Journal of Computer Applications
计算机应用,2014,34(9):2656 - 2658
ISSN 1001-9081
CODEN JYIIDU
2014-09-10
http://www.joca.cn

文章编号:1001-9081(2014)09-2656-03
doi:10.11772/j.issn.1001-9081.2014.09.2656

对“改进遍历矩阵和像素值扩散的图像加密算法”的密码分析

杨吉云[1],田维兴[1*],周发贵[2]
(1.重庆大学 计算机学院,重庆 400044; 2.78020 部队,昆明 650223)
(*通信作者电子邮箱 306234446@qq.com)

摘 要:最近提出了一个基于混沌的改进遍历矩阵和像素值扩散的图像加密算法,该加密算法首先将 Logistic 混沌映射构造一个遍历矩阵用于在图像空域迭代置换,然后再采用一个新的混沌序列对像素值进行扩散。通过对该加密算法的分析,找出了该算法存在的安全漏洞,从而提出了选择明文/已知明文的攻击方法,通过选择特殊的明文图像及其对应的密文图像,可在未知密钥的条件下对同样大小的密文图像进行破解。仿真实验结果表明这种攻击方法非常有效。

关键词:混沌;图像加密;密码分析;选择明文攻击;遍历矩阵
中图分类号:TP309.7 **文献标志码**:A

Cryptanalysis of Image encryption algorithm based on improved ergodic matrix and pixel value diffusion

YANG Jiyun[1], TIAN Weixing[1*], ZHOU Fagui[2]
(1. *College of Computer Science, Chongqing University, Chongqing 400044, China*;
2. *Army of 78020 Troops, Kunming Yunnan 650223, China*)

Abstract: Recently, an image encryption algorithm based on improved ergodic matrix and pixel value diffusion was proposed, where an ergodic matrix was constructed to be used in the iterative permutation of the spatial image by means of the Logistic chaotic mapping and then the pixel value diffusion was realized according to a new chaotic sequence. According to the analysis of this algorithm, the security hole could be found, so the chosen/known plaintext attack method was put forward to reveal the secret key, and recovered the ciphertext image of the same size by choosing some special plaintext images and the corresponding ciphertext images without the secret key. And the simulation results illustrate the effectiveness of the proposed attack method.

Key words: chaos; image encryption; cryptanalysis; chosen plaintext attack; ergodic matrix

0 引言

随着 Internet 技术的飞速发展,数字多媒体传输的安全越来越受到人们的关注。由于传统的加密方法都是针对文本信息来设计的,无法对像图像这样数据量大、相邻像素之间相关性大、数据冗余度高的信息进行加密。于是针对图像数据的特点,如何设计一个好的图像加密方案成为了研究焦点。

混沌系统产生的混沌信号具有随机性、对初值和参数的敏感性、遍历性等特性,而这些特性又满足 Shannon 理论关于混乱和扩散[1]的要求,因此在 1989 年 Mattews[2] 首次提出基于混沌的加密方法。而 1997 年 Fridrich[3] 在图像加密中运用了混沌映射后,引发了一股混沌图像密码的加密设计与安全分析的研究热潮,各种各样的混沌系统被引入到图像加密中,如文献[4-5]用到了帐篷映射(tent map),文献[6-8]用到了 Logistic 映射,文献[9]用到了陈氏系统(chen system),还有许多加密算法采用了超混沌系统[10]以及其他的各种混沌系统[11]。而对于目前提出的基于混沌的图像加密算法,绝大部分都是分为置换和扩散两个阶段进行加密。与此同时,混沌图像加密算法的安全性也受到了广泛的关注,研究者们发现其中一些算法并不能有效抵抗已知明文攻击或者选择明文攻击[12-15]。

本文分析了文献[8]提出的加密算法,该算法首先将 Logistic 混沌映射产生的随机序列生成用于像素位置置换的遍历矩阵,再将另外的混沌映射生成乱数序列用于像素值的扩散,并且引入了密文反馈机制。经过分析发现,该加密算法并不能抵抗选择明文攻击,通过选择 7 对特殊的明文像素矩阵和 $\log_{256}(m\times n)$ 对明密文图像即可还原出其余的用相同密钥加密的图像。

1 改进遍历矩阵和像素值扩散图像加密算法

不失一般性,假设待加密的图像是大小为 $m\times n$ 的灰色图像。根据文献[8]提出的加密算法,其加密过程分为像素位置置乱和像素值扩散两个部分,其具体描述如下。

1.1 像素位置置乱

该算法采用 Logistic 混沌映射产生一个遍历矩阵 $\boldsymbol{E}$。Logistic 映射如式(1)所示:

收稿日期:2014-04-11;**修回日期**:2014-06-19。

作者简介:杨吉云(1975 -),男,重庆万州人,副教授,主要研究方向:无线传感网络、信息安全、计算机检测与控制; 田维兴(1984 -),男,重庆涪陵人,硕士研究生,主要研究方向:密码算法分析、信息安全; 周发贵(1980 -),男,云南南华人,助理研究员,硕士研究生,主要研究方向:密码算法分析、信息安全。

$$a_{k+1} = \mu a_k(1 - a_k) \tag{1}$$

给定系统参数 μ 和初值 a_0,迭代式(1)多次,使之生成一个含 $m \times n$ 个不同数值的随机序列 P,然后对 P 序列按大小关系进行排序,以排序后的各个元素在原序列 P 中的位置序号作为序列 N 对应位置的元素,则 N 是由 $1,2,\cdots,m \times n$ 组成的一个序列,将 N 按照顺序生成 $m \times n$ 的遍历矩阵 $\boldsymbol{E}(i,j)$。然后根据遍历矩阵,对像素位置进行置换。

假设灰度图像的像素明文矩阵为 $\boldsymbol{M}(i,j)$,$\boldsymbol{R}(i,j)$ 为经一次置乱后的矩阵,计算过程如式(2)所示:

$$\boldsymbol{R}(i,j) = \boldsymbol{M}(\lceil \boldsymbol{E}(i,j)/n \rceil, \boldsymbol{E}(i,j) - (\lceil \boldsymbol{E}(i,j)/n \rceil - 1) \times n) \tag{2}$$

该算法共进行 D 次位置置乱,其中 D 作为密钥。最后将置乱后的矩阵 $\boldsymbol{R}(i,j)$ 按列转化为一维向量 $\boldsymbol{R}(k)$。

1.2　像素值扩散

给定参数 t 和初值 x_0,由式(3)生成随机序列 x_k:

$$x_{k+1} = \sin(t \times \arcsin(x_k)) \tag{3}$$

然后根据式(4)对 x_k 序列再次进行随机化得到序列 y_k,使之分布更加均匀。

$$y_k = (2/\pi)\arcsin(x_k) \tag{4}$$

由于像素值的取值是在 0 ~ 255,需要对 y_k 离散化操作,按式(5)离散化得到序列 z_k:

$$z_k = \lfloor (y_k + 1)/2 \times 256 + 0.5 \rfloor \tag{5}$$

最后根据式(6)用 z_k 对像素值进行混乱和扩散最终完成图像加密。

$$C(k) = z_k \oplus ((R(k) + z_k) \bmod 256) \oplus C(k-1) \tag{6}$$

其中:$C(0) = S$,作为初始密钥;$\lceil \rceil$ 和 $\lfloor \rfloor$ 分别表示向上和向下取整。该算法共有 6 个参数作为密钥:μ, a_0, D, t, x_0, S。

解密:先由式(7)解出向量 $\boldsymbol{R}(k)$,再将一维向量 $\boldsymbol{R}(k)$ 转化为矩阵 $\boldsymbol{R}(i,j)$,再由 $\boldsymbol{R}(i,j)$ 和遍历矩阵 $\boldsymbol{E}(i,j)$ 根据式(8)还原出明文图像矩阵 $\boldsymbol{M}(i,j)$。

$$\boldsymbol{R}(k) = ((z_k \oplus C(k) \oplus C(k-1) + 256 - z_k) \bmod 256 \tag{7}$$

$$\boldsymbol{M}(\lceil \boldsymbol{E}(i,j)/n \rceil, \boldsymbol{E}(i,j) - (\lceil \boldsymbol{E}(i,j)/n \rceil - 1) \times n) = \boldsymbol{R}(i,j) \tag{8}$$

2　密码分析

根据 Kerchoff 准则,在现代密码体制下,一个安全加密算法的安全性只依赖于密钥的保密性,而所有与算法结构相关的知识都应是公开的[16]。在密码学中,其攻击方式主要有已知明文攻击、选择明文攻击、唯密文攻击、选择密文攻击和差分攻击等五种。对于上述加密算法,只需还原出 $S, z_k, \boldsymbol{E}(i,j)$,即可破解加密的图像。在本文,主要用选择明文攻击和已知明文攻击。

2.1　像素值扩散阶段分析

在扩散阶段,虽然引进了密文反馈机制,但只是采用异或运算,且加密一个像素值时同一乱数使用了两次,则为攻击者提供了机会。选择一个全 0 组成的明文矩阵,则 $\boldsymbol{R}(k) = 0$,从而根据式(6),得到等式:$C(k) = C(k-1) = S$ 恒成立,还原出 S。

再分析 z_k,对任意的 $a, b \in \mathbf{Z}$,有等式:$\bmod((a \oplus 128) + b, 256) = \bmod(a + b, 256) \oplus 128$ 成立,其证明过程见文献[17],由此可知对于式(6),z_k 和 $z_k \oplus 128$ 加密结果相同。当两幅图像 $\boldsymbol{M}_1$ 和 $\boldsymbol{M}_2$ 采用相同密钥进行加密时,可以得到如下等式:

$$\begin{aligned} C_1(k) \oplus C_2(k) &= z_k \oplus ((\boldsymbol{R}_1(k) + z_k) \bmod 256) \oplus \\ &\quad C_1(k-1) \oplus z_k \oplus ((\boldsymbol{R}_2(k) + z_k) \bmod 256) \oplus \\ &\quad C_2(k-1) = ((\boldsymbol{R}_1(k) + z_k) \bmod 256) \oplus \\ &\quad C_1(k-1) \oplus ((\boldsymbol{R}_2(k) + z_k) \bmod 256) \oplus \\ &\quad C_2(k-1) \end{aligned} \tag{9}$$

当 $\boldsymbol{M}_1$ 和 $\boldsymbol{M}_2$ 分别选择为全 a 和 $b(a \neq b)$ 矩阵时,从式(9)可以得到:

$$C_a(k) \oplus C_b(k) \oplus C_a(k-1) \oplus C_b(k-1) = ((\boldsymbol{R}_a(k) + z_k) \bmod 256) \oplus ((\boldsymbol{R}_b(k) + z_k) \bmod 256) \tag{10}$$

上式左边部分和 $\boldsymbol{R}_a$、$\boldsymbol{R}_b$ 已知,则进一步简化为:

$$y = ((a + z_k) \bmod 256) \oplus ((b + z_k) \bmod 256)$$

其中 $a, b, z_k \in \{0,1,2,\cdots,255\}$。

文献[14]提出式(10)中的 $\{z_k, z_k \oplus 128\}$ 值可以用三组不同的 (a,b) 唯一确定,例如:(9,127),(1,52),(33,65),从而还原出 z_k;再由式(7),可还原出位置置换后的矩阵 $\boldsymbol{R}(i,j)$。

2.2　置换阶段分析

在置换阶段,位置变化只与初始值 μ、a_0 和 D 有关,而与明文图像无关。因此当密钥相同时,不同图像同一位置的元素在位置置换后仍保持一致。并且,位置置换一次和置换多次效果一样,只需还原与多次遍历矩阵 $\boldsymbol{E}(i,j)$ 等效的一次遍历矩阵 $\boldsymbol{E}'(i,j)$ 即可还原明文图像,即需要获取元素在 $\boldsymbol{M}$ 矩阵的位置和在 $\boldsymbol{R}$ 矩阵的位置对应关系,假设 $\boldsymbol{M}(i,j) = 1$,其他全为 0,找到它在置换后的矩阵 $\boldsymbol{R}$ 中等于 1 的元素的位置,假设为 $\boldsymbol{R}(i',j')$,即 $\boldsymbol{M}(i,j) = \boldsymbol{R}(i',j') = 1$,根据式(8),则有 $\boldsymbol{E}'(i',j') = (i-1) \times n + j$,即可通过它们的对应关系还原 $\boldsymbol{E}'(i,j)$。当已知 $\boldsymbol{R}(i,j)$ 后,则转化为只有位置置换的图像加密算法,而对于只有位置变换的矩阵,只需要 $\log_{256}(m \times n)$ 对已知/选择明密文对即可还原大部分的对应位置[18],进而还原出等效的一次遍历矩阵 $\boldsymbol{E}'(i,j)$。

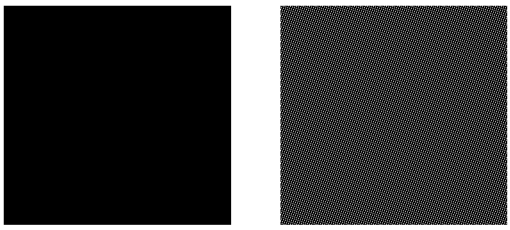
3　仿真实验

为了验证前面提出的密码攻击的可行性,选择大小为 256×256 的图像来做实验。假定密钥的取值情况为:$\mu = 3.859375$,$a_0 = 0.496093$,$D = 5$,$t = 31$,$x_0 = 0.152343$,$S = 41$。

首先对选择全 0 像素值的矩阵(图 1(a))加密,则加密后的矩阵(图 1(b))像素值都等于 S,即还原了 S。再选择 6 个特殊的明文矩阵(其值分别为 9、127、1、52、33、65)(图 2)和相对应的密文图像(图 3)还原出用于像素值混乱扩散的乱数序列 z_k,根据式(10),当选择了(9,127),(1,52),(33,65)这三组分别作为 a、b 配对时,可穷举每个 z_k 的值来还原序列 z_k,因此还原 z_k 序列的时间复杂度的上界为 $128 \times m \times n$。本文在 Matlab7.0,CPU 主频为 2.0 GHz 的 Intel 双核处理器,2 GB 内存的仿真实验环境下,还原长度为 256×256 的 z_k 的时间小于 10 s。在 z_k 和 S 已知的情况下,即可对加密系统的第二阶段扩散解密,得到置乱后的矩阵 $\boldsymbol{R}$。

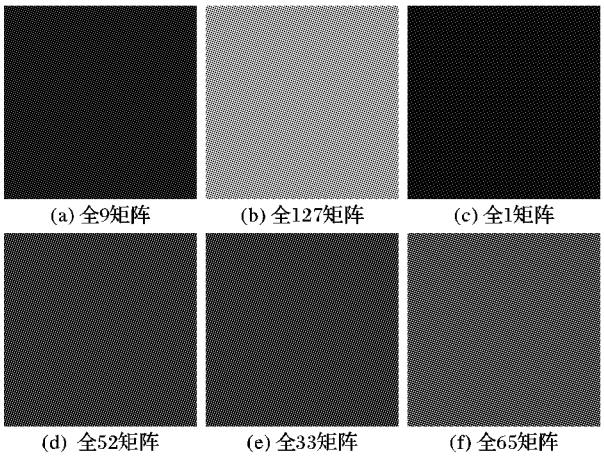
最后,相当于对仅有位置置换的矩阵破解,可以通过选择 $\log_{256}(256 \times 256)$ 对特殊的明文图像来破解获取等效的遍历矩阵。用前面还原的等效密钥对加密图像进行解密操作,其

解密结果如图 4。



(a) 选择的全0矩阵 (b) 全0矩阵加密后的矩阵

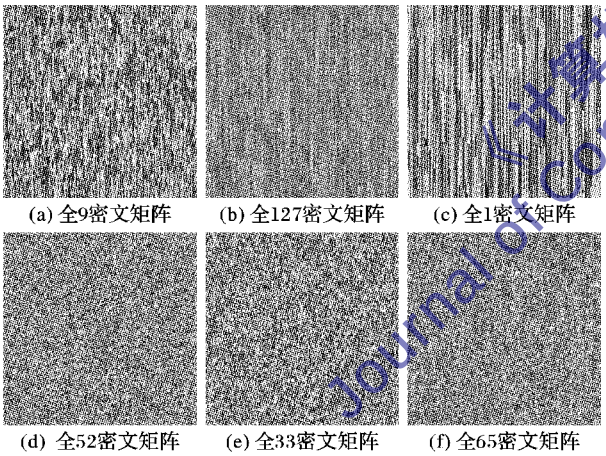
图 1 选择的全 0 矩阵还原 S



(a) 全9矩阵 (b) 全127矩阵 (c) 全1矩阵

(d) 全52矩阵 (e) 全33矩阵 (f) 全65矩阵

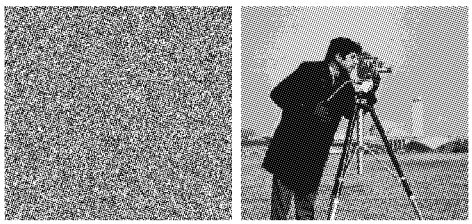
图 2 选择的 6 个特殊矩阵还原 z_k



(a) 全9密文矩阵 (b) 全127密文矩阵 (c) 全1密文矩阵

(d) 全52密文矩阵 (e) 全33密文矩阵 (f) 全65密文矩阵

图 3 图 2 中各个明文矩阵对应的加密矩阵图像



(a) 加密后的密文图像 (b) 还原的明文图像

图 4 用还原的等效密钥恢复的图像结果

4 结语

本文针对文献[8]中提出的基于混沌的改进遍历矩阵和像素值扩散的图像加密算法的安全性进行了分析，并提出了选择明文/已知明文攻击来还原等效密钥，首先选择一个全 0 的明文图像还原 S，再选择 6 对特殊明文矩阵图像还原 z_k，然后根据文献[18]提出的方法还原出遍历矩阵 $\boldsymbol{E}(i,j)$。整个攻击过程是在未知密钥的前提下进行的，同时给出了实验结果。在后续的研究中将对该加密算法进行改进。

参考文献：

[1] SHANNON C E. Communication theory of secrecy systems [J]. Bell System Technical Journal, 1949, 28(4): 656 – 715.

[2] MATTHEWS R. On the derivation of a "chaotic" encryption algorithm [J]. Cryptologia, 1984, 8(1): 29 – 41.

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

[4] ZHANG G, LIU Q. A novel image encryption method based on total shuffling scheme [J]. Optics Communications, 2011, 284(12): 2775 – 2780.

[5] KHANZADI H, ESHGHI M, BORUJENI S E. Image encryption using random bit sequence based on chaotic maps [J]. Arabian Journal for Science and Engineering, 2013, 39(2): 1039 – 1047.

[6] WANG X, TENG L, QIN X. A novel colour image encryption algorithm based on chaos [J]. Signal Processing, 2012, 92(4): 1101 – 1108.

[7] XIE T, HE X. A new color image encryption scheme based on chaos [J]. Application Research of Computers, 2013, 30(1): 318 – 320. (谢涛, 何兴. 一种新的基于混沌的彩色图像加密方案[J]. 计算机应用研究, 2013, 30(1): 318 – 320.)

[8] WANG J. Image encryption algorithm based on improved ergodic matrix and pixel value diffusion [J]. Journal of Computer Applications, 2012, 32(6): 1646 – 1649, 1653. (王继军. 基于改进遍历矩阵和像素值扩散的通用图像加密算法[J]. 计算机应用, 2012, 32(6): 1646 – 1649, 1653.)

[9] ZHANG L, HU X, LIU Y, *et al*. A chaotic image encryption scheme owning temp-value feedback [J]. Communications in Nonlinear Science and Numerical Simulation, 2014, 19(10): 3653 – 3659.

[10] WANG J, JIANG G. Cryptanalysis of a hyper-chaotic image encryption algorithm and its improved version [J]. Acta Physica Sinica, 2011, 60(6): 83 – 93. (王静, 蒋国平. 一种超混沌图像加密算法的安全性分析及其改进[J]. 物理学报, 2011, 60(6): 83 – 93).

[11] SUN F, LYU Z. Digital image encryption with chaotic map lattices [J]. Chinese Physics B, 2011, 20(4): 040506.

[12] LI C, ZHANG L, OU R, *et al*. Breaking a novel colour image encryption algorithm based on chaos [J]. Nonlinear Dynamics, 2012, 70(4): 2383 – 2388.

[13] LI C, ARROYO D, LO K-T. Breaking a chaotic cryptographic scheme based on composition maps [J]. International Journal of Bifurcation and Chaos, 2010, 20(8): 2561 – 2568.

[14] WANG X, HE G. Cryptanalysis on a novel image encryption method based on total shuffling scheme [J]. Optics Communications, 2011, 284(24): 5804 – 5807.

[15] ZHANG L, LI C, SHU S, *et al*. Cryptanalyzing a chaos-based image encryption algorithm using alternate structure [J]. Journal of Systems and Software, 2012, 85(9): 2077 – 2085.

[16] HUANG F, GUAN Z. Cryptosystem using chaotic keys [J]. Chaos, Solitons & Fractals, 2005, 23(3): 851 – 855.

[17] LI C, CHEN G. On the security of a class of image encryption schemes [C]// ISCAS 2008: Proceedings of the 2008 IEEE International Symposium on Circuits and Systems. Piscataway: IEEE, 2008: 3290 – 3293.

[18] LI S, LI C, CHEN G, *et al*. A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks [J]. Signal Processing: Image Communication, 2008, 23(3): 212 – 223.