基于耦合混沌系统和细胞自动机的图像加密算法*

彭 川[1,2], 李元香[1]
(1. 武汉大学 软件工程国家重点实验室, 武汉 430072; 2. 中南民族大学 计算中心, 武汉 430074)

摘 要: 提出一种基于耦合混沌系统和细胞自动机的加密方法。耦合混沌系统比单一混沌系统具有更复杂的动力学特性,可以增大密钥空间,提高加密系统的安全性;利用耦合触发细胞自动机实现明文分块的并行加密,提高加/解密速度,改进置乱效果。加密时首先经过混沌加密,然后利用混沌序列产生反转规则,由细胞自动机再次加密;解密过程正好相反。实验表明,这种混合加密方法具有更大的密钥空间和更好的置乱效果,能够有效抵抗蛮力攻击和差分分析攻击。

关键词: 耦合混沌系统; 密钥空间; 耦合触发细胞自动机; 置乱效果
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2012)06-2218-03
doi:10.3969/j.issn.1001-3695.2012.06.057

Couple chaos system and cellular automata based image encryption algorithm

PENG Chuan[1,2], LI Yuan-xiang[1]
(1. *State Key Laboratory of Software Engineering, Wuhan University, Wuhan* 430072, *China*; 2. *Computing Center, South-Central University for Nationalities, Wuhan* 430074, *China*)

Abstract: This paper proposed a new kind of data encryption method based on couple chaos system and couple CTCA. Couple chaos system had more better encryption performance because of its much larger key space and chaotic characteristic. CTCA was used by way that plain data was divided into two parts and encrypted by two TCA systems respectively, which could improve the encryption efficiency and expand key space. After encrypted by chaos system, encrypted the original data by CTCA again. Experiments show that this method has a large key space and good scrambling effect and the cryptosystem can resist brute attack and differential attack effectively.

Key words: couple chaos system; key space; CTCA(toggle cellular automata); scrambling effect

0 引言

混沌系统具有类随机、对初始状态和参数的极其敏感等特性,具有良好的密码学特性,非常适合用于信息加密,其安全性依赖于密钥流的随机性[1]。自 1989 年 logistic 混沌映射作为密钥发生器用于信息加密以来,混沌系统用于信息加密已经得到广泛的研究。如何将混沌系统应用于保密通信和信息安全领域是当前信息安全领域的一个热点问题,其研究主要集中在如何使用混沌系统构造伪随机数发生器的相关算法及性能分析上[2~4]。对于混沌用于序列密码已经展开了大量的研究,特别是基于低维混沌系统的加密技术。但低维混沌系统维数低、动力学特性相对简单,因此其加密方法安全性不够高。

耦合混沌系统是将两个及以上的混沌系统进行耦合而形成的混沌系统。耦合混沌系统仍然具有混沌特性,而且可以拓展混沌系统的维数,表现出更为复杂的非线性动力学特性。将耦合混沌系统用于数据加密可以明显增大密钥空间,加强系统的安全性能。细胞自动机(CA)算法简单、并行度高,并且在某些局部规则作用下表现出全局混沌的特点,具有较高的加/解密速度,是一种数据加密的有效方法[5,6]。其具有广泛的应用前景。文献[7]提出了基于触发细胞自动机(TCA)的分组加密方发法。TCA 采用一种特殊的局部线性不可逆细胞自动机,具有简单、便于硬件实现等特点;缺点是采用串行加密导致加密效率低,如规则半径较小导致密钥空间小、每轮引入随机数导致数据膨胀等问题。文献[8]提出了一种基于 TCA 反向迭代的加密方法,解决了数据膨胀问题,但仍存在误差单向扩散和较大规则半径才能保证加密系统的安全性等不足。文献[9]研究了一种二维 CA 的反向迭代加密方法,对加密数据每列中的数据位实现了并行加密,一定程度上提高了加密速度,但也存在误差单向扩散和加密效率不高的问题。文献[10]提出了基于随机复合细胞自动机的密码系统,解决了单一细胞自动机存在的单向误差和规则半径问题,但加/解密速度较慢,需要较大的迭代轮数才能达到相对较好的效果,且其“雪崩效应”还不够理想,有待进一步提高。

针对上述问题,本文提出了一种基于混沌系统和细胞自动机反向迭代的混合数据加密算法并将其用于图像加密。算法通过构造耦合混沌系统和耦合触发细胞自动机对数据进行加密。引入耦合混沌系统的作用有两个:a)利用耦合混沌系统产生随机序列对数据加密;b)利用耦合混沌序列产生耦合 TCA 的转换规则,进而用耦合 TCA 对明文加密。利用耦合混沌系统实现加密增大了密钥空间,加强了置乱和扩散效果,增

收稿日期: 2011-10-31; **修回日期**: 2011-12-14 **基金项目**: 国家自然科学基金资助项目(61070009,60873114);中南民族大学中央高校科研业务专项资金资助项目(CZQ11006)

作者简介:彭川(1979-),男,讲师,博士研究生,CCF 会员,主要研究方向为演化算法、信息安全、演化硬件(chuan.peng@live.com);李元香(1962-),男,教授,博导,CCF 高级会员,主要研究方向为演化计算、并行计算.

强了加密系统的安全性;利用耦合 TCA 反向迭代加密则改进了传统 TCA 反向迭代加密方法中的串行加密方式,实现了分块并行加密,提高了加密效率,并避免了误差单向扩散、较小半径的安全性不高等问题。

1　耦合混沌系统

混沌现象是非线性动力系统中确定的类随机过程,这种过程是非周期的且又不收敛,但它是有界的,且对初始状态和系统参数具有极其敏感的依赖性。给定适当的系统参数时,系统将处于混沌状态。通常用 Lyapunov 指数标志系统的混沌状态:若 Lyapunov 指数为正时,系统处于混沌态。一维混沌系统可描述为

$$x_{n+1}=F(x_n)\quad x\in \mathrm{R} \tag{1}$$

其中:x_n、x_{n+1}表示映射状态变量,F 表示非线性映射函数。

Logistic 映射是一种典型的一维混沌动力系统,可用以下非线性方程来描述:

$$x_{n+1}=\mu x_n(1-x_n)\quad \mu\in[0,4],x_n\in[0,1] \tag{2}$$

当 3.569 945 6 $<\mu\leqslant$4 时,系统的动力学形态十分复杂,将进入混沌状态,即具有正的 Lyapunov 指数。通常在将混沌序列用于数据加密时,可对生成的混沌序列进行二值量化处理。本文量化处理所用的阈值函数为

$$f(x_i)=\begin{cases}1 & \text{if}\quad x_i\geqslant 0.5\\ 0 & \text{if}\quad x_i<0.5\end{cases}\quad i\in(1,2,\cdots,n) \tag{3}$$

其中:x_i 为生成的混沌序列中第 i 个元素值,$f(x_i)$为其量化值。

下面给出耦合混沌系统的相关定义。

定义 1　由两个一维混沌系统 $C_1:x_{n+1}=F(x_n)$、$C_2:y_{n+1}=F(y_n)$按照以下方式组合得到新的混沌系统 C_0,称为线性双耦合混沌系统,并称 C_1、C_2 为耦合系统 C_0 的子系统。

$$C_0:\begin{cases}x_{n+1}=F(x_n)+\alpha\times(y_n-x_n)\\ y_{n+1}=F(y_n)+\beta\times(x_n-y_n)\end{cases}\quad \alpha,\beta\in(0,1) \tag{4}$$

其中:x_n、y_n 分别表示两个混沌系统的状态变量;F 表示映射函数;α、β 表示耦合系数。由定义 1 可知两个 logistic 混沌映射的耦合模型为

$$\begin{cases}x_{n+1}=\mu_1 x_n(1-x_n)+\alpha\times(y_n-x_n)\\ y_{n+1}=\mu_2 y_n(1-y_n)+\beta\times(x_n-y_n)\end{cases}\quad \alpha,\beta\in(0,1);\mu_1,\mu_2\in[0,4] \tag{5}$$

下面讨论上述线性双耦合混沌系统的混沌特性。对于 logistic 混沌系统 C_1、C_2,分别取状态变量初值 0.5、0.6;取耦合系数 $\alpha=0.1$,$\beta=0.22$;不失一般性,任意固定某一 μ 值,另一 μ 值的取值范围为[2.5,4],按照式(5)构造双 logistic 耦合混沌系统。实验分别给出了单一系统和耦合系统的分叉图和 Lyapunov 特征指数图。图 1 为单一混沌系统的分叉图;图 2 为耦合混沌系统的分叉图;图 3、4 分别为其对应 Lyapunov 特征指数图。

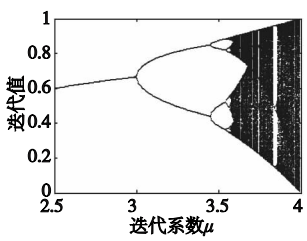

图1　单一混沌系统分叉图

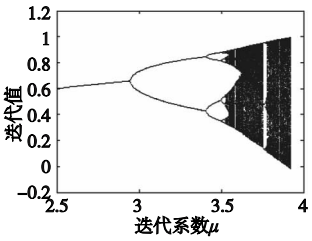

图2　耦合混沌系统分叉图

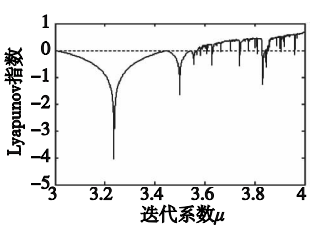

图3　单一混沌系统Lyapunov指数

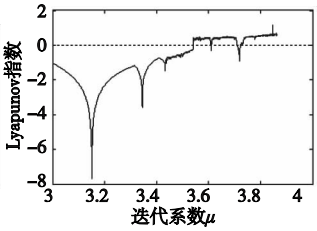

图4　耦合混沌系统Lyapunov指数

由图可知,耦合混沌系统仍然保持了单一混沌系统的混沌分叉特征,只不过耦合混沌系统参数的取值范围发生了变化。图 5、6 分别反映了耦合混沌系统对初始值和耦合系数的敏感性。经过若干次迭代,耦合系统对初值及耦合系数的微小改变会生成完全不同的混沌序列,说明耦合混沌系统对初始值和耦合系数具有很强的敏感性。实验表明,耦合系统仍然具有良好的混沌特性。

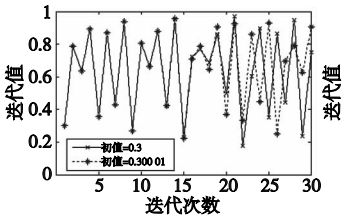

图5　对子系统初值的敏感性

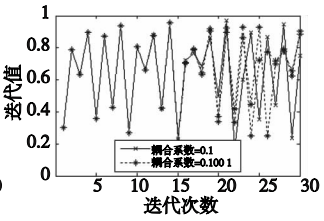

图6　对耦合系数的敏感性

基于以上分析,可以利用上述耦合混沌系统实现数据加密。耦合混沌系统具有比单一混沌系统更复杂的动力学特性,将其用于加密时可取两个混沌子系统的初值及耦合系数作为密钥,显然比利用单一混沌系统进行加密具有更大的密钥空间,因此极大地增强了加密系统的安全性。

2　耦合触发细胞自动机

定义 2　细胞自动机(CA)是一个四元组,表示为 CA = (d,s,N,f)。其中:d 表示空间维数;s 表示有限状态集;N 表示邻域向量,由 Z_d 上 m 个不同位置向量组成,可表示为 $N=(x_1,x_2,\cdots,x_m)$;f 表示局部转换函数即规则,是从 S_m 到 S 的映射。

对于一维细胞自动机,其邻域向量可表示为 $N=(\langle -r\rangle,\cdots,\langle -1\rangle,\langle 0\rangle,\langle 1\rangle,\cdots,\langle r\rangle)$,其迭代过程可表示为 $s_i^{t+1}=f(s_{i-r}^t,\cdots,s_i^t,\cdots,s_{i+r}^t)$,$i\in$Z。其中:$r$ 表示规则半径,s_i^t 表示第 i 个细胞在 t 时刻的状态。规则半径 $r=0$ 时,称做初等细胞自动机。

定义 3　对于细胞自动机 CA,若局部转换函数满足如下条件,则该细胞自动机称为触发细胞自动机(TCA):a)改变邻域内某一个细胞在某时刻的状态,保持其他细胞状态不变;b)局部转换规则的输出值反转。

TCA 的局部转换规则可表示为

$$1\oplus S_i^{t+1}=f(S_{i-r}^t,\cdots,1\oplus S_{i+j}^t,\cdots,S_{i+r}^t)\quad -r\leqslant j\leqslant r \tag{6}$$

其中:$S_i^t\in\{0,1\}$表示第 i 个细胞在 t 时刻的状态;r 为细胞自动机的规则半径;j 为触发细胞。式(6)表示了第 i 个细胞相对于第 $i+j$ 个细胞的反转规则,当 $j=-r$ 时,最左边的细胞成为触发细胞,此时称该细胞自动机为左触发细胞自动机;当 $j=r$ 时,称该细胞自动机为右触发细胞自动机。在初等细胞自动机中,规则 90、153 是相对于第 $i+1$ 位的右反转规则;规则 15、90 是相对于第 $i-1$ 位的左反转规则;规则 60、150 是相对于第 i 位的自反转规则。以规则 90 为例,其反转规则如表 1 所示,其

规则号可用二进制表示为(00111100)。

表 1 规则 90 的反转规则表

S_{i-1}^t	S_i^t	S_{i+1}^t	S_i^{t+1}	S_{i-1}^t	S_i^t	S_{i+1}^t	S_i^{t+1}
0	0	0	0	0	0	1	1
0	1	0	0	0	1	1	1
1	0	0	1	1	0	1	0
1	1	0	1	1	1	1	0

表中 S_{i+1}^t 的状态反转将会导致 S_i^{t+1} 的状态反转,即右触发。二维 TCA 是一维 TCA 在二维上的扩展,由于图像具有二维特征,因此二维细胞自动机非常适合用于图像加密。本文所用二维右触发细胞自动机的反转规则表示为

$$1\oplus c_{i,j}^{t+1}=f(c_{i-r,j-r}^t,\cdots,c_{i,j}^t,\cdots,1\oplus c_{i,j+r}^t,\cdots,c_{i+r,j+r}^t)$$

当半径 $r=1$ 时,中央细胞 $c_{i,j}^t$ 的下一时刻状态由其当前状态及 $c_{i-1,j}^t$、$c_{i,j-1}^t$、$c_{i+1,j}^t$、$c_{i,j+1}^t$ 即上下左右四个细胞的当前状态决定,且右细胞为触发细胞,即右细胞的状态反转会导致中央细胞的状态反转。

定义 4 对于触发细胞自动机 TCA1 和 TCA2,若其局部转换规则分别为

$$1\oplus S1_i^{t+1}=f(S1_{i-r}^t,\cdots,1\oplus S2_{i+j}^t,\cdots,S1_{i+r}^t);$$

$$1\oplus S2_i^{t+1}=f(S2_{i-r}^t,\cdots,1\oplus S1_{i+j}^t,\cdots\cdots,S2_{i+r}^t)\quad -r\leqslant j\leqslant r$$

此时称 CA1、CA2 构成了一个耦合 TCA 系统,其中 $S1_i^t$、$S2_i^t$ 分别表 CA1、CA2 的细胞 i 在 t 时刻的状态,CA1 和 CA2 互为耦合 TCA。

耦合 TCA 系统的主要特征表现为某个细胞自动机中细胞 i 的演化不仅与其自身状态有关,还与其耦合细胞自动机对应位置的邻域细胞状态有关。耦合细胞自动机比单一细胞自动机具有更为复杂的动力学特性。通过耦合 TCA 对明文实现分块并行加密,可以成倍提高加密速度。加密时取反转规则为密钥,可在不增加邻域半径情况下增大了密钥空间。由于其具有耦合性质,解密时必须对两部分的密文同时解密,否则将无法得到完整的解密信息,加强了系统的安全性。

3 基于耦合混沌系统和耦合 TCA 的图像加密算法

根据上述分析,可设计基于耦合混沌和耦合触发细胞自动机的加密算法。

对于给定明文数据 P。

a)给定两个 logistic 混沌系统初值 μ_1、x_1、μ_2、x_2;给定耦合系数 α、β,构造耦合混沌系统,并得到两个混沌序列 L_1、L_2;

b)将混沌序列 L_1、L_2 二值量化处理得到二进制混沌序列 LB_1、LB_2;

c)将明文块 P 分为对称的两部分 PL、PH,并分别用 LB_1、LB_2 与 PL、PH 进行异或运算得到 LPL、LPH;

d)利用混沌序列 LB_1、LB_2 产生反转规则 R_1、R_2,对于半径为 r 的 TCA,生成反转规则的步骤如下:

(a)分别将 LB_1、LB_2 分为 2^{2r} 个分组;

(b)设 $k=(L/2)/2^{2r}$,即每个分组有 k 个元素,分组中元素表示为 $n_1,n_2,\cdots,n_i,\cdots,1<i<k$;

(c)计算序列 $\{n_i\}$ 组成的二进制数对应的十进制数 d,求 $dd=d/2^k$,显然 $0<dd<1$,每个分块可得到 2^{2r} 个这样的数;

(d)量化上一步得到的数字序列,得到两个长度为 2^{2r} 的二值序列;

(e)根据上一步得到的二值序列,用文献[9]提到的方法产生 TCA 的规则 R_1、R_2。

e)根据规则 R_1、R_2 建立耦合 TCA 对分块进行反向迭代加密,LPL、LPH 分别对应规则 R_1、R_2 的 TCA;

f)合并上步得到密文分块,即为最终加密密文。

解密正好是加密过程的逆过程。

4 仿真实验和分析

4.1 加/解密效果实验

为验证本文算法性能,进行了仿真实验。实验设定混沌映射初值(即密钥)$u_1=3.7$,$u_2=3.8$,$x_1=0.3$,$x_2=0.5$;耦合系数 $\alpha=0.1$,$\beta=0.2$;规则 R_1、R_2(即子密钥)由耦合混沌序列生成。图 7(a)是大小为 128×128 的原始图像;(b)和(c)分别为加密图像和正确解密图;(d)为错误密钥得到的错误解密图。实验对于各个密钥的微小改变都只能得到错误的解密图像,限于篇幅,此处并未给出所有图示。实验表明,本文加密算法正确可行。

(a)原始图 (b)加密图 (c)正确解密图 (d)错误解密图

图7

4.2 密钥空间分析

单一 TCA 的密码系统以触发规则为密钥,对于邻域半径为 r 的触发细胞自动机,其密钥空间为 $2^{2^{2r+1}}$。本文基于耦合混沌系统和耦合 TCA 的加密算法中,由于两个加密部分采用不同的迭代规则,其对应密钥空间为 $2^{2^{2r+1}}\times 2^{2^{2r+1}}$;另外由于取混沌系统初始值和耦合系数一起构成密钥,整个加密系统的密钥空间将远大于 $2^{2^{2r+1}}\times 2^{2^{2r+1}}$。表 2 为本文算法和其他算法在不同半径情况下对应的密钥空间情况。由于采用了混沌和细胞自动机的混合加密方法,本文算法显然具有更大的密钥空间(混沌系统参数精确到 4 位小数)。这表明本文算法可以在较小的半径下获得很大的密钥空间,足以抵抗蛮力攻击。而且较小的半径更有利于降低硬件实现的复杂性。

表 2 几种算法的密钥空间比较

加密算法	$r=1$	$r=2$	$r=3$
单一 TCA 加密	32	1.31×10^5	3.69×10^{19}
耦合 TCA 加密	1 024	1.72×10^{10}	1.36×10^{39}
本文算法	10^{19}	1.72×10^{26}	1.36×10^{55}

4.3 数据敏感性分析

性能优良的加密系统应该具有理想的“雪崩效应”,即密钥或者明文的每一个位的变化都将引起密文每位以 50% 的概率发生变化。明文敏感性实验中,每次随机改变原图像某一位的值,然后计算迭代后加密图变化的位数。实验采取的方法是,共迭代 40 步,每一步迭代中都重复该过程 50 次,最后求每步迭代中明文变化引起的密文数据的平均变化率。图 8(a)~(c)分别反映了采用单一 TCA 加密、耦合 TCA 加密和本文加密算法明文改变一位时,密文数据的平均变化率情况。

实验结果表明,单一 TCA 在迭代 20 次后,数据变化率才达到理想的 50%;耦合 TCA 在迭代 15 次左右达到 50%;基于耦合混沌和耦合 TCA 的加密算法只需 10 次左右就可以达到理想值 50%。这说明本文的加密算法以较少的迭代次数就可以获得理想的加密效果,具有更高的效率。

(下转第 2239 页)

(上接第 2239 页)

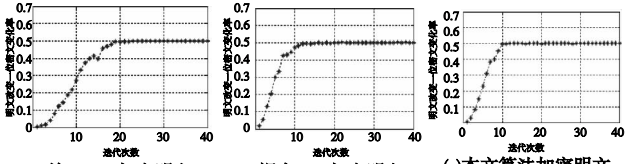

图8　明文改变一位密文变化率

在密钥敏感性实验中,随机改变密钥的一位,保持明文不变,对改变密钥值分别求第 n 步迭代加密后数据平均变化率。实验中取 $n=100$,即迭代 100 步。图 9 反映了密钥改变一位时密文数据的平均变化率情况。

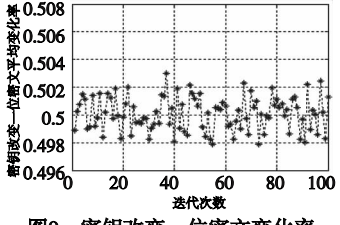

图9　密钥改变一位密文变化率

结果表明,各步迭代中密文平均变化率始终非常接近 50%,说明本文算法具有较好的密钥敏感特性。

以上实验结果表明,本文算法具有比较理想的明文、密钥敏感性,满足“雪崩效应”的要求,能有效抵抗差分分析攻击。

5　结束语

本文提出了一种基于耦合混沌系统和耦合 TCA 反向迭代的混合加密方法,解决了一些算法中存在的串行加密速度较慢、“雪崩效应”不理想、加密半径较小无法保证系统安全性等问题。其优点主要体现在:a)耦合混沌系统比单一混沌系统具有更好的加密特性,加强了系统的安全性;b)采用耦合 TCA 加密实现了并行加密方式,加快了加/解密速度,能满足图像加密等数据量较大的加密要求;c)以较小的邻域半径就可以获得较大的密钥空间,因此便于硬件实现。实验表明了本文算法具有良好的性能和可行性。

参考文献:

[1] 罗启彬,张健. 一种新的混沌伪随机序列生成方式[J]. 电子与信息学报,2006,28(7):1262-1265.

[2] 向菲,丘水生. 基于混沌系统互扰的流密码设计[J]. 物理学报,2008,57(10):6132-6137.

[3] 林金秋,司锡才,孟维晓,等. 基于混沌的一种图像加密算法[J]. 计算机应用研究,2010,27(2):697-698,703.

[4] 李孟婷,赵泽茂. 一种新的混沌伪随机序列生成方法[J]. 计算机应用研究,2011,28(1):341-344.

[5] SUNG J,HONG D,HONG S. Cryptanalysis of an involutional block cipher using cellular automata[J]. Information Processing Letters,2007,104(5):183-185.

[6] TAN S K,GUAN S U. Evolving cellular automata to generate nonlinear sequences with desirable properties[J]. Applied Soft Computing,2007,7(3):1131-1134.

[7] GUTOWITZ H,VICTOR J D,KNIGHT B W. Local structure theory for cellular automata[J]. Physica D,1987,28(1-2):18-48.

[8] 张传武,沈野樵,彭启琮. 细胞自动机反向迭代加密技术研究[J]. 计算机学报,2004,27(1): 125-129.

[9] 夏学文,熊曾刚,李元香. 二维可反向迭代细胞自动机在数据加密中的应用[J]. 计算机科学,2010,37(3):46-48.

[10] 平萍, 赵学龙,张宏,等. 复合元胞自动机系统反向迭代加密技术研究[J]. 物理学报,2008,57(10):6187-6195.