基于交叉分段和并行扩散的混沌图像加密算法

吴家新[1],蒋国平[2]
(1. 南京邮电大学 计算机学院,江苏 南京 210003;
2. 南京邮电大学 自动化学院,江苏 南京 210003)

摘 要:结合 Logistic 混沌系统,提出一种新的基于交叉分段和并行扩散的混沌图像加密算法(Cross Subsection and Parallel Diffusion,CSPD)。算法将明文交叉分成两段,降低明文段相邻像素点之间的相关性;每段密文之间形成两轮的并行扩散,提高算法对明文图像和密钥的敏感性;采用动态的密钥流生成规则,使得加密所需的密钥流与明文密切相关。实验结果和安全性分析表明:基于交叉分段和并行扩散的混沌图像加密算法具有密钥空间大,统计特性分布均匀,加密系统敏感性高和算法时间复杂度低等特点。

关键词:混沌;图像加密;交叉分段;并行扩散;Logistic
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2014)12-0133-05
doi:10.3969/j.issn.1673-629X.2014.12.031

Chaotic Image Encryption Algorithm Based on Cross Subsection and Parallel Diffusion

WU Jia-xin[1],JIANG Guo-ping[2]
(1. College of Computer,Nanjing University of Posts and Telecommunications,
Nanjing 210003,China;
2. College of Automation,Nanjing University of Posts and Telecommunications,
Nanjing 210003,China)

Abstract:Combined with the Logistic chaotic system,a novel algorithm is proposed based on cross subsection and parallel diffusion. The algorithm divides the plaintext into two segments to reduce the correlation between adjacent pixels of the plaintext. Each cipher text forms two rounds of parallel diffusion,which improves the sensitivity of algorithm for plaintext and key. Moreover,the algorithm adopts dynamic key generation rules,which makes the keystreams closely related to the plaintext. Experimental results and security analysis show that the chaotic image encryption algorithm based on cross subsection and parallel diffusion has a large key space,uniform distribution of the statistical characteristics,high sensitivity of the encryption system,and low time complexity etc.

Key words:chaos;image encryption;cross subsection;parallel diffusion;Logistic

0 引 言

数字图像是人们进行信息交互的重要手段,在人们的日常生活中扮演着重要角色。对图像数据进行加密是保证用户隐私安全的有效方式。传统密码学主要针对一般数据的加密和保护,对于图像数据不太适合,原因是图像具有数据量大、数据之间相关性高等特点。传统密码学算法加密具有这类特点的数据必然导致效率低下。混沌系统由于具有良好的伪随机性,对初值极度敏感,具有无限大的周期等特性,产生的混沌序列在适当处理后非常适合图像数据的加密。近年来,基于混沌系统的图像加密技术不断被研究和提出[1-5]。

利用混沌的伪随机特性,图像加密算法的设计主要分为像素位置的置乱、像素值的替代以及两者的结合等方法[6-9]。位置的置乱能够很大程度上破坏相邻像素的相关性,而像素值的替代使得最终的密文图像具有很强的随机特性,因此,两者相结合的图像加密算法能够很好地抵御统计和差分攻击,提高加密算法的

收稿日期:2014-01-03 **修回日期**:2014-04-10 **网络出版时间**:2014-09-11
基金项目:国家自然科学基金资助项目(61374180)
作者简介:吴家新(1990-),男,江苏淮安人,硕士研究生,研究方向为信息安全、混沌图像加密;蒋国平,教授,博士生导师,研究方向为复杂系统与网络控制、信息安全、混沌通信。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20140911.1010.050.html

安全性。文献[6-7]的图像加密算法对于不同的明文像素值都使用相同的密钥流序列,而获得密钥流就等同于获得了密钥,因此不能够抵御选择明文攻击和选择密文攻击。文献[8]针对文献[6]中提出的算法,给出了相应的攻击方法,并提出了改进的算法(简记为 IHIE 算法),使得每次加密都使用不同的密钥流序列,能够很好地抵御选择明文攻击和选择密文攻击。但是该算法对明文图像敏感性低,即单个像素点的变化只能影响该像素点之后的密文像素点。文献[9]针对文献[7]中提出的算法,同样给出了相应的攻击方法,并提出了改进的算法(简记为 ITSS 算法)。该算法在使用不同密钥流序列加密明文图像的同时,通过采取两轮的密文前后反馈加密,提高算法对明文图像的敏感性。但是该算法采用了流式加密的思想来进行两轮的密文加密:算法效率低下,耗时巨大。

文中为了获得高效安全的图像加密算法,提出一种新的基于交叉分段和并行扩散的混沌图像加密算法(Cross Subsection and Parallel Diffusion, CSPD)。首先,采用交叉分段策略,降低明文段的相邻像素点之间的相关性;其次,省略像素置乱步骤,减少位置置乱算法带来的系统时间开销;然后,每一轮的明文段之间独立扩散,实现图像的并行加密,进一步提高算法效率;最后,形成两轮密文段之间的交叉扩散,实现充分的混淆和扩散,使得加密所需的密钥流与明文密切相关,将一个明文字节的影响扩散到全部的密文字节中。

1 混沌系统分析

在文中选择 Logistic 混沌系统:

$$x_{n+1} = u \times x_n \times (1 - x_n) \tag{1}$$

式中,u 称为分岔参数。当 $x_n \in (0,1)$,且 $3.569\ 945 < u \leqslant 4$ 时,Logistic 映射产生的混沌序列处于混沌状态。为了获得良好的混沌特性,文中结合 Logistic 混沌特性,给出相应的修正和约束:

(1)当分岔参数 u 处于 3.569 945 和 4 之间时,Logistic 混沌系统亦存在周期性的窗口。这些窗口主要集中于[3.57,3.66]和[3.84,3.86]区间内,用户应尽量避免选择这些区间的分岔参数作为子密钥。

(2)良好的混沌系统对相关参数和初值具有极度的敏感性。由于 Logistic 混沌系统产生的混沌序列具有暂态过程,使得迭代的前 S 项序列对分岔参数 u 和初始值 x_0 敏感性差,文中结合计算机的精度给出 S 的临界值为 60。在使用 Logistic 混沌系统时,可以先让系统迭代 S 次之后,再使用生成的序列,这样可以避免混沌系统暂态过程的发生,使 Logistic 混沌系统具有更好的安全性。

(3)混沌序列分布特性均匀是混沌系统具有良好伪随机特性的必要条件。对于式(1),如果 $u=4$,则 Logistic 系统产生的序列 X 的概率密度为:

$$\rho(X) = \frac{\pi^{-1}}{\sqrt{x \times (1 - X)}} \tag{2}$$

从式(2)中可看出,序列 X 不是均匀分布。于是采用以下修正[10-11]:

$$Y = \frac{2 \times \arcsin\sqrt{X}}{\pi} \tag{3}$$

通过式(3)得到的随机变量 Y 服从均匀分布。

(4)服从均匀分布的随机变量 Y 是实数类型,取值均匀分布在区间[0,1]之内。对于 8 位的数字图像,像素取值是在[0,255]内的整型。文中需要两组中间密钥序列记为 $\{k_j(i): i = 1,2,\cdots,\frac{L}{2}; j = 1,2\}$,其中 $k_1(i)$ 用于第一段密文像素值的并行扩散,$k_2(i)$ 用于第二段密文像素值的并行扩散。由于计算机仿真精度可以精确到 10^{-15},故分别通过式(4)修正。

$$K = \mathrm{mod}[\mathrm{floor}(Y \times 10^{15}), 256] \tag{4}$$

结合上述四点对 Logistic 混沌系统的修正和约束,生成文中需要的两组中间混沌密钥序列 $\{k_j(i): i = 1,2,\cdots,\frac{L}{2}; j = 1,2\}$。经过修正和约束的两组中间混沌密钥序列具有更好的伪随机性。

2 图像加密算法

采用 Logistic 混沌系统,将分岔参数和初始值($u_1 = 3.999\ 99$, $x_{10} = 0.123\ 45$)、($u_2 = 3.999\ 87$, $x_{20} = 0.213\ 45$)作为密钥,生成两组中间混沌密钥序列 $\{k_j(i): i = 1,2,\cdots,\frac{L}{2}; j = 1,2\}$。文中通过两组中间混沌密钥序列实现对两段明文序列的加密。设明文图像表示的二维矩阵为 $\boldsymbol{P}_{M\times N} = \begin{pmatrix} p_1 & \cdots & p_N \\ \vdots & \vdots & \vdots \\ p_{(M-1)N+1} & \cdots & p_L \end{pmatrix}$,其中 $L = M \times N$。通过按行的顺序扫描二维矩阵 $\boldsymbol{P}_{M\times N}$,将其转换为明文序列 $\{P(i), i = 1,2,\cdots,L\}$。将明文序列 $\{P(i), i = 1,2,\cdots,L\}$ 交叉分成两段,分别表示为:

$$\begin{cases} \left\{P(i), i = 1, \frac{L}{2} + 1, 3, \frac{L}{2} + 3, \cdots, L - 1\right\} \\ \left\{P(i), i = 2, \frac{L}{2} + 2, 4, \frac{L}{2} + 4, \cdots, L\right\} \end{cases}$$

对于加密过程,第一轮加密输入为两段明文序列 $\begin{cases} \left\{P(i), i = 1, \frac{L}{2} + 1, 3, \frac{L}{2} + 3, \cdots, L - 1\right\} \\ \left\{P(i), i = 2, \frac{L}{2} + 2, 4, \frac{L}{2} + 4, \cdots, L\right\} \end{cases}$;输出记

为:$\begin{cases}\left\{I(i),i=1,\frac{L}{2}+1,3,\frac{L}{2}+3,\cdots,L-1\right\}\\ \left\{I(i),i=2,\frac{L}{2}+2,4,\frac{L}{2}+4,\cdots,L\right\}\end{cases}$,并作为第二轮加密的输入,输出的密文序:

$$\begin{cases}\left\{C(i),i=1,\frac{L}{2}+1,3,\frac{L}{2}+3,\cdots,L-1\right\}\\ \left\{C(i),i=2,\frac{L}{2}+2,4,\frac{L}{2}+4,\cdots,L\right\}\end{cases}。$$

第一轮:加密系统设置固定参数 I_1 和 I_2,并行加密两段明文步骤如下:

步骤(1):令 i=1。生成动态密钥流:

$\begin{cases}\text{key}_1(1)=I_1\oplus k_1(1)\\ \text{key}_2(1)=I_2\oplus k_2(1)\end{cases}$;同时加密两段明文的首个像素点:$\begin{cases}I(1)=P(1)\oplus\text{key}_1(1)\\ I(1+1)=P(1+1)\oplus\text{key}_2(1)\end{cases}$;生成动态密钥流:$\begin{cases}\text{key}_1(1+1)=I(1)\oplus k_1(1+1)\\ \text{key}_2(1+1)=I(1+1)\oplus k_2(1+1)\end{cases}$;同时加密两段明文的第二个像素点:

$$\begin{cases}I(\frac{L}{2}+1)=P(\frac{L}{2}+1)\oplus\text{key}_1(1+1)\\ I(\frac{L}{2}+2)=P(\frac{L}{2}+2)\oplus\text{key}_2(1+1)\end{cases}。$$

步骤(2):令 $i=i+2$。生成动态密钥流:

$\begin{cases}\text{key}_1(i)=I(\frac{L}{2}+i-2)\oplus k_1(i)\\ \text{key}_2(i)=I(\frac{L}{2}+i-1)\oplus k_2(i)\end{cases}$;同时加密两段明文的第 i 个像素点:$\begin{cases}I(i)=P(i)\oplus\text{key}_1(i)\\ I(i+1)=P(i+1)\oplus\text{key}_2(i)\end{cases}$;生成动态密钥流:

$\begin{cases}\text{key}_1(i+1)=I(i)\oplus k_1(i+1)\\ \text{key}_2(i+1)=I(i+1)\oplus k_2(i+1)\end{cases}$;同时加密两段明文的第 i+1 个像素点:

$$\begin{cases}I(\frac{L}{2}+1)=P(\frac{L}{2}+i)\oplus\text{key}_1(i+1)\\ I(\frac{L}{2}+i+1)=P(\frac{L}{2}+i+1)\oplus\text{key}_2(i+1)\end{cases}。$$

步骤(3):若 $i<L$,转步骤(2),否则进行第二轮的加密。

第二轮:加密系统设置动态参数 C_1 和 C_2。令参数 $C_1=I(L)$ 和 $C_2=I(L-1)$,使得第二轮加密形成的密文段之间能够相互扩散,保证单个像素点的变化能够影响到全部的密文像素点,然后继续独立加密两段中间密文,保证算法的并行性。具体步骤如下:

步骤(1):令 i=1。生成动态密钥流:

$\begin{cases}\text{key}_1(1)=C_1\oplus k_1(1)\\ \text{key}_2(1)=C_2\oplus k_2(1)\end{cases}$;同时加密两段中间密文的首个像素点:$\begin{cases}C(1)=I(1)\oplus\text{key}_1(1)\\ C(1+1)=I(1+1)\oplus\text{key}_2(1)\end{cases}$;生成动态密钥流:$\begin{cases}\text{key}_1(1+1)=C(1)\oplus k_1(1+1)\\ \text{key}_2(1+1)=C(1+1)\oplus k_2(1+1)\end{cases}$;同时加密两段中间密文的第二个像素点:

$$\begin{cases}C(\frac{L}{2}+1)=I(\frac{L}{2}+1)\oplus\text{key}_1(1+1)\\ C(\frac{L}{2}+2)=I(\frac{L}{2}+2)\oplus\text{key}_2(1+1)\end{cases}。$$

步骤(2):令 $i=i+2$。生成动态密钥流:

$\begin{cases}\text{key}_1(i)=C(\frac{L}{2}+i-2)\oplus k_1(i)\\ \text{key}_2(i)=C(\frac{L}{2}+i-1)\oplus k_2(i)\end{cases}$;同时加密两段中间密文的第 i 个像素点:$\begin{cases}C(i)=I(i)\oplus\text{key}_1(i)\\ C(i+1)=I(i+1)\oplus\text{key}_2(i)\end{cases}$;生成动态密钥流:

$\begin{cases}\text{key}_1(i+1)=C(i)\oplus k_1(i+1)\\ \text{key}_2(i+1)=C(i+1)\oplus k_2(i+1)\end{cases}$;同时加密两段中间密文的第 i+1 个像素点:

$$\begin{cases}C(\frac{L}{2}+i)=I(\frac{L}{2}+i)\oplus\text{key}_1(i+1)\\ C(\frac{L}{2}+i+1)=I(\frac{L}{2}+i+1)\oplus\text{key}_2(i+1)\end{cases}。$$

步骤(3):若 $i<L$,转步骤(2)。否则将输出的密文序列 $\begin{cases}\left\{C(i),i=1,\frac{L}{2}+1,3,\frac{L}{2}+3,\cdots,L-1\right\}\\ \left\{C(i),i=2,\frac{L}{2}+2,4,\frac{L}{2}+4,\cdots,L\right\}\end{cases}$ 转换为最终的密文序列,记为 $\{C(i),i=1,2,\cdots,L\}$。

通过上述两轮加密过程可以看出:基于交叉分段和并行扩散的混沌图像加密算法基本思想如图 1 所示。解密的过程为加密过程的逆。

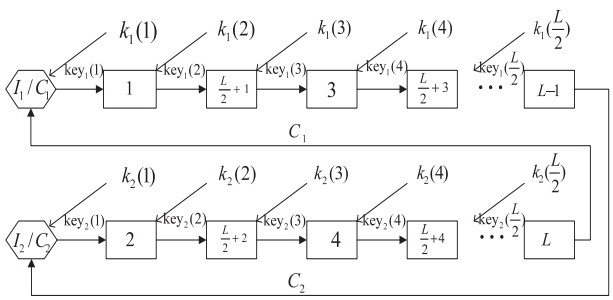


图 1　算法示意图

3　实验仿真与安全性分析

实验硬件环境为 Intel 2.8 GHz 的酷睿双核处理

器,4 G 内存;软件环境为 Matlab7. 12. 0(R2011a),运行于 32 位的 Windows7 系统上。使用 512 × 512 的 8 位 Lena 和 Baboon 灰度图像作为测试图像。子密钥设置为(u_1 = 3. 999 99,x_{10} = 0. 123 45)、(u_2 = 3. 999 87,x_{20} = 0. 213 45),相关参数设置为 S = 60,I_1 = 213,I_2 = 105。

3.1 密钥空间和加密效率

文中通过修正和约束的 Logistic 混沌迭代方程,采用两组分岔参数和初始值作为密钥。当计算机的精度为 10^{-15}时,除去约束的分岔参数小数点后两位,密钥空间可达 $10^{13}\times10^{15}\times10^{13}\times10^{15}=10^{56}\approx2^{185}$,相当于 185 bit 的密钥长度,完全满足文献[12]提出的密钥空间安全性要求。故算法完全可以抵御暴力攻击。

选择 512 × 512 的 8 位 Lena 图形衡量不同加密算法的效率。文中提出的 CSPD 算法平均耗时 2. 949 4 s,比文献[8]提出的 IHIE 算法的平均结果(4. 027 2 s)快了 1 s 多,比文献[9]提出的 ITSS 算法的平均结果(5. 851 4 s)快了 2. 9 s 多。相比于 IHIE 和 ITSS 算法,效率的提高主要在于省略了冗余的置乱环节,减少了系统性能的开销;由于 CSPD 算法并行化的实现,避免了两轮加密对算法效率的影响。

3.2 统计特性

3.2.1 信息熵

通过图像信息熵的分析,可以看出像素值的随机性。对于 8 位深度的灰度图形,信息熵计算公式如式(5)所示[13]:

$$H=\sum_{i=0}^{2^8-1}p_i\log_2\frac{1}{p_i} \tag{5}$$

其中,p_i表示像素值为 i 发生的概率。所以,对于理想的随机密文图像,理论信息熵为 8。在相同测试环境下,表 1 给出了 CSPD、IHIE 和 ITSS 算法得到的测试图像的密文信息熵。从表中可以看出,CSPD 算法优于 IHIE 算法,和 ITSS 算法结果相近,得到的密文具有很强的随机性。

表 1 Lena 和 Baboon 密文图像信息熵

Entropy value	Ciphered image	
	Lena	Baboon
CSPD	7. 994 2	7. 996 3
IHIE	7. 991 3	7. 990 5
ITSS	7. 995 8	7. 994 6

3.2.2 相关性

相邻像素具有高度的相关性是数字图像的本质特征。因此,一个安全的图像加密算法应该尽可能破坏掉图像之间的相关性。借用 Matlab 自带的 corrcoef( ) 函数测试明文和密文图像在水平和垂直方向的相关性。从表 2 中可以看出,尽管明文图像的水平和垂直相关系数趋于 1,但是经过加密,它们的相关系数从不同程度上趋于零。表 2 同样给出了 IHIE 和 ITSS 算法得到的密文图像的相关系数。对比发现,文中提出的 CSPD 算法在保证加密效率的同时,对相邻像素的相关性破坏程度相似于 IHIE 和 ITSS 算法。

表 2 水平和垂直方向的明文和不同算法得到的密文图像的相关系数

Coefficient	Lena		Baboon	
	Horizontal	Vertical	Horizontal	Vertical
Plain image	0. 982 6	0. 948 4	0. 816 3	0. 891 7
CSPD	-0. 002 7	0. 001 7	-0. 003 3	-0. 003 5
IHIE	-0. 003 6	0. 002 2	0. 003 5	-0. 003 0
ITSS	-0. 002 3	-0. 002 9	-0. 003 1	-0. 003 7

综合上述对图像的信息熵和相关性的分析,文中提出的 CSPD 算法能够有效抵御统计攻击。

3.3 敏感性分析

一个好的图像加密算法能够使得加密系统具有高度的敏感性。敏感性表现在两个方面:其一,明文中的每一位能够影响密文中的许多位,理想的情况是让明文中的每一位影响密文中的所有位,这样可以隐蔽明文的统计特性,抵御差分攻击;其二,密钥的轻微改变能够导致加密所得的密文图像和解密所得的解密图像截然不同。

3.3.1 明文图像的轻微改变

差分攻击是对图像加密算法常见的一种攻击方式,属于选择明文攻击。算法对明文的敏感性越强,抵抗差分攻击的能力也越强。可以用像素变化率(Number of Pixel Change Rate,NPCR)和归一化像素值平均变化强度(Unified Average Changing Intensity,UACI)去衡量算法对明文图像的敏感度。文献[14]首次给出了 NPCR 和 UACI 的定义:有 C_1 和 C_2 两幅密文图像,它们对应的明文图像有且仅有一个像素值不同。对于 C_1 和 C_2 中的任意像素值,若 $C_1(i,j)=C_2(i,j)$,则定义 $D(i,j)$ 为 0;若 $C_1(i,j)\neq C_2(i,j)$,则 $D(i,j)$ 为 1。计算 NPCR 和 UACI 如式(6)和式(7)所示:

$$\mathrm{NPCR}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)\times100\% \tag{6}$$

$$\mathrm{UACI}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C_1(i,j)-C_2(i,j)|}{255}\times100\% \tag{7}$$

对于 l 位的灰度级图像,可以通过式(8)和式(9)得到 NPCR 与 UACI 的理想期望值[15]:

$$u_{\mathrm{NPCR}}=\frac{2^l-1}{2^l} \tag{8}$$

$$u_{\mathrm{UACI}}=\frac{2^l+1}{3\cdot2^l} \tag{9}$$

当 l 为 8 时,u_{NPCR} = 99. 609 4%,u_{UACI} =

33.463 5%。表3 给出了 Lena 在 CSPD、IHIE 和 ITSS 算法下 NPCR 和 UACI 均值的对比。可见,文中的 CSPD 算法相比于 IHIE 算法,对明文更加敏感,敏感性程度和 ITSS 算法相近,对差分攻击的抵御效果更好。

表 3　Lena 在不同算法下 NPCR 和 UACI 的均值

	NPCR/%	UACI/%
Desired Expectation Value	99.609 4	33.463 5
CSPD	99.590 1	32.640 7
IHIE	96.790 1	28.541 2
ITSS	99.764 9	33.391 3

3.3.2　密钥的轻微改变

加密算法对密钥的敏感性至关重要。对于每一个子密钥,轻微的改变必须能够导致加密所得的密文图像和解密所得的解密图像截然不同。文中引入均方差(Mean Squared Error,MSE)衡量加密系统对密钥的敏感性。给出 MSE 定义:选择两组密钥 K_1 和 K_2,它们仅有一个子密钥不同,相差粒度为计算机所能识别的最小精度(文中仿真精度为 10^{-15})。分别考虑两种情况:其一,使用 K_1 和 K_2 加密同一幅明文图像产生密文图像 C_1 和 C_2;其二,使用 K_1 加密一幅明文图像 P 产生密文图像 C,使用 K_2 解密密文图像 C 产生解密图像 D。计算 MSE(C_1,C_2) 和 MSE(P,D) 分别如式(10)和式(11)所示:

$$\mathrm{MSE}(C_1,C_2)=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{(C_1(i,j)-C_2(i,j))^2}{255} \tag{10}$$

$$\mathrm{MSE}(P,D)=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{(P(i,j)-D(i,j))^2}{255} \tag{11}$$

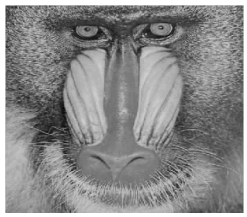
选取 Lena 图像,分别测试 8 个子密钥的敏感性。如表4 所示:△ = 10^{-15} 表示相应的子密钥相差 10^{-15},MSE(C_1,C_2) 和 MSE(P,D) 越大,说明对密钥的敏感性也越大。数据显示,文中的 CSPD 算法设计的子密钥合理,具有高度的密钥敏感性。图 2(a)和(b)分别给出了 Baboon 正确和错误解密图像。当使用轻微改变的密钥解密时,得到的解密图像完全杂乱无章,人眼不能分辨,可见密钥的轻微改变导致解密失败。

表 4　Lena 密钥敏感性测试

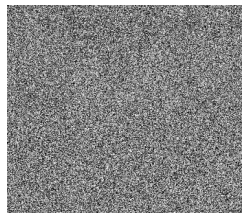
△ = 10^{-15}	Lena				
	Δu_1	Δx_1	Δu_2	Δx_2	Δu_3
MSE(C_1,C_2)	10 760.0	10 413.7	10 957.2	10 843.2	10 757.2
MSE(P,D)	7 675.3	7 281.6	7 274.5	7 236.5	7 052.4

3.4　典型攻击分析

根据 Kerckhoff 原则,假设攻击者知道加密系统和解密系统的算法。通常存在四种主要的攻击类型:



(a)所有子密钥完全相等



(b)子密钥Δu_1 相差 10^{-15}

图 2　Baboon 正确和错误的解密图像

(1)唯密文攻击:指攻击者仅仅能够获得一些被加密过的密文,而对明文一无所知;

(2)已知明文攻击:指攻击者已经获得了一些密文和对应的密文;

(3)选择明文攻击:指攻击者可以事先任意搜集一定数量的明文,让加密算法加密,这样透过未知的密钥获得加密后的密文;

(4)选择密文攻击:指攻击者可以事先任意搜集一定数量的密文,让解密算法解密,这样透过未知的密钥获得解密后的明文。

一般来说,选择明文和选择密文攻击是最具威胁的攻击,如果一个密码系统可以抵御这两种攻击,则可以抵御其他类型的攻击。文中算法采用交叉分段的思想,降低明文段的相邻像素点之间的相关性,形成两轮密文段之间的交叉扩散,实现充分的混淆和扩散,使得加密系统具有高度的敏感性,攻击者无法通过选择明文和选择密文攻击破解加密系统。因此,文中提出的基于交叉分段和并行扩散的图像加密算法对于四种主要类型的攻击完全免疫。

4　结束语

文中通过深入分析 Logistic 混沌系统的特性,并作出相应的修正和约束,使得 Logistic 混沌系统适合于图像的加密。通过将明文图像交叉分段,形成密文段之间的并行图像加密,提出的 CSPD 图像加密算法,实现充分的混淆和扩散,使得加密所需的密钥流与明文密切相关,将一个明文字节的影响扩散到全部的密文字节中。实验结果表明,基于交叉分段和并行扩散的混沌图像加密算法具有如下特点:选择的混沌系统形式简单,计算时间开销小;密钥空间大,可以达到 185 bit 的密钥长度;所得的密文图像统计特性分布均匀,像素与像素之间的相关性趋于 0;加密系统具有高度的敏感性;对常见的攻击形式免疫。因此,文中提出的基于交叉分段和并行扩散的方法具有良好的应用前景。

参考文献:

[1]　马在光,丘水生. 基于广义猫映射的一种图像加密系统

(下转第 141 页)

C 均值聚类算法对孤立点敏感,容易陷入局部最优的问题,从而提高入侵检测准确率。

3.3　收敛性分析

两种算法收敛性分析见图 3。从图中可以看出,传统模糊 C 均值聚类算法收敛速度过快,在 200 次左右算法收敛,而检测率并无明显增加,说明算法已陷入局部最优现象。新算法由于增加粒子群全局搜索和变异操作,经 300 次迭代收敛速度才渐渐变缓,趋于收敛,并且检测率明显优于 C 均值聚类算法。

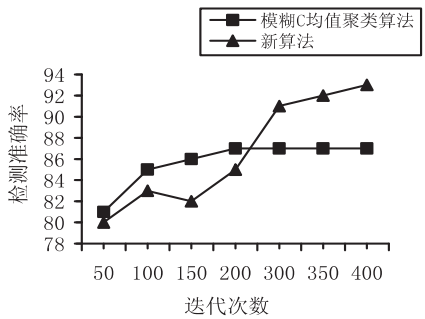


图 3　收敛性分析图

4　结束语

文中提出一种基于粒子群算法的模糊聚类算法,引入 PSO 全局搜索能力和变异操作避免传统 C 均值聚类算法中过早收敛的问题,提高入侵检测系统的检测率。

参考文献:

[1] 李昆仑,黄厚宽,田盛丰,等. 模糊多类支持向量机及其在入侵检测中的应用[J]. 计算机学报,2005,28(2):274-280.

[2] 唐少先,蔡文君. 基于无监督聚类混合遗传算法的入侵检测方法[J]. 计算机应用,2008,28(2):409-411.

[3] 洪飞龙,范俊波,贺　达. 数据挖掘在入侵检测系统中的应用研究[J]. 计算机应用,2004,24(12):82-83.

[4] 杨德刚. 基于模糊 C 均值聚类的网络入侵检测算法[J]. 计算机科学,2005,32(1):86-87.

[5] 王　勇. 模糊 C-均值算法在入侵检测系统中的应用研究[D]. 哈尔滨:哈尔滨理工大学,2007.

[6] 肖　建,白裔峰,于　龙. 模糊系统结构辨识综述[J]. 西南交通大学学报,2006,41(2):135-142.

[7] 肖立中,邵志清,马汉华,等. 网络入侵检测中的自动决定聚类数算法[J]. 软件学报,2008,19(8):2140-2148.

[8] 刘坤朋,罗　可. 改进的模糊 C 均值聚类算法[J]. 计算机工程与应用,2009,45(21):97-98.

[9] 张　敏,于　剑. 基于划分的模糊聚类算法[J]. 软件学报,2004,15(6):858-868.

[10] 刘文远,王颖洁,邓成玉,等. 基于遗传算法的模糊聚类分析[J]. 计算机工程,2004,30(19):117-118.

[11] 张曙红,孙建勋,诸克军. 基于遗传优化的采样模糊 C 均值聚类算法[J]. 系统工程理论与实践,2004,24(5):121-125.

[12] 刘向东,沙秋夫,刘勇奎,等. 基于粒子群优化算法的聚类分析[J]. 计算机工程,2006,32(6):201-202.

[13] Farnstrom F, Lewis J, Elkan C. Scalability for clustering algorithms revisited[C]//Proc of ACM SIGKDD. [s. l.]: [s. n.],2000.

[14] George K, Han Eui-Hong. Hierarchical clustering using dynamic modeling[J]. Computer,1999,32(8):68-75.

(上接第 137 页)

[J]. 通信学报,2003,24(2):51-57.

[2] Ye R. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism[J]. Optics Communications,2011,284(22):5290-5298.

[3] 龙卓珉,俞　斌. 针对超混沌系统图像加密算法的选择明文攻击[J]. 计算机工程,2012,38(17):148-151.

[4] 林　冰,蒋国平. 一种基于块置乱和反馈密钥的图像加密算法[J]. 计算机技术与发展,2012,22(5):123-126.

[5] 薛香莲. 一种新的基于超混沌映射的彩色图像加密算法[J]. 计算机应用与软件,2013,30(8):318-321.

[6] Gao Tiegang, Chen Zengqiang. A new image encryption algorithm based on hyper-chaos[J]. Physics Letters A,2008,372(4):394-400.

[7] Zhang G, Liu Q. A novel image encryption method based on total shuffling scheme[J]. Optics Communications,2011,284(12):2775-2780.

[8] 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.

[9] Zhu Congxu, Liao Chunlong, Deng Xiaoheng. Breaking and improving an image encryption scheme based on total shuffling scheme[J]. Nonlinear Dynamics,2013,71(1-2):25-34.

[10] 曹光辉,胡　凯,佟　维. 基于 Logistic 均匀分布图像置乱方法[J]. 物理学报,2011,60(11):125-132.

[11] 范九伦,张雪锋. 分段 Logistic 混沌映射及其性能分析[J]. 电子学报,2009,37(4):720-725.

[12] Alvarez G, Li Shujun. Some basic cryptographic requirements for chaos-based cryptosystems[J]. International Journal of Bifurcation and Chaos,2006,16(8):2129-2151.

[13] Amigo J M, Kocarev L, Szczepanski J. Theory and practice of chaotic cryptography[J]. Physics Letters A,2007,366(3):211-216.

[14] Chen Guanrong, Mao Yaobin, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons & Fractals,2004,21(3):749-761.

[15] Wu Y, Noonan J P, Agaian S. NPCR and UACI randomness tests for image encryption[J]. Journal of Selected Areas in Telecommunications,2011,2(4):31-38.

基于交叉分段和并行扩散的混沌图像加密算法

作者： 吴家新， 蒋国平， WU Jia-xin， JIANG Guo-ping
作者单位： 吴家新,WU Jia-xin(南京邮电大学 计算机学院,江苏 南京,210003)， 蒋国平,JIANG Guo-ping(南京邮电大学 自动化学院,江苏 南京,210003)

刊名： 计算机技术与发展 ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2014(12)