

基于混沌选择的自适应图像加密算法

王 阳^{1,2}, 吴成茂¹, 梁 睿¹

(1 西安邮电大学 电子工程学院, 陕西 西安 710121; 2 中国人民解放军 68304 部队, 陕西 渭南 715200)

摘 要: 提出一种高维混沌与多轮选择加密相结合的图像加密新算法. 首先对明文图像做 2×2 分块处理, 然后在主密钥流的控制下任意选择一种子块加密顺序. 顺序选定后, 用上一子块全部像素灰度值的异或运算结果作为四维混沌映射的初值, 产生密钥流复合加密下一子块, 直到四个子块全部加密完毕后再次选择新一轮子块加密顺序. 实验结果表明, 新的算法改进了原算法单方向加密的不足, 使得明文一个像素值的变化能影响到更多密文像素值, 在速度不变的情况下安全性有了提高.

关键词: 四维混沌; 自适应加密; 图像分块; 复合加密

中图分类号: TP309.7

文献标识码: A

文章编号: 1000-7180(2013)05-0132-05

Self-adaptive Image Encryption Algorithm Base on Chaos Choice

WANG Yang^{1,2}, WU Cheng-mao¹, LIANG Rui¹

(1 School of Electronic Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710121, China;
2 Unit 68304, PLA, Weinan 715200, China)

Abstract: A new image encryption algorithm combined with high-dimensional chaos and multi-wheel choice encryption was presented. Firstly, original images was divided into 2×2 size blocks, the encryption orders of blocks was chosen by main key stream. Secondly, the XOR operation result of all pixels' grey scale value in the last block was used as initial of four-dimensional chaos key stream to composite encrypting the next block. A single wheel operation would complete while all four blocks were encrypted, and a new wheel was chosen by main key stream. The experiment result indicated that the new algorithm enhanced the conventional algorithm and the macro change of original pixels would influence more cryptograph pixels while operation time unchanged.

Key words: four-dimensional chaos; self-adaptive encryption; image partition; composite encryption

1 引言

数字图像是一种信息含量丰富、空间有序性高的数据载体. 以往针对文本信息的加密技术如数据加密标准(DES)、高级加密标准(AES)存在密钥空间小、加密速度慢等不足, 难以实现对图像数据的高速、安全加密.

混沌具有对初值与系统参数的敏感性、白噪声的统计特性和序列遍历性等特点, 符合密码学要求的扩散、置乱和随机特性^[1]. 研究者利用混沌对数字图像的加密主要体现在三个方面: 一是利用混沌映

射产生伪随机序列改变明文像素的灰度值^[2]; 二是采用多维混沌映射置乱图像像素位置, 如 Arnold 映射^[3]、Tent 映射^[3]; 三是两种方法相结合使用. 已有的研究表明直接用低维混沌序列改变像素灰度值具有安全缺陷, 易被选择明文攻击破解^[4]. 文献[5]提出了一种基于分块自适应加密结构和像素灰度值的加密算法, 这里简称为 SIEC 算法.

针对 SIEC 算法使用低维混沌映射、明文像素位置没有改变、只有一种子块加密方向等问题, 本文在分块自适应加密结构的基础上, 利用高维混沌产生复杂密钥流选择多种加密顺序对图像进行多轮加

收稿日期: 2012-04-20; 修回日期: 2012-05-22

基金项目: 陕西省教育厅自然科学专项基金项目(2010JK816)

密运算,每轮加密中对下一子块的复合加密方式由上一子块的信息决定,在不明显降低加密速度的前提下提高算法的扩散性和安全性。

2 复合加密算法

2.1 加密规则

文献[6]提出的自适应加密算法是一种密钥流选择结构,其过程是:

Step1:输入密码并转换为二进制密钥流 key,长度为 128bit;

Step2:当 key[i]=0 时,选择左/右置乱加密算法;当 key[i]=1 时,选择上/下置乱加密算法;

Step3:当 i<128 时,i=i+1,转到 Step2;否则结束,输出密文图像。

该算法一次运算任意选择两种基于置乱的加密方式,使明文像素值的改变能影响更多密文像素值,提高了扩散的效果.如果在这种选择机制下融入基于灰度值改变的像素扩散加密方式,就能进一步提高该加密结构的复杂度和安全性,弥补排列加密易受选择明文攻击的缺陷。

2.2 像素排列加密

文献[6]提出的基于像素位置置乱的加密算法使用明文图像的一半像素信息排列另一半像素,共有四种加密方式:左对右排列加密方式、右对左排列加密方式、上对下排列加密方式及下对上排列加密方式。

自适应加密算法弥补了一般排列加密与密钥无关导致无法抵抗已知明文攻击的缺陷.但是自适应加密算法的排列只改变像素的位置,未改变像素灰度值,所以密文图像的直方图统计分布同明文图像一致,使用选择明文攻击就可以破解这种排列加密^[7].基于像素灰度值改变的像素扩散加密方式具有较高的加密速度,如果一轮加密运算用密钥流任意选择多种扩散加密方式和排列加密方式,就可以形成每轮唯一的复合加密方式。

2.3 像素扩散加密方式

基于像素灰度值改变的扩散加密方式的过程是本轮图像的一个像素与相邻像素做异或运算,运算结果作为新的像素值替换原像素值后完成加密.文献[8]提出了一种沿图像矩阵正对角线方向的像素扩散加密,定义为:

$$A_{x+1}(i,j) = A_x(i,j) \oplus A_{x+1}(i-1,j-1) \oplus A_{x+1}(i-1,j) \oplus A_{x+1}(i,j-1)$$

上式是从图像的左上角向右下角进行扩散加

密,还可以从右下角向左上角扩散加密:

$$A_{x+1}(i,j) = A_x(i,j) \oplus A_{x+1}(i+1,j+1) \oplus A_{x+1}(i+1,j) \oplus A_{x+1}(i,j+1)$$

此外,还可以沿反对角线方向对像素扩散加密,即从右上角到左下角扩散,定义为:

$$A_{x+1}(i,j) = A_x(i,j) \oplus A_{x+1}(i+1,j-1) \oplus A_{x+1}(i+1,j) \oplus A_{x+1}(i,j-1)$$

相应的,从左下角到右上角的像素扩散加密方式为:

$$A_{x+1}(i,j) = A_x(i,j) \oplus A_{x+1}(i-1,j+1) \oplus A_{x+1}(i-1,j) \oplus A_{x+1}(i,j+1)$$

除了沿对角线方向进行像素扩散加密外,还可以逐行、逐列对图像像素进行扩散加密。

2.4 改进的加密规则及复杂度分析

在保留自适应加密算法的 4 种排列加密方式同时引入 8 种像素扩散加密方式,共计 12 种加密方式.设密钥流 k_n 长度为 L,含有值为 1 到 12 的密值,每个密值与加密方式一一映射:

$k_n[i]=0 \rightarrow$ 左上角向右下角扩散加密;

$k_n[i]=1 \rightarrow$ 右下角向左上角扩散加密;

.....

$k_n[i]=10 \rightarrow$ 上对下排列加密;

$k_n[i]=11 \rightarrow$ 下对上排列加密。

对单个子块要进行 L 次加密,每次加密从 12 种加密方式中随机选择一种,除去全为排列加密或全为扩散加密的情况,一共有 12^{L-1} 种加密方式的组合,从而形成了对每个子块唯一的复合加密算法.攻击者单纯获取密钥流内容无法破解该算法,在获取加密规则的情况下,还可以通过加密规则动态化来提高安全性,动态变化范围是 12!,能有效抵抗穷举攻击。

3 混沌密钥流的产生

3.1 四维混沌映射

通过混沌系统可以获得伪随机、离散、遍历的实数序列,利用混沌初值敏感性的特点,每轮加密中只要改变混沌系统初值,就可以获得唯一的混沌序列,进一步转换为密钥流。

文献[9]提出的四维混沌系统:

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) + x_2 x_3 x_4 \\ \dot{x}_2 = b(x_1 + x_2) - x_1 x_3 x_4 \\ \dot{x}_3 = -cx_3 + x_1 x_2 x_4 \\ \dot{x}_4 = -dx_4 + x_1 x_2 x_3 \end{cases}$$

其中 $X = [x_1, x_2, x_3, x_4]^T$ 是状态变量, $a = 35, b = 10, c = 1, d = 10$, 为正值参数. 运用 Runge-Kutta 方法求解混沌系统方程, 选定 x_1 为密钥流产生初值, 其余不变, 步长 $h = 0.005$, 每次迭代运算获得 4 组离散实数混沌序列 X_1, X_2, X_3, X_4 .

为了增加混沌序列的非线性, 还要做非线性整数化处理. 非线性处理定义为:

$$e(t) = g(X_m, X_n) = k_1 X_m \times k_2 X_n$$

其中 k_1, k_2 取整数, 为非线性变换参数, X_m, X_n 为四维混沌映射的任意两个输出变量.

3.2 整数化处理

一般混沌映射产生的是 $[0, 1]$ 分布的实数序列, 为满足复合加密算法的规则需要, 对混沌序列 $e(t)$ 做整数化处理使其在 $[0, 11]$ 内遍历分布. 整数化处理的定义为:

$$k_n = (\text{round}(|e(t)|) \times m) \bmod m \quad (1)$$

设 m 为 12, 函数 $\text{round}(x)$ 表示对 x 取整.

4 混沌选择的自适应加密算法

4.1 单轮子块加密顺序

SIEC 算法按照顺时针的顺序加密四个子块, 即先对明文图像 I 分块, 再按照 I_1 (右上角) $\rightarrow I_2$ (右下角) $\rightarrow I_3$ (左下角) $\rightarrow I_0$ (左上角) 的顺序对子块像素做灰度值改变. 该算法只有一种加密顺序, 每个子块的像素的变化无法影响到上一个子块的像素, 因此要多轮加密, 同时子块加密的顺序也应该是多方向的.

若对明文图像做 2×2 分块处理, 则理论上共有 $4!$ 种加密顺序, 为了保证加密速度, 本算法选定其中四种作为单轮子块加密顺序, 如图 1 所示.

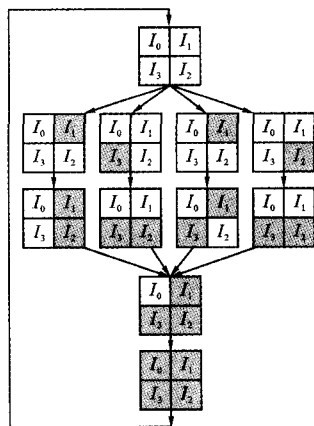


图 1 单轮子块加密顺序

顺时针加密顺序:

I_1 (右上角) $\rightarrow I_2$ (右下角) $\rightarrow I_3$ (左下角) $\rightarrow I_0$ (左上角);

逆时针加密顺序:

I_3 (左下角) $\rightarrow I_2$ (右下角) $\rightarrow I_1$ (右上角) $\rightarrow I_0$ (左上角);

Z 型加密顺序:

I_1 (右上角) $\rightarrow I_3$ (左下角) $\rightarrow I_2$ (右下角) $\rightarrow I_0$ (左上角);

X 型加密顺序:

I_2 (右下角) $\rightarrow I_3$ (左下角) $\rightarrow I_1$ (右上角) $\rightarrow I_0$ (左上角);

和复合加密一样, 子块加密顺序也可以被混沌密钥流选择. 设定单轮子块加密顺序同密钥流值 $\text{key}[i]$ 一一对应. 密钥流的产生过程同第 3 节一致, 只需将式(1)中的 m 设定为 4 即可产生 $[0, 3]$ 分布的混沌密钥流.

4.2 加密过程

本算法的加密过程同 SIEC 算法的加密过程基本一致, 改进之处在于:

(1) 加密顺序的选定: 分块操作之后, 输入密码产生长度为 l 的主密钥流 key , 选择四种加密顺序: 如果 $\text{key}[i] = 0$, 选择顺时针加密顺序, 如果 $\text{key}[i] = 1$, 选择逆时针加密顺序, 如果 $\text{key}[i] = 2$, 选择 Z 型加密顺序; 如果 $\text{key}[i] = 3$, 选择 X 型加密顺序. 在完成一个加密顺序后进入密钥流选定的下一个加密顺序, 弥补了原算法单一子块加密顺序扩散性不好的缺陷;

(2) 对子块的复合加密: 加密顺序选定后, 计算第一个子块所有像素灰度值的异或值, 经过变换作为四维混沌映射的初值, 产生长度为 L 的子密钥流 k_1 对下一子块做复合加密:

如果 $k_1[i] = 0$, 选择左上角向右下角扩散加密方式;

如果 $k_1[i] = 1$, 选择右下角向左上角扩散加密方式;

.....

如果 $k_1[i] = 10$, 选择上对下排列加密方式;

如果 $k_1[i] = 11$, 选择下对上排列加密方式.

如果 $i < L, i = i + 1$, 继续对下一个子块复合加密; 否则计算被加密子块所有像素灰度值的异或值产生密钥流, 按顺序对下一子块加密, 直到完成所有子块的加密.

4.3 解密过程

解密过程同 SIEC 算法的解密过程类似. 子块解密顺序、像素排列解密方式、像素扩散解密方式都是相应加密顺序、方式的逆运算, 只需严格按主密钥

流和子密钥流的逆方向解密即可得到原图像。

5 实验结果与安全性分析

实验计算机硬件配置为 Intel 1.6GHz 处理器, 512MB 内存, 软件为 Windows XP 操作系统、matlab 7.0 运行环境. 选用大小为 128×128 的灰度图像、二值图像、单色图像做明文图像, 通过直方图分析、相邻像素相关性分析、密钥空间/运行效率分析、抗差分攻击能力分析和信息熵分析验证了算法的安全性。

5.1 密钥空间分析与运行效率

算法中主密钥和子密钥流长度都为 128bit, 主密钥流包含 4 种信息, 子密钥流包含 12 种信息, 一轮加密的密钥空间为 $4^{128} \times 12^{128}$, 能有效抵抗现有的穷举攻击。

在相同环境下对 Lena. bmp 图像做加密时间测试, SIEC 算法的加密时间为 51.609s, 本算法的加密时间为 91.188s. 已知 SIEC 算法一次加密进行 2 轮运算, 每轮包括四次像素替代运算. 本算法一次加密共有 8 轮运算, 每轮进行 48 次像素替代/置乱加密. 因此, 本算法在适当增加运行时间开销的前提下, 改善原有自适应图像加密算法(SIEC 算法)的安全性, 能满足安全性要求较高场合下图像加密的需要。

5.2 相邻像素相关性分析

相邻像素相关性可以体现出图像像素的扩散情况, 如果明文图像中的两个像素相关性很大, 相应的在密文图像中相关性应该很小. 经过测试得到了灰度图像 Lena 加密前后在三个方向的相邻像素相关系数, 如表 1 所示. Lena 的加密前和加密后在水平、垂直和对角线三个方向的像素值分布如图 2 所示. 明文的统计信息已经充分扩散到密文中, 可以抵抗相关分析攻击。

5.3 抗差分攻击性能分析

攻击者采取对图像作微小修改来观察加密结果的变化, 这样可能发现加密算法的规律. 一般采用像素变化率 NPCR 作为度量指标, 测得本算法 $NPCR = 99.9652\%$, 同 SIEC 算法接近. 表明算法可以较好地抵抗差分攻击。

表 1 明文和密文的相邻像素相关性系数

	明文图像	密文图像
水平	0.9577	0.00530
垂直	0.9272	0.00518
对角线	0.9253	0.00517

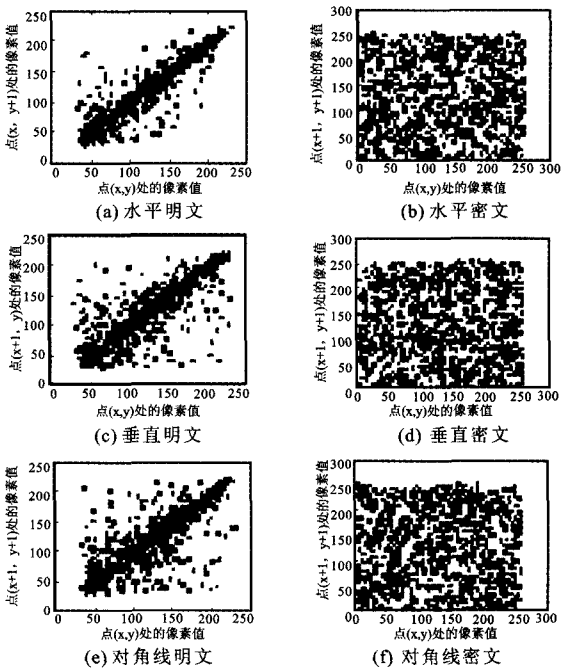


图 2 加密前后的像素分布

5.4 信息熵分析

信息熵反映了图像中的灰度分布情况, 信息熵越大包含的不确定信息就越多. 明文图像的信息熵为 7.4340, SIEC 算法的密文图像信息熵为 7.7626, 本算法的密文图像信息熵为 7.9810. 以看出使用本算加密的图像信息熵更高, 接近灰度级为 256 的图像的最大信息熵 8, 说明安全性更好。

6 结束语

本文通过引入具有多轮多方向的选择加密结构, 在密文的像素相关性指标中低于 SIEC 算法的实验结果, 改善了单一子块加密方向加密扩散性不高的问题. 在保留高效的自适应分块加密结构的基础上, 融入像素排列加密方式和像素扩散加密方式对子块复合加密, 改善了 SIEC 算法没有改变像素位置的缺陷, 使得算法能有效抵御已知明文攻击、选择明文攻击; 利用高维混沌序列的作为主密钥和子密钥流, 通过增加加密方式使得密钥空间成指数增加, 复杂度远高于原算法的单位混沌密钥流. 同时加密运算的时间远低于理论估计, 通过改进可在硬件电路中高效实现。

另外, 针对单值、二值图像被加密后密文直方图分布未能改变的算法缺陷做出了相应改进, 使其可以获得与灰度图像一样较好的密文直方图。

参考文献:

- [1] 胡春强, 邓绍江, 秦明甫, 等. 基于 Logistic 与标准映射的数字图像加密算法[J]. 计算机科学, 2010, 37(12): 57-59.
- [2] Pareek n k, Vinod Patidar, Sud k k. Image encryption using chaotic logistic map [J]. Image and Vision Computing, 2006, 24(9): 926-934.
- [3] 侯文滨, 吴成茂. 基于 Arnold 变换的图像分存加密方法[J]. 计算机应用, 2011, 31(10): 2682-2686.
- [4] 袁岁维, 范九伦, 朱敏涛. 基于三维帐篷映射的彩色图像加密[J]. 计算机应用研究, 2009, 26(12): 4780-4783.
- [5] 邓绍江, 黄桂超, 陈志建, 等. 基于混沌映射的自适应图像加密算法[J]. 计算机应用, 2011, 31(6): 1502-1511.
- [6] Chen gang, zhao xiaoyu, li junli. A self-adaptive algorithm on image encryption[J]. Journal of Software, 2005, 19(11): 1975-1974.
- [7] 李莉. 空域图像的自适应和并行加密算法的研究与分析[D]. 重庆: 重庆大学, 2011.
- [8] Taneja nidhi, Raman B, Gupta indra. Chaos based cryptosystem for still visual data [EB/OL]. [2012-04-20][2012-3-1]. <http://springer.lib.tsinghua.edu.cn>.
- [9] Qi guoyuan, Chen guanrong. Analysis and circuit implementation of a new 4D chaotic system[J]. Physics Letters A, 2006, 352(4-5): 386-397.

作者简介:

王 阳 男, (1986—), 硕士研究生. 研究方向为图像加密.
吴成茂 男, (1968—), 高级工程师. 研究方向为图像处理.
梁 睿 男, (1986—), 硕士研究生. 研究方向为图像处理.

(上接第 131 页)

- [6] 王中德. 沃尔什函数的构造、编序和生成[J]. 电子学报, 1988, 16(1): 122-123.
- [7] 李喜艳, 周清雷, 张文宁. 多峰值全局优化的混合编码遗传算法[J]. 微电子学与计算机, 2010, (03): 119-121.
- [8] Li Zhengsheng, Ma Wenyan. Weights and parity of Gray Code[C]//Conference Proceeding. Third International Conference on Electronic Measurement & Instruments, Beijing: CIA and Electronic Measurement and Instrument Society of CIE, 1997: 536-538.

作者简介:

李正生 男, (1957—), 博士生, 教授. 研究方向为自动化测试与控制、信号与信息处理, 电子系统故障诊断.
马文彦 女, (1956—), 硕士, 高级实验师. 研究方向为核技术与核安全.
闫 杰 男, (1960—), 博士, 教授, 博士生导师. 研究方向为飞行器控制、制导与仿真.