

基于 Logistic 映射的可变置乱参数的图像加密算法

谢国波, 丁煜明

(广东工业大学 计算机学院, 广东 广州 510006)

摘 要: 近年来, 人们提出了很多基于混沌理论的数字图像加密算法, 但是其中有很大一部分采用传统的置乱-扩散体系, 当攻击者通过选择明文攻击时, 这种算法的安全性就大大降低. 针对这个问题, 提出了一种结合 Logistic 映射的变置乱参数的 Arnold 变换的图像加密算法, 增加了置乱-扩散两个操作之间的关联性. 仿真结果和数值分析表明, 该算法具有密钥空间大, 密钥敏感性强等特点, 能够有效地抵抗统计攻击.

关键词: 图像加密; 置乱-扩散; Logistic 映射; Arnold 变换

中图分类号: TP309.7

文献标识码: A

文章编号: 1000-7180(2015)04-0111-05

Image Encryption Algorithms With Variable Confusion Parameters Based on Logistic Mapping

XIE Guo-bo, DING Yu-ming

(School of Computer, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: Recently, a variety of encryption algorithms of digital image based on chaos theory have been studied, but a large part of them adopt the traditional confusion-diffusion architecture, the security of which is greatly reduced when attacked by selecting plain-image. In this paper, to address this problem, we propose a algorithm through changing the parameters of Arnold transform combined with Logistic mapping, which increases the correlation of the two operations. Simulation results and numerical analysis show that the algorithms has a large key space, be sensitive of secret keys, which can be effective to resist statistical attack.

Key words: image encryption; confusion-diffusion; logistic mapping; arnold transform

1 引言

数字图像作为信息的一种载体, 包含着大量丰富且比较直观的信息. 随着网络技术、多媒体技术以及数字通信技术等相关技术的发展, 数字图像信息的安全传递问题也越来越出, 也日益受到人们的关注. 然而, 由于数字图像具有数据量大, 相邻像素间的相关性强等特点, 传统的加密方法(如 AES、DES、RSA 等)因需要大量的计算时间和较高的计算性能, 并不适合对实时图像加密^[1].

随着混沌密码学的发展, 基于混沌系统的图像

加密得到了越来越广泛的应用, 成为了密码学的一个重要的研究方向. 从加密方式上来看, 基于混沌系统的图像加密研究方向主要分为以下几类: 基于图像像素置乱、基于图像像素灰度的替代以及基于前两者的结合^[2]. 而根据目前大多数的研究成果来看, 先进行图像位置置乱再进行灰度值替换或者算法似乎更受研究者的青睐^[3-7]. 在文献[3]中, 邓晓衡等首先采用 Kent 混沌映射产生的混沌序列实现对图像像素位置的全局置乱, 然后根据另一个新生成的混沌序列, 对图像的灰度值进行扩散, 有效地克服了传统的置乱-扩散结构算法不能有效地抵抗选择明文

收稿日期: 2014-06-23; 修回日期: 2014-08-18

基金项目: 广东省重大科技专项(2012A080103010); 广东省重点实验室建设专项(2011A091000046); 粤港关键领域重点突破项目(2012A080107007)

攻击的缺陷. 在文献[5]中, 朱从旭等先利用二维 Arnold 变换改变图像像素点的位置, 然后利用三维 Lu 混沌映射来改变图像的像素值, 有效地克服了一维混沌系统不能抵御相空间重构攻击的缺点, 提高了图像加密算法的安全性. 文献[6]中, 廉士国等将改进型的标准映射与 DES 加密算法结合起来, 同时对图像的位置进行替换和像素灰度值的替换, 安全性高且成本低廉, 在诸如图像、音频甚至视频等多媒体数据的加密应用方面具有较大的应用空间.

针对传统的置乱-扩散体系结构中使用 Arnold 变换对图像位置进行置乱, 然后再进行灰度值置乱的, 将置乱和扩散分为两个独立的操作的存在的问题, 本文通过将 Logistic 的迭代次数与图像的像素点的值结合起来, 并以此来改变 Arnold 变换的置换参数. 经过置换后交换两个像素点的值, 然后再进行灰度值替代, 并再次交换像素点的值, 用于下一轮的置乱-扩散, 提高了置乱和扩散两个操作的关联性, 也避免了 Arnold 变换的周期性问题, 从而达到增强算法的安全性的目的.

2 Arnold 映射和 Logistic 映射

2.1 Arnold 映射

Arnold 映射^[8-11], 俗称“猫映射”, 最早是由 Arnold 引入, 因经常用一张猫脸图像作为演示而得名. 二维猫映射的方程定义如式(1)所示.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1 \quad (1)$$

式中, (x_n, y_n) 表示原图像的像素点, 经过位置置乱后变换到像素点 (x_{n+1}, y_{n+1}) , $\bmod 1$ 表示只取整数部分, 因此 (x_n, y_n) 的相空间被限制在单位正方形 $[0, 1] \times [0, 1]$ 里面. 它的 Lyapunov 指数分别为 $\lambda_1 = 0.962\ 41$, $\lambda_2 = -0.962\ 33$, 因此猫映射是一个混沌映射.

为满足图像(此处只考虑等长图像)变换的要求, 可将式(1)进行推广, 推广后的猫映射方程的一般形式如式(2)所示.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & a * b + 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \quad (2)$$

式中, a, b 均为正整数, N 表示图像的大小.

2.2 Logistic 映射

Logistic 映射^[12-15]非常简单, 但却是被应用得

最为广泛的一个经典的混沌映射, 其定义式如式(3)所示.

$$x_{n+1} = \mu * x_n * (1 - x_n) \quad (3)$$

式中, $\mu \in (0, 4]$ 称为 Logistic 射的控制参数, $x_n \in (0, 1)$. Logistic 映射的动态行为与控制参数 μ 密切相关, 对于不同的 μ 值, 系统将呈现不同的特性. 研究表明, 当 $0 < \mu \leq 3.569\ 945\ 6$ 时, Logistic 呈现出周期性; 而当 $3.569\ 945\ 6 < \mu \leq 4$ 时, Logistic 映射处于混沌状态, 对初始值具有高度的敏感性, 初始值的微小变化都足以引起迭代序列的极大变化.

3 变置换参数的产生

传统的 Arnold 映射在置换图像位置时, 其参数一般是不变的, 经过一定次数的迭代后又得到原始的图像, 这是因为参数不变时 Arnold 映射具有周期性. 例如, 黄仿元在文献[16]中分析了 Arnold 置乱算法的周期性, 计算出了几种不同大小的图像的 Arnold 变换的周期, 如对于 $128 * 128$ 的图像, 其周期为 96. 而 Dyson 和 Falk 在文献[17]中给出了对于正整数 N , 当 $N > 2$ 时, 周期 $T \leq N^2/2$. 所以, 当攻击者破译扩散过程后, 对二维置乱的破解就变得相对容易了.

为了防止攻击者利用这一安全漏洞, 因此希望置换参数除了可以与 Logistic 映射相关外, 还可以与图像相关, 即不同的图像有不同的置换参数, 且每一次进行图像置乱时置换参数都是不同的. 考虑在 Matlab8.1 环境下仿真时, 由于矩阵、序列以及像素点等的下标都是从 1 开始, 进行 Arnold 变化后需要将变换后得到的像素点加 1, 所以对于 $N * N$ 的数字图像, 经过变换后, 像素点 (N, N) 总是会变换到像素点 $(1, 1)$. 因此, 可以利用此特性来建立置换参数与图像之间的关系, 具体关系如式(4)所示.

$$M = P(1, 1) + 100 \quad (4)$$

式中, $P(1, 1)$ 为原始图像在像素点 $(1, 1)$ 的灰度值, M 为用于产生置换参数时的迭代次数. 在置乱过程中, 由于像素点 (N, N) 总是会变换到像素点 $(1, 1)$, 这也使得图像的解密成为可能. 同时, 为了避免攻击者利用这一特性解密图像, 在每次置乱后将像素点 (N, N) 与指定的像素点 (x_1, y_1) 交换. 为此, 在加密算法中使用了两个 Logistic 映射, 如式(5)和式(6)所示, 分别用于产生 Arnold 变换的置换参数和扩散

过程中的密钥流.

$$x_1(n+1) = \mu_1 * x_1(n) * (1 - x_1(n)) \quad (5)$$

$$x_2(n+1) = \mu_2 * x_2(n) * (1 - x_2(n)) \quad (6)$$

将式(5)迭代 M 次,然后根据式(7)和式(8)产生 Arnold 变换的置乱参数.

$$a = \lfloor x_1(M) * 10^9 \rfloor \bmod N \quad (7)$$

$$b = \lfloor x_1(M) * 1015 \rfloor \bmod N \quad (8)$$

式中, N 表示图像的大小, $\lfloor \cdot \rfloor$ 表示向下取整.

4 图像的加密和解密

该加密算法的流程如图 1 所示.

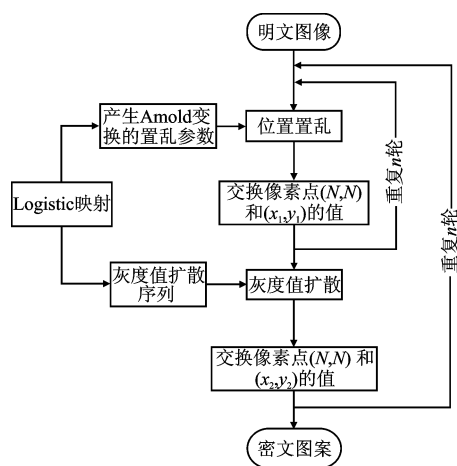


图1 加密算法流程图

具体加密步骤如下:

(1) 根据第3节中所介绍的方法得到 Arnold 映射的参数,并将图像置乱一次;

(2) 交换像素点 (N, N) 和 (x_1, y_1) 的值;

(3) 将步骤(1)和(2)重复 n 轮;

(4) 由于前面产生的迭代序列混沌特性可能不好,所以将式(7)迭代 $N * N + 100$ 次,从 Logistic 序列的第 101 项开始取用.当迭代奇数次时,按式(9)取整,否则按式(10)取整,得到序列 $f(k)$.

$$f(k) = \lfloor x_2(k+100) * 10^9 \rfloor \bmod 256 \quad (9)$$

$$f(k) = \lfloor x_2(k+100) * 10^{15} \rfloor \bmod 256 \quad (10)$$

然后将置乱后的图像的灰度值与产生的序列 $f(k)$ 进行异或运算,改变图像的灰度值.

(5) 交换像素点 (N, N) 和像素点 (x_2, y_2) 的值.根据安全性需要,可将步骤(1)到(4)重复 m 轮,当然了,这也会耗费更多的计算时间.

解密过程与加密过程类似,在得到加密图像文件和正确的密钥前提下,只需要执行加密操作的逆

操作就可以得到正确的解密图像,在解密过程中计算置乱参数时,Logistic 映射的迭代次数 M 应按式(11)计算.

$$M = P(x_1, y_1) + 100 \quad (11)$$

5 仿真和分析

5.1 实验结果

为了验证上述算法的合理性以及有效性,以如图 2(a)所示的像素为 $N * N (N=256)$ 的 lena 作为原始图像在 Matlab8.1 平台下进行仿真实验.初始条件选定如下:两个 Logistic 映射的控制参数均为 4, $x_1(1)=0.123\ 456\ 789$, $x_2(1)=0.987\ 654\ 321$,用于与像素点 (N, N) 交换的两个像素点分别选定为 $(x_1, y_1)=(100, 130)$, $(x_2, y_2)=(220, 80)$,置换循环次数 $n=5$,置换-扩散循环次数为 $m=4$.运行后得到的加密图像如图 2(b)所示.实验结果表明,使用该算法获得了很好的加密效果.

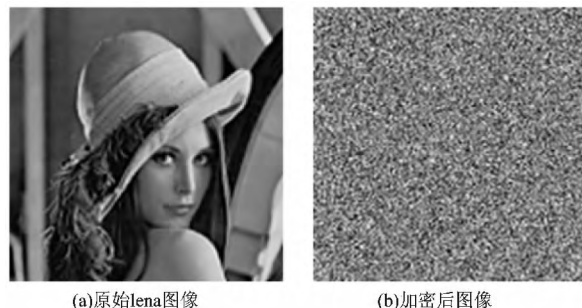


图2 原始图像和加密后图像

5.2 密钥空间分析

密钥空间的大小是体现一个加密算法安全性高低的一个重要方面.在本算法中,由于 Logistic 映射的初始值 $x_1(1)$ 、 $x_2(1)$ 的精度可以达到 10^{-15} ,而 x_1, y_1, x_2, y_2 的取值均介于 1 到 N 之间,且在置乱-扩散过程中有包括里外两层循环.所以,该算法具有足够大的密钥空间,在这么大的密钥空间面前,各种穷举攻击几乎是没有任何意义的,换句话说,也就是该加密算法的抗暴力破解性能强.

5.3 密钥敏感性分析

一个好的加密算法应对密钥具有高度的敏感性,密钥发生的一点微小变化都足以引起密文的极大变化.为了测试图像加密算法对初始密钥的敏感性,我们在仅仅对初始密钥作细微的改变,而保持其他条件均保持不变的情况下,来对图像的解密效果进行测

试. 如当其他条件均保持不变, 只是将 $x_1(1)$ 改为 0.123 456 789 1 后, 或者将 (x_1, y_1) 由 (100, 130) 改为 (101, 130) 均会导致解密的失败, 分别如图 3(a)、(b) 所示, 而图 3(c) 为正确解密图像. 从测试效果来看, 当密钥发生微小变化时, 对图像的解密几乎没有任何作用, 可见该算法对密钥具有高度的敏感性.

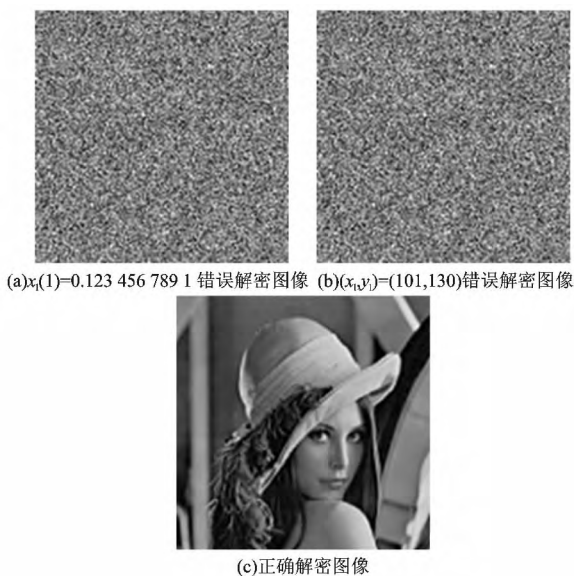


图 3 密钥敏感性分析图

5.4 统计分析

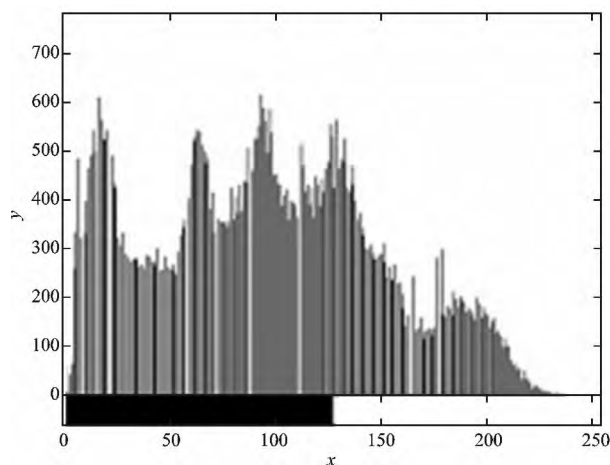
统计分析主要是从原始图像和加密后图像的灰度直方图以及相邻像素点的相关性两个方面对加密算法的效果进行测试分析, 以便更好地评估算法的安全性.

5.4.1 灰度直方图分析

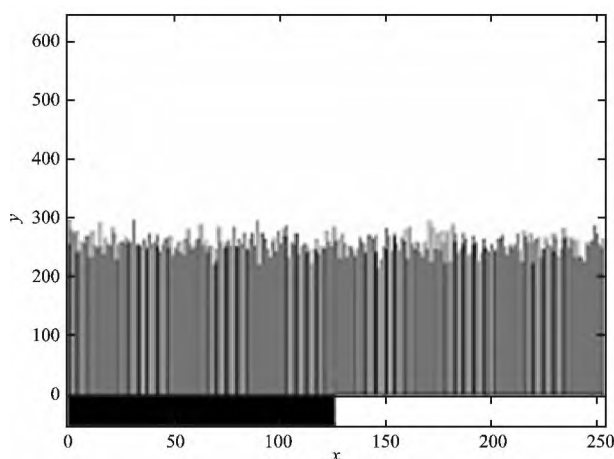
原始图像和加密后的图像的灰度直方图分别如图 4(a)、图 4(b) 所示. 从图中可以明显的看到, 加密后的图像的灰度直方图像素点的值的分布比较均匀, 较好地隐藏了图像的统计信息, 由此也会说明, 该加密算法能够有效地抵御基于图像像素值的统计攻击.

5.4.2 相关性分析

由于原始图像中包含了大量冗余信息, 相邻像素点之间的具有很大的相关性, 为了尽量避免攻击者使用基于相邻像素点之间的相关性的统计信息破解加密图像, 设计的加密算法也应当能够有效地降低相邻像素点之间的相关性. 我们分别从明文图像和密文像中随机选取 1 000 对相邻的像素点, 然后利用式(12)~(15)来计算明文图像和密文图像在水平、垂直以及对角线方向相邻的这 1 000 对像素点的相关系数.



(a) 原始图像灰度直方图



(b) 加密后图像灰度直方图

图 4 图像加密前后灰度直方图

$$\text{cov}(x, y) = E\{(x - E(x))(y - E(y))\} \quad (12)$$

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)} \sqrt{D(y)}} \quad (13)$$

$$E(x) = \left(\sum_{i=1}^N x_i \right) / N \quad (14)$$

$$D(x) = \left\{ \sum_{i=1}^N (x_i - E(x))^2 \right\} / N \quad (15)$$

式中, x 和 y 分别表示明文灰度级图像以及对应密文图像的相邻像素点的灰度值, $E(x)$ 和 $D(x)$ 分别表示 x 的期望和方差, N 表示随机选取的像素点的个数, 计算的结果如表 1 所示. 计算结果说明对于明文图像, 无论是在水平、垂直方向还是在对角线方向相邻的像素点, 它们之间的相关性都非常高, 而与该明文图像对应的密文图像, 其相关性都比较低, 说明密文图像的灰度值分布比较均匀, 较好地隐藏了图像的统计特征, 由此说明算法具有很好的抗统计攻

击性能.

表1 相邻像素点的相关系数

	明文图像	密文图像
水平相邻像素点	0.948 4	0.013 6
垂直相邻像素点	0.974 2	0.006 2
对角线相邻像素点	0.925 1	0.017 5

6 结束语

本文在 Arnold 变换的基础上,利用 Logistic 迭代序列对初始值具有高度敏感性的特点,通过将 Logistic 映射的迭代次数与图像的像素点灰度值结合起来,来产生进行 Arnold 变换的置乱参数,并且为了保证每次置乱-扩散过程中 Arnold 置乱参数的不同,每次置乱循环结束后都将用于获取迭代次数相关的点的灰度值与选取的图像的相关的像素点进行交换,从而有效地避免了 Arnold 的周期性问题.与此同时,再利用 Logistic 映射对置乱后的图像进行灰度值替换,从而实现了图像位置的置乱和灰度值的改变,最终完成了对图像的加密操作.该算法实现比较简单,增强了置乱-扩散两个操作的相关性,能有效地抵御选择明文攻击和各种统计攻击,具有密钥空间大,抗破解能力较强等特点,取得了较好的加密效果.

参考文献:

- [1] N K Pareek, Vinod Patidar, K K Sud. Image encryption using chaotic logistic map[J]. Image and Vision Computing, 2006, 24(1): 926-934.
- [2] 张红星, 张雪峰. 一种改进的基于广义猫映射的图像加密算法[J]. 西安邮电学院报, 2012, 17(5): 48-51.
- [3] 邓晓衡, 廖春龙, 朱从旭, 等. 像素位置与比特双重置乱的图像混沌加密算法[J]. 通信学报, 2014, 35(2): 216-223.
- [4] 李玲, 王伟男, 李津杰, 等. 基于 Logistic 映射和超混沌的自适应图像加密算法[J]. 微电子学与计算机, 2012, 29(1): 42-46.
- [5] 朱从旭, 李力, 陈志刚. 基于多维混沌系统组合的图像加密新算法[J]. 计算机工程, 2007, 33(22): 142-144.
- [6] Lian Shiguo, Sun Jinsheng, Wang Zhiqian. A block cipher based on a suitable use of the chaotic standard map [J]. Chaos, Solitons and Fractals, 2005, 26(1): 117-129.
- [7] Tu Li, Hu Juan, Zhang Chi. Image encryption algorithm based on arnold transformation and logistic mapping[J]. Advances in Information Sciences and Service Science, 2012, 23(4): 282-289.
- [8] 毛雷波. Arnold 变换及其逆变换研究[J]. 重庆工商大学学报: 自然科学版, 2012, 29(3): 16-21.
- [9] Pan Tiangong, Li Dayong. A novel image encryption using arnold cat [J]. International Journal of Security and Its Application, 2013, 7(5): 377-386.
- [10] 仲兴荣, 刘家胜, 黄贤武. 一种基于混沌猫映射的图像加密算法 [J]. 微电子学与计算机, 2007, 24(12): 131-133.
- [11] 鲍芳, 李军, 李旭. 基于高维广义猫映射的图像加密算法[J]. 西安理工大学学报, 2012, 28(2): 193-197.
- [12] 郑永爱. 混沌映射的随机性分析[J]. 计算机应用与软件, 2011, 28(12): 274-276.
- [13] 王化丰, 张桂香, 邵勇. 基于 Logistic 映射的混沌流密码设[J]. 计算机工程, 2007, 33(10): 164-168.
- [14] 余金峰, 杨文革, 路伟涛, 等. 满映射 Logistic 数字混沌序列的产生及性能分析[J]. 电讯技术, 2013, 53(2): 140-145.
- [15] 周蕊, 于晓明, 焦占亚. 一种基于混沌序列的数字图像加密算法 [J]. 微电子学与计算机, 2010, 27(12): 62-64.
- [16] 黄仿元. 基于 Arnold 变换的图像置乱算法及其实现 [J]. 贵州大学学报: 自然科学版, 2008, 25(2): 276-279.
- [17] Dyson F J, Falk H. Period of a discrete cat mapping [J]. The American Mathematical Monthly, 1992, 99(7): 603-614.

作者简介:

谢国波 男, (1977-), 博士, 副教授. 研究方向为嵌入式系统、混沌保密通讯. E-mail: guoboxie@163.com.

丁煜明 男, (1990-), 硕士. 研究方向为嵌入式系统、混沌保密通讯.