基于多耦合元胞自动机的加密算法*)

平 萍 周 曜 张 宏 刘凤玉

(南京理工大学计算机科学与技术学院 南京 210094)

摘 要 提出了耦合系数的概念,构造了一个新的耦合元胞自动机模型,并分析了耦合系数对耦合元胞自动机时空演化的影响。针对已有的单耦合元胞自动机加密系统中存在的不足,提出了基于多耦合元胞自动机的加密算法,该算法将多个元胞进行耦合,增强了两个元胞自动机之间的作用,扩大了相互影响的范围,使得误差扩散更为快速。仿真结果表明,该算法具有更为理想的扩散和扰乱特性,可抵抗蛮力攻击和差分分析攻击。

关键词 密码学,耦合系数,元胞自动机

Encryption Based on Multi-coupling Cellular Automata

PING Ping ZHOU Yao ZHANG Hong LIU Feng-yu

(School of Computer Science and Technology, Nanjing University of Science& Technology, Nanjing 210094, China)

Abstract By proposing a coupling parameter, this paper constructed a new model of coupling cellular automata and anlalyzed the time and space evolution of coulping cellular automata. As there were some disadvantages on the cipher based on simple coupling cellular automata, we presented a new encryption algotirhm based on multi-coupling cellular automata. The method of coupling many cells can enhance the interrelation between two cellular automaton, and make the error diffuse quickly. Simulation experiment shows that the diffusion and confusion properties of the algorithm are very ideal, it can resist bruce attack and differential cryptanalysis attack.

Keywords Cryptography, Coupling parameter, Cellular automata

1 引言

随着网络技术的迅速发展,在全世界范围内形成一个庞大的信息网,从而不可避免地存在信息安全问题,数据加密技术已成为网络中最基本的安全技术,复杂的密码算法已经难以适应高速实时信息传输的需要。元胞自动机是空间、时间、状态均离散化的动力系统,其固有的组成单元的简单性、单元之间作用的局部性和信息处理的高度并行性,并表现出复杂的全局特性等特点[1]使得元胞自动机在密码学领域有着独特的优势。

Wolfram 首次提出了基于元胞自动机的密码算法。在他的模型中将元胞自动机的初始状态作为密钥,利用规则 30 元胞自动机迭代产生的伪随机序列作为序列密码[2],从而开创了元胞自动机在密码学中的应用。此后,涌现了许多基于元胞自动机理论的随机数发生器、对称密码、非对称密码和 Hash 函数文献[3-6]。在对称密码方面,Gutowitz 提出了基于不可逆元胞自动机的分组加密算法[7],该算法采用了一种特别的局部线性不可逆元胞自动机,反向迭代实现加密,正向迭代实现解密,具有简单、方便硬件实现等优点,其不足主要体现在密钥空间小、误差扩散具有单向性,对明文的扰乱程度不够。因此文献[8]提出了一种耦合触发元胞自动机密码系统(CTCA),利用两个元胞自动机中单个元胞的耦合,在几乎不增加运算量及系统复杂度的同时,将密钥空间大大提高,从而提高密码系统强度,但由于只是邻域内中心位置元胞的简单耦合,明文的统计特性需要经过多次迭代才能较好地隐藏在密文中,且存在一些规则使得两个元胞自动机之间的作用是单向的。因此,本文提出了一种基于多耦合触发元胞自动机的加密模型,通过耦合两个元胞自动机的多个元胞,增强了两个元胞自动机之间的作用,扩大了相互影响的范围,不仅具有更复杂的动力学行为,而且具有更为理想的扩散和扰乱特性,使得明文和密文之间存在复杂而敏感的非线性关系。

2 耦合元胞自动机系统模型

2.1 耦合元胞自动机系统

定义 1 元胞自动机 CA 是一个四元组 $CA=(d,S,N,f)$,其中:

d:空间维数;

S:有限状态集;

N:邻域向量,是由 Z^d 中 m 个不同的位置向量组成,记为 $N=(\vec{x}_1,\vec{x}_2,\cdots,\vec{x}_m)$。空间位置为 $\vec{x}\in Z$ 的元胞的邻居有 $\vec{x}+\vec{x}_i, i=1,2,\cdots,m$;

f:局部转换函数,又简称为规则,是从 S^m 到 S 的映射;

根据定义,一维元胞自动机的邻域向量可以表示为 $N=(\langle -r\rangle,\cdots,\langle -1\rangle,\langle 0\rangle,\langle 1\rangle,\cdots,\langle r\rangle)$,其演化过程的一般表达式为:

$$s_i^{t+1}=f(s_{i-r}^t,\cdots,s_i^t,\cdots,s_{i+r}^t),i\in Z \quad (1)$$

*)国家自然科学基金(批准号:90718021)重点项目资助的课题。平 萍 博士研究生,研究方向为信息安全、细胞自动机、加密技术理论与算法设计;周 曜 博士研究生,研究方向为信息安全与移动自组织网络;张 宏 教授,博导,研究方向为信息安全、数据挖掘;刘凤玉 教授,博导,研究方向为信息安全、入侵检测、软件抗衰。

其中 r 表示规则半径，s_i^t 为第 i 个细胞在 t 时刻的状态。

定义 2 设 $CA_a=(d,S,N,f_a)$，$CA_b=(d,S,N,f_b)$ 是两个元胞自动机系统，称

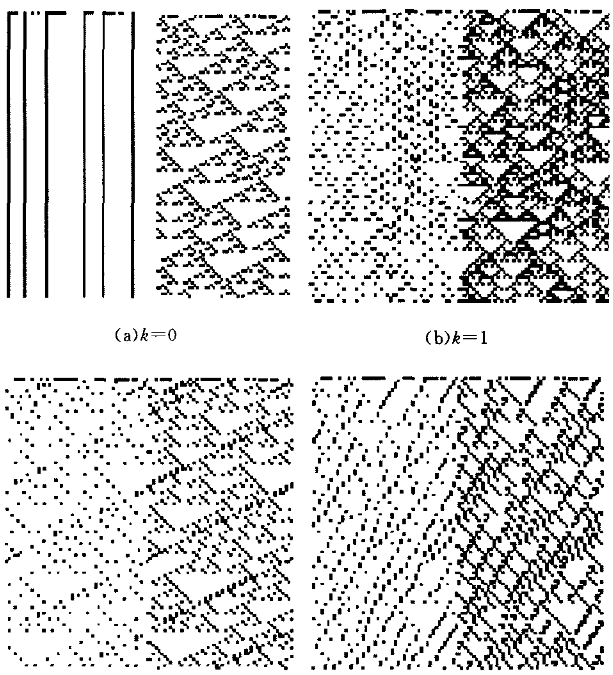
$$\begin{cases} s_{a,i}^{t+1}=f_a(s_{a,i-r}^t,\cdots,s_{b,j}^t,\cdots,s_{b,j+k-1}^t,\cdots,s_{a,i+r}^t) \\ s_{b,i}^{t+1}=f_b(s_{b,i-r}^t,\cdots,s_{a,j}^t,\cdots,s_{a,j+k-1}^t,\cdots,s_{b,i+r}^t) \end{cases} \tag{2}$$

$$0\leqslant k\leqslant 2r+1,\ i-r\leqslant j\leqslant i+r-k+1$$

是由 CA_a 和 CA_b 构成的耦合元胞自动机系统，记为 $CCA=(d,S,N,f_a,f_b,k)$，其中 k 称为耦合系数，表示两个元胞自动机的邻域内共有 k 个元胞进行了置换，j 表示置换的开始位置。

2.2 耦合系数对时空演化的影响

耦合系数 k 的取值大小反应了两个元胞自动机相互作用、相互影响的程度，即耦合程度。当 $k=0$ 时，表示完全不耦合，等同于两个独立的元胞自动机系统；当 $k=1$ 时，称为单耦合元胞自动机系统，两个元胞自动机的邻域内只有一个元胞进行了置换，如文献[8]中使用的元胞自动机系统；当 $1<k\leqslant 2r+1$ 时，称为多耦合元胞自动机系统，即两个元胞自动机的邻域内有多个元胞进行了置换。图 1 给出了耦合系数 k 分别取 0,1,2,3 时耦合元胞自动机系统的时空演化情况，其中参数设置为：$d=1$，$S=\{0,1\}$，$r=2$，$f_a=144$，$f_b=262$ 以及 $j=r$。



(a) $k=0$　　(b) $k=1$

(c) $k=2$　　(d) $k=3$

图 1 耦合元胞自动机系统的时空演化图

从图中可以看到，当 $k=0$ 时，是两个独立的元胞自动机系统的演化过程，左边元胞自动机系统的演化具有不变性，右边元胞自动机的演化具有分形自相似的特点。随着 k 的增大，两个元胞自动机之间的相互作用越明显，当 $k=3$ 时，左边元胞自动机演化过程中的不变性已被破坏，右边元胞自动机的演化也没有明显的分形自相似特征，而是一种无序混乱的形态。因此，在耦合元胞自动机系统中，耦合元胞个数越多，扩散作用越明显，它能将一个元胞的变化更大范围地扩散开去，影响其它元胞。

3 对 CTCA 密码系统的分析

文献[8]提出了一种基于耦合触发元胞自动机的密码系统，这里简称为 CTCA，利用两个元胞自动机邻域内中心位置元胞的置换实现耦合，属于单耦合元胞自动机系统。在 CTCA 中用到了一种特殊的触发规则，其一般演化表达式为：

$$1-s_i^{t+1}=f(s_{i-r}^t,\cdots,1-s_{i+l}^t,\cdots,s_{i+r}^t)\quad -r\leqslant l\leqslant r,l\in\mathbb{Z} \tag{3}$$

其中 l 表示触发元胞的位置。当 $l=-r$ 时，表示左触发规则；当 $l=r$ 时，表示右触发规则。只有这两种触发规则才具有无信息损失的特点。

结合耦合和触发的性质，以左触发规则为例，CTCA 中元胞自动机的演化表达式为：

$$\begin{cases} 1-s_{a,i}^{t+1}=f_a(1-s_{a,i-r}^t,\cdots,s_{b,j}^t,\cdots,s_{a,i+r}^t) \\ 1-s_{b,i}^{t+1}=f_b(1-s_{b,i-r}^t,\cdots,s_{a,j}^t,\cdots,s_{b,i+r}^t) \end{cases} \tag{4}$$

为了进一步说明耦合系数对密码系统的影响，首先对耦合系数 $k=1$ 的 CTCA 密码系统进行数据敏感性分析。

CTCA 的参数设置为：$d=1$，$S=\{0,1\}$，$r=1$，$f_a=30$，$f_b=90$。随机选取一明文序列，保持密钥不变，改变其中的一位，得到的密文序列与原明文的加密结果进行逐位比较，相同用"—"表示，不同则用"x"表示，测试结果如表 1 所示。

表 1 单个明文误差的扩散

步骤	元胞自动机A（rule30）	元胞自动机B（rule90）
0	--------------x----	--------------------
1	----- x--------------	------------ -------------
2	---------x-x-x-x------------------	--------------------------------
3	-------x-x-x-x-x--------------------	---------------------------------
4	-------x---x---x----------------------	-----------------------------------
5	-- x x x x-x-x--------------------	----- ----------------
6	x-x-x-x-x-x-x---x------------------------	-------------------------------------
7	--x---x---x-x-x-x--------------------------	--------------------------------------
8	--x---x-----x---x----------------------------	---------------------------------------
9	--x---x--- -x x x ------------------------	------------------ -- ---------------

从表 1 可以看出，CTCA 的误差扩散只是局限于元胞自动机 A 的范围内，并未影响元胞自动机 B 的演化，这种现象并非偶然，我们仔细分析规则 30 和规则 90 的真值表会发现，规则 30 的布尔表达式为 $s_i^{t+1}=(s_i^t+s_{i+1}^t)\oplus s_{i-1}^t$，规则 90 的布尔表达式为 $s_i^{t+1}=s_{i-1}^t\oplus s_{i+1}^t$，故由式(4)可得该耦合元胞自动机的演化表达式为：

$$\begin{cases} s_{a,i}^{t+1}=(s_{b,i}^t+s_{a,i+1}^t)\oplus s_{a,i-1}^t=f_a(s_{a,i-1}^t,s_{b,i}^t,s_{a,i+1}^t) \\ s_{b,i}^{t+1}=s_{b,i-1}^t\oplus s_{b,i+1}^t=f_b(s_{b,i-1}^t,s_{b,i+1}^t) \end{cases} \tag{5}$$

根据演化表达式可知，元胞自动机 A 中，元胞的演化不仅与自身邻域内的元胞状态有关，而且和配对的元胞自动机 B 邻域内的元胞状态有关，因此元胞自动机 A 的演化受元胞自动机 B 的影响。而元胞自动机 B 中，元胞的演化只与自身邻域内的元胞状态有关，不受元胞自动机 A 的影响。由此可知，虽然 CTCA 将元胞自动机 A 和 B 邻域内中心位置的元胞 $s_{a,i}^t$ 和 $s_{b,i}^t$ 进行了置换，但上述两个元胞自动机之间的作用是单向的，并且这种单向性在 CTCA 中是普遍存在的，若 CTCA 中有一个元胞自动机的演化规则具有如下形式：

$$s_i^{t+1}=f(s_{i-r}^t,\cdots,s_{i-1}^t,s_{i+1}^t,\cdots,s_{i+r}^t) \tag{6}$$

这种单向性便存在，若 CTCA 中两个元胞自动机的演化规则都具有式(6)的形式，那么置换中心元胞并不能使它们相互影响，该耦合元胞自动机系统实则是两个独立的元胞自动机系统。

由于单耦合元胞自动机的相互影响范围有限，使得攻击

者能够通过寻找密文的相似性获得明文的相关信息，从而降低了耦合元胞自动机密码系统的安全性。

表 2　规则 30 和 90 的真值表

$s_{i-1}^t s_i^t s_{i+1}^t$	Rule 30 $s^{t+1}{}_i$	Rule 90 s_i^{t+1}
001	0	0
001	1	1
010	1	0
011	1	1
100	1	1
101	0	0
110	0	1
111	0	0

4　多耦合元胞自动机密码系统设计

为了克服单耦合元胞自动机密码系统中存在的密文相似性问题，本文构造一种多耦合元胞自动机密码系统，不仅扩大了两个元胞自动机之间相互作用的范围，而且将多个元胞耦合，起到了加速扩散作用，它能将一个元胞的变化更快扩散开去，从而影响其它元胞。

根据多耦合和触发的性质，以左触发规则为例，可以构造一类特殊的多耦合触发元胞自动机：

$$\begin{cases} 1-s_{a,i}^{t+1}=f_a(1-s_{a,i-r}^t,\cdots,s_{b,j}^t,\cdots,s_{b,j+k-1}^t,\cdots,s_{a,i+r}^t) \\ 1-s_{b,i}^{t+1}=f_b(1-s_{b,i-r}^t,\cdots,s_{a,i}^t,\cdots,s_{a,j+k-1}^t,\cdots,s_{b,i+r}^t) \end{cases}$$

$$k>1 \qquad (7)$$

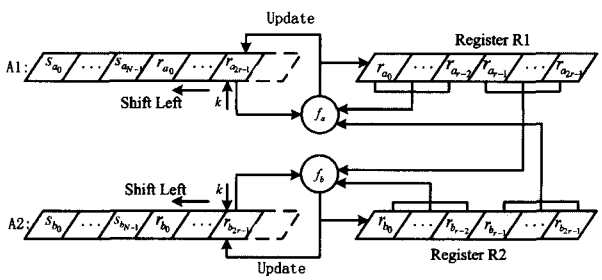


图 2　多耦合触发元胞自动机数据加密模型

密码系统的加密过程是一个多耦合元胞自动机系统的迭代过程，取一类特殊的触发规则为密钥，将明文编码作为初始状态，反向迭代一定时步得到的最终状态即为密文。接收方收到密文之后，使用同一个多耦合元胞自动机系统以及同一个触发规则，正向迭代与加密相同时步，恢复得到明文。

图 2 和图 3 分别给出了耦合位置 $j=r$，耦合系数为 $k=r+1$ 的多耦合元胞自动机系统加密模型和解密模型。

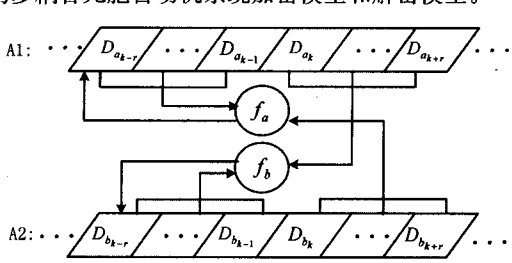


图 3　多耦合触发元胞自动机数据解密模型

5　仿真实验与安全性分析

5.1　仿真实验

以明文“cellular”为例，通过编码器输出对应的二进制序列为“01100011011001010110110001101100011101010110110001100010011100101”。采用耦合系数 $k=2$ 的多耦合触发元胞自动机密码系统对明文加密，得到结果如下：

表 3　多耦合触发元胞自动机中 A 的加密过程

步骤	元胞自动机A加密（rule30）
0	01100011011001010110110001101100011
1	10010011010110011001001010010110100
2	10101100101111101110110101101001011110
3	00110011010001110111011001011101010001010
4	11001111011110000111000101011110001101000
5	01001110100101111000111001001010000011001010
6	01010001011010100111001011011010111101011010
7	10101110100101010111110100100100100100100101010101
8	01011001100010101000101011000111011010010101101001
9	10101000011110110111010100000100000010010010011010
10	01010101100001111001001100111011111111010001001010100

表 4　多耦合触发元胞自动机中 B 的加密过程

步骤	元胞自动机B加密（rule90）
0	01110101011011000110000101110010
1	00111000000010100010101100111111000
2	10001010111100011001110110001101011010
3	01000111111011000100010011111000011111111
4	01111010000011011000000110000000100101101
5	01000000001010011101111010001010010000111000001
6	00000101111110100111011001111111101011000101111
7	10111111101011111000001011101101000100011110101010
8	11011001100000101101010011111000010110100100000111
9	01111000011010000111110111100000100100000001010101111
10	00101110011011000110001000011110111100010000000001110

表 5　多耦合触发元胞自动机中 A 的解密过程

步骤	元胞自动机A解密（rule30）
0	01010101100001111001001100111011111111010001001010100
1	10101000011101101110101000001000000100100100101101 0
2	01011001100010101000101011000111011010010101101001
3	10101110100101010111110100100100100100100101010101
4	01010001011010100111001011011010111101011010
5	01001110100101111000111001001010000011100101
6	11001111011110000011100010101111000111010000
7	00110011010001110111011001011101010000101
8	10101100101111101110110101101001110
9	10010011010110011001001010010011010 0
10	01100011011001010110110001101100001

表 6　多耦合触发元胞自动机中 B 的解密过程

步骤	元胞自动机B解密（rule90）
0	00101110011101100011000100001111010111000100000000001110
1	01111000011010000111110111100000100100000001010101111
2	11011001100001011010100111111000010111010001000001111
3	10111111101010111100000101110110100010001111010101 0
4	00000101111111010011101100111111110101100010111 1
5	01000000010100111011110100010100100011100001
6	01111010000011011000000110000000100101101
7	01000011111011000100010011111000001111111
8	10001010111100011001110110001101011010
9	00111000000010100010101100111111000
10	01110101011011000110000101110010 1 0

5.2　安全性分析

5.2.1　密钥空间

规则的空间即为密钥的空间，单个触发元胞自动机规则空间（密钥空间）为 $2^{2^{2r}}$，那么多耦合触发元胞自动机的规则空间（密钥空间）为 $2^{2^{2r}}\times 2^{2^{2r}}$。如果使用穷举法对密文分析，当规则半径 $r=4$ 时，最坏的情况要尝试 $2^{2^{2r}}\times 2^{2^{2r}}=1.34\times 10^{154}$ 次，这使得蛮力攻击变得不可能。

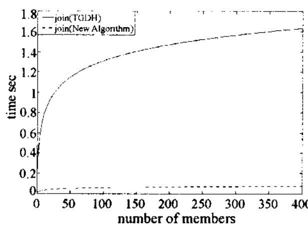
5.2.2　数据敏感性测试

我们使用相同的参数设置（$d=1$，$S=\{0,1\}$，$r=1$，$f_a=30$，$f_b=90$）对耦合系数为 $k=2$ 的多耦合元胞自动机加密系统进行数据敏感性测试，结果如表 7 所示。

（下转第 121 页）

4 性能分析

本算法的存储开销与基于密钥树的组密钥分发具有相同的特点:组成员的存储开销为 O(log$n$)。成员加入时最多只需 4 次 DH 计算和 5 条单播消息,而 TGDH 算法共需要 $2D+3$ 次 DH计算,以及 3 条单播消息。当成员离开时,最多需要 4 次 DH 计算和 D 次加解密计算及通信量,而 TGDH 算法需要 $2(D-1)$次 DH 计算和 2 次通信量,可见本算法在成员离开时将计算开销转化为通信开销。由于本算法采用 3 叉树,当成员数量相同时,本算法的效率要高于 TGDH 算法。算法的试验平台采用的是网络仿真工具 NS2,它可以完整地模拟整个网络环境。图 5 是 NS2 环境下得到的 TGDH 算法和新算法在成员加入时新的组密钥建立时间比较,从图中可以看出,本算法在组建立时具有明显的优势;图 6 是两种算法在成员离开时新的组密钥建立时间比较,当组规模越大,新算法优势越明显。



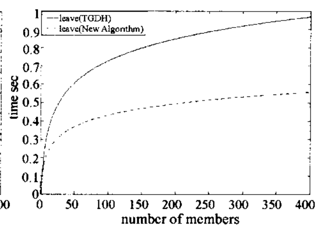


图 5 成员加入组密钥建立时间比较　图 6 成员离开时组密钥建立时间

结束语 本文探讨了一种可用于成员关系对等的组播组的密钥建立及分发的新算法。算法基于组播组的特性采用密钥协商的方法为成员通信建立基本的密钥链,并利用了集中式密钥管理中可信节点为组成员生成和分发密钥具有高效率高可扩展性的优点,根据节点位置的不同选择不同的 sponsor,负责生成和分发密钥,从而很好地解决了集中式密钥分发算法中的单点失效问题,实验证明本算法具有一定的实用性。

参考文献

[1] Hardjono T , Cain B , Doraswamy N . A Framework for Group Key Management for Multicast Security[Z]. IETF,1999

[2] Wong C K,Gouda M,Lam S S. Secure group communications using key graphs. IEEE/ACM Transactions on Networking, 2000,8(1):16-30

[3] Setia S , Koussih S , Jajodia S , et al . Kronos : a scalable group rekeying approach for secure multicast[A]//IEEE Symposium on Security and Privacy[C]. Oakland(USA)CA:IEEE computer Society Press,2000:215-228

[4] Steiner M,Tsudik G,Waidner M. Diffie-Hellman Key Distribution Extended to Group Communication // Proceedings of 3rd ACM Conference on Computer and Communications Security [C]. 1996

[5] Burmester M , Desmedt Y . A Secure and Efficient Conference Key Distribution System

[6] Steiner M,Tsudik G,Waidner M. CLIQUES:A New Approach to Group Key Agreement//Proceedings of ICDCS'98[C]. 1998

[7] Diffe W,Hellman M E. New directions in cryptography. IEEE Trans. Inform. Theory,1976,IT-22:644-654

[8] Kim Y,Perrig A,Tsudik G. Simple and Fault-Tolerant Key Agreement for Dynamic Collaborative Groups// Jajodia S,ed. 7th ACM Conference on Computer and Communications Security [C]. Athens,Greece,2000:235-244

[9] Goshi J,Ladner R E. Algorithms for Dynamic Multicast Key Distribution Trees // 10th ACM Conference on Computer and Communications Security[C]. Boston,USA,2003:240-246

[10] Wallner D,Harder E,Age R. Key management for multicast:Issues and architectures. IETF RFC2627,1999

[11] Snoeyink J,Suhi S,Varghese G. A Lower Bound for Multicast Key Distribution//IEEE INFOCOM. 2001

[12] http//www. crypto. com

(上接第 109 页)

表 7 单个明文误差的扩散

步骤	元胞自动机A (rule30)	元胞自动机B (rule90)
0	———————x———————	———————————————
1	-xxxxxx-xx- xx-x————————	xxxxx-xx- xx-x- - - - - -
2	-xxxxxx-xx—xx—x——————————	—————————————————
3	—xxxx-x-x-xx—x———————————	-xxxx-x-x-xx—x———————————
4	—xxxx-x-x-xx- -x————————————	- —— ————————— - - - -
5	-x-xxx-x-xx-x—x————————————	-xxx-x-xx-x—x—————————————
6	-x-xxx-x-xx-x—x—————————————	————————————————————
7	-x- —xx-xx- - x -	- - xx xx——x————————————
8	-x——xx-xx——x————————————	———————————————————————
9	-x———x—x-x—x—————————————	———x—x-x—x—————————————

与前面的表 1 比较,由于多耦合元胞自动机系统对多个元胞进行了置换,扩大的两个元胞自动机相互影响的范围,使得原来单向作用的两个元胞自动机转变为相互作用,误差扩散的速度也有了明显的提高。

结束语 本文对耦合元胞自动机系统进行了深入的研究,给出了耦合元胞自动机系统的一般定义,并用耦合系数分析了不同耦合元胞自动机系统的动力学行为。针对单耦合元胞自动机密码系统中的不足,提出了一种新的多耦合元胞自动机密码系统。仿真结果表明,多耦合元胞自动机系统比单耦合元胞自动机系统具有更强的相互作用能力,更为快速的误差扩散,因此具有很高的安全性。

参 考 文 献

[1] 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

[2] Wolfram S. Cryptography with cellular automata[C]. Advances in cryptology // Crypto' 85 Proceedings, LWCS, 218. Berlin: Springer -Verlag,1986:429-432

[3] Sipper M , Tomassini M . Generating parallel random number generators by cellular programming[J]. International Journal of Modern Physics C,1996,7(2):181-190

[4] Zhao X L,Li Q M,Xu M W,et al. A Synmmetric cryptography based on extended cellular automata[C]//IEEE-SMC2005. Hawaii USA,2005,10

[5] Guan P. Cellular automata public-key cryptosystems[J]. Complex System,1987,1:51-57

[6] Mihaljevic M,Zheng Y,Imai H. A family of fast dedicated one-way hash functions based on linear cellular automata over GF (q) [J]. IEICE Transactions on Fundamentals, 1999, E82-A (1):40-47

[7] Gutowitz H. Method and apparantus for encryption,decryption and authentication using dynamical systems [P]. USA:5,365,589,1994

[8] 赵学龙,游静,李千目,等. 耦合触发元胞自动机在数据加密中的应用[J]. 信息与控制,2005,34(6):746-752