算机应用与软件，2008, 25(10): 252 - 254.

[9] 张燕，黄贤武，刘家胜. 基于三维混沌的彩色图像加密新算法[J]. 计算机工程与应用，2008, 44(20): 202 - 205.

[10] 岳乐，彭波. 基于混沌加密的彩色图像自适应密写算法[J]. 计算机应用，2007, 27(10): 2470 - 2472.

[11] 邓志鸿，唐世渭. Ontology 研究综述[J]. 北京大学学报，2002, 38(5): 730 - 738.