基于忆阻细胞自动机的图像像素值置换加密技术

王晓东 王丽丹 段书凯
(西南大学电子信息工程学院 重庆 400715)

摘 要 忆阻细胞自动机是一种全新的细胞自动机,它的响应会引起细胞状态和细胞间链接状态的变化。在分析了忆阻细胞自动机中的细胞间链接状态丰富变化的基础上,设计了一种全新的图像加密算法:以一个 $W\times H$ 的忆阻自动机阵列为公钥,以细胞的初始状态和细胞迭代次数为私钥,将细胞与相邻细胞间的一组链接状态加权后设置成加密矩阵,同时采用像素置换方法对数字图像进行加密。这种加密算法具有较好的混乱特性、扩散特性和良好的保密性、抗蛮力破解特性,能够满足数字图像加密的安全性要求。

关键词 忆阻细胞自动机,图像加密,像素替换
中图法分类号 TP391.41 **文献标识码** A

Pixel Value Replacement Method to Encryption Image Based on Memristive Cellular Automata

WANG Xiao-dong WANG Li-dan DUAN Shu-kai
(School of Electronics and Information Engineering, Southwest University, Chongqing 400715, China)

Abstract Memristive cellular automata is a kind of new cellular automata, and its operation can produce transformation of cells state and make its links changed. We analyzed the varied change of cellular automata and the links between the cells, then we designed a new encryption algorithm: use a $W\times H$ cells automata arrays as Public-Key, the initial states and respond time as Private-Key, get the links between the cells as a encryption matrix. Meanwhile, we used the pixel value replacement method to encrypt a image. This algorithm has the advantage of confusion and diffusion properties, besides, it owes its advantage in fine security, large key space and diffusion. The algorithm analyzes turn out that this method is of high encryption efficiency and security, which could just meet the digital image demands on security.

Keywords Memristive cellular automata, Image encryption, Pixel value replacement

1 引言

随着信息技术的发展,数字图像传输应用也越来越广泛,图像信息的安全与保密也引起人们的高度重视。因此,寻找能够改变图像信息的统计特性以及构建庞大的密钥空间,是数字图像加密的重要研究方向。

近年来,利用细胞自动机(Cellular Automata, CA)进行密码系统的设计吸引了众多学者的关注,其原因就在于CA能通过简单的规则来实现复杂的行为模式[1-4]。1985年,S. Wolfram首次利用细胞自动机的前向迭代来生成密钥流,开创了细胞自动机在密码学领域中的应用[5]。此后很多研究表明,可以通过提高细胞自动机结构的复杂性,如提高细胞自动机的维数或采用动态规则方法,来提高密钥流的周期和安全性(即随机性)[6-8]。2009年,M. Itoh 和 L. O. Chua 设计了基于忆阻器的细胞自动机(Memristive Cellular Automata, MCA)[9],随后 A. Adamatzky 和 L. O. Chua 在此基础上分析了忆阻细胞自动机的动态特性[10]。这种忆阻细胞自动机复杂的动态特性很适合于数字图像的加密算法。本论文根据忆阻细胞自动机初始状态的敏感性和链接状态的复杂性,提出了一种基于忆阻细胞自动机的图像加密算法。该算法很好地改变了图像的统计特性,具有安全性好、密钥量大等特点。实验分析表明,该方法具有较高的加密效率和安全性。

本文第2节分析忆阻细胞自动机的动态特性,然后推出运用细胞间链接状态的加密算法;第3节中运用该算法对图像进行加密实验并分析加密的效果;最后在第4节中对图像加密实验进行了分析并提出了进一步的工作展望。

2 基于忆阻细胞自动机的数字图像加密算法

2.1 演化规则的设定[9,10]

忆阻自动机是一种以动态激励结构的细胞自动机,每个细胞通过链接获得与它邻近细胞的信息。每个细胞的状态更新取决于它紧邻且彼此间链接是导通的那些细胞的状态,且每个细胞都通过同样的规则同步更新自己的状态。忆阻细胞自动机的细胞有3种状态:休眠状态、激励状态和抑止状态。

到稿日期:2012-11-09 返修日期:2013-03-22 本文受国家自然科学基金(60972155,61101233),教育部"春晖计划"科研项目(z2011148),中央高校基本科研业务费专项资金(XDJK2012A007,XDJK2010C02),重庆市高等学校青年骨干教师资助计划(渝教人〔2011〕65号),重庆市高等学校优秀人才支持计划(渝教人〔2011〕65号),留学人员科技活动项目择优资助经费(国家级优秀类,渝人社办〔2012〕186号)资助。
王晓东(1985—),男,硕士生,主要研究方向为通信电路与系统、模式识别,E-mail:vikings335@gmail.com;王丽丹(1976—),女,博士,副教授,硕士生导师,主要研究方向为人工神经网络、非线性系统与电路设计,E-mail:ldwang@swu.edu.cn(通信作者);段书凯(1973—),男,博士,教授,博士生导师,主要研究方向为人工神经网络、非线性理论与电路。

每个链接有导通和截止两种状态，用状态 0 和状态 1 表示。每个链接的状态更新取决于它所连接的细胞状态。让 $u(x)=\{y:|x-y|_{\infty}=1\}$ 是元胞 x 的邻居。细胞 x 的一组输入链接 $\{l_{xy}:y\in u(x)\}$ 中，只有 $x^t,y^t\in(+,-)$ 且 $x^{t=+}$、$y^t=-$ 时链接 l_{xy} 是导通的，反向的 l_{yx} 则为截止的。

这里采用两种方法来计算活跃邻居细胞的加权和：

$$\Sigma_+=\sum_{y\in u(x)}x(y^t,+) \tag{1}$$

$$\sigma_+=\sum_{y\in u(x)}l_{xy}x(y^t,+) \tag{2}$$

这里，当 $y^t=+$ 时，$x(y^t,+)=1$，其余情况下 $x(y^t,+)=0$。

因此，我们考虑两种类型的忆阻自动机。如果 $\sigma_+>0$，则自动机 A_1 为休眠细胞被激活。如果 $\Sigma_+>1$ 或 $\sigma_+>0$，则自动机 A_2 为休眠细胞被激活。

A_i^{01}（$i=1$ 或 2）细胞自动机在响应激励的同时，在激励传播方向上的链接会转换为抑止状态。同理我们可以知道，A_i^{10} 细胞自动机在响应激励的同时，在激励传播反方向上的链接会转换为抑止状态。

2.2 数字图像的加密算法设计

忆阻细胞自动机是二维细胞自动机，细胞分布在无穷大平面的格点上，而一般的图像都是有限长和有限宽的，这样为了在图像上应用忆阻细胞自动机，必须在技术上做一些处理。解决的方法是将自动机看作一个拓扑平面，即认为图像的上下左右边界都是吸收边界，亦即当细胞自动机的响应传递到边界上时，边界的细胞不产生响应，就好像激励被吸收了一样。这样我们就只用考虑图像的中间点有 8 个邻居，边界的细胞都默认处于休眠状态，不参与响应。

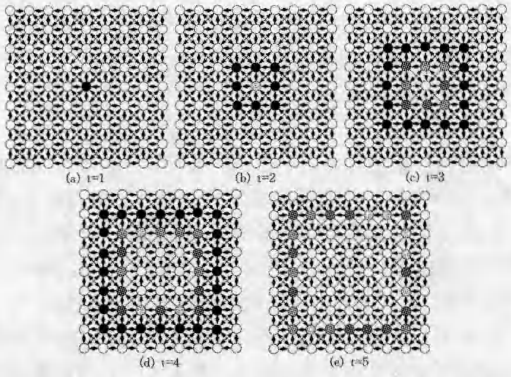


图 1 A_1^{01} 细胞自动机的激励响应和链接状态的改变

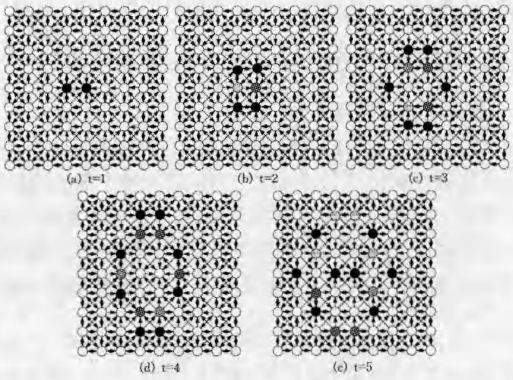
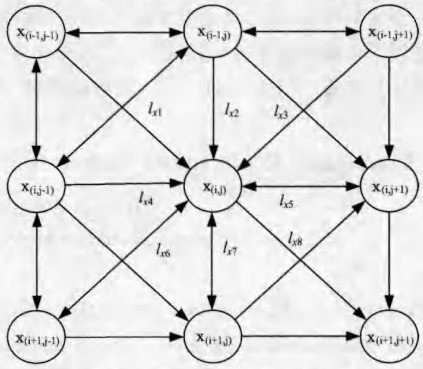


图 2 A_2^{01} 细胞自动机激励响应和链接状态的改变

我们首先建立一个 A_1^{01} 细胞自动机模块，如图 1 所示，对它施加激励，待经过一段时间的响应达到平衡之后，细胞间的链接状态会产生很大的变化。然后将图 1(e) 链接状态赋值给 A_2^{01} 细胞自动机模块，如图 2 所示，施加激励响应一段时间。然后，经过两种细胞自动机特有的初始状态响应，细胞间将会出现独特的连接状态，如图 2(e) 所示。其中黑色细胞表示激活状态，灰色细胞表示抑止状态，白色细胞表示休眠状态，箭头表示细胞间连接的导通状态。

这里，我们知道每两个细胞间的链接都是双向的，如果把通向代表同一个细胞 $x_{(3,3)}$ 的所有链接 l_{wx}（w 为 x 周围邻居的位置）定义为一组，就相当于定义了整个细胞自动机的所有链接。然后按照链接状态 0 为阻断、1 为导通，将细胞 $x_{(i,,j}$ 的所有链接按图 3 的 $l_{x1}-l_{x2}$ 的顺序从高位到低位排列为一个 8 位二进制数，再把该二进制数转化为一个十进制数，这样通过图 2(e) 中 $x_{(3,3)}$ 来分析细胞与周围邻居的链接（见图 3）。



细胞 $x_{(i,j)}$ 经过激励响应后的一组链接由由指向 $x_{(i,j)}$ 的一组箭头表示。则该细胞的链接状态所表示的权值为 $(1111\ 1110)_2$ 或 $(254)_{10}$。

图 3

这样，对应要加密的图像，我们按照其像素多少生成两个二维忆阻细胞自动机阵列。忆阻细胞自动机中的每个细胞都会有一组链接响应，可对应于需加密图像的像素点产生一个数据矩阵，而每一个非边界细胞都有 8 条通向自己的链接，所代表的二进制数转换为十进制有 0～255 种可能，且每个细胞的链接状态都会有很大差异，因此使用忆阻细胞自动机的链接来进行图像加密十分可靠。

3 图像加密数值仿真实验

以灰度图像为例，说明如何使用忆阻细胞自动机对图像加密。对于 $W\times H$ 的灰度图像，首先生成 $W\times H$ 的二维忆阻细胞自动机阵列，然后采用两个初始状态 D_1 和 D_2 对忆阻细胞自动机进行两次激励，激励响应的次数 t_1 和 t_2 由加密方和解密方共同约定（注意 t 抑止太小，至少要等于 W 或 H 中最小者的 1/2，否则会影响保密性），响应后得到的独特链接状态值和目标图像像素异或就可用于图像的加密和解密。

3.1 仿真实验

对 200×188 的灰度图像 lena（如图 4 所示）进行加密时，首先生成两个 200×188 的二维忆阻细胞自动机阵列，建立一个 A_1^{01} 细胞自动机模块，对它施加激励，待经过一段轮次的响应达到平衡之后，细胞间的链接状态会产生很大的变化（选用有图像像素点数目 0.08% 的细胞为激活状态初始配置的初始激励，并设定激励响应次数 $t_1=t_2=100$）。然后将细胞间的链接状态赋值给 A_2^{01} 细胞自动机模块，再施加 t_2 次激励响应。这时，经过两种细胞自动机特有的初始状态响应，细胞间将会出现独特的链接状态，如图 5 所示。然后把图 4 和图 5 相同位置的像素异或得出加密后的图像，如图 6 所示，再把

加密后的密图(见图 6)发送给接收方。

在进行解密时,接受方按照生成细胞自动机,同时采用相同激励和响应次数进行操作,然后将得到的链接转化图与得到的加密图像进行像素异或,即可得到解密后的图像,如图 7 所示,它与原始图像(见图 4)完全相同。

图 4 原始图像

图 5 生成的链接转化图像

图 6 加密后得到的图像

图 7 解密后的图像

这里可以看到,实验中的加密算法和解密算法实际上是分别用忆阻细胞自动机系统进行的完全相同的两次迭代处理产生的。忆阻细胞自动机动力学中的零误差特性[1]产生完全同步的结果,为本实验的可行性提供了良好的数据支持。

3.2 安全性分析

1)密钥量大

在图像加密时,选取图像像素点数目 0.08%的细胞为激活状态的初始配置。以 188×200 的 lena 图为例,需选择 30 个像素点的细胞为激活状态,则选择一组初始状态的密钥选取有 C_{37600}^{30} 种可能,那么两次迭代所选取的密钥量将会达到 10^{209},再加上两次迭代时间的选择,将使得整个算法的密钥空间非常大,保密性更强;而由于忆阻细胞自动机的同步运行特性,使得庞大的密钥空间对加密和解密速度却没有太大的影响,且使用蛮力搜索攻击将遭遇不可思议的困难。对相同大小图像,这个密钥量远大于中臧鸿雁等基于离散混沌系统广义同步定理的数字图像加密方案[11]的 10^{76} 的密钥量,也大于朱从旭等使用一种基于广义 Chen 氏混沌系统的图像加密算法[12]的 10^{44} 的密钥量。

2)扩散性好[7]

在加密和解密过程中,所产生的效果由系统中初始激活细胞的位置即密钥决定。从忆阻细胞自动机的动力学特性的式(1)和式(2)可以得到,忆阻细胞自动机进行迭代时,每个细胞的状态变化取决于与之相邻的细胞以及之间链接的状态。因此,初始状态的每一个激活细胞都会如图 1 和图 2 所示向周围扩张自己的影响。因此在初始时激活细胞位置的改变,将会在迭代 n 次后影响到邻近大范围细胞的状态。同时,我们也可以知道,细胞间的链接状态在迭代过程中与细胞状态息息相关,也就是说加密数据的产生与初始状态的激励紧密联系,即不同初始状态的系统在经过两轮设定的迭代次数后,逐步形成的链接状态将会产生惊人的不同,这就为我们的图像加密提供了良好的加密数据。

选用另一组初始细胞状态作为密钥,经过相同次数的迭代后生成的链接转化图像如图 8 所示。图 9 即为第一次实验的加密数据与第二次试验的解密数据相作用后的解密效果图。可以看到,选择不相同的初始状态所得到的解密数据无法解开加密图像。

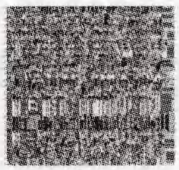


图 8 另一组初始细胞状态生成的链接转化图像

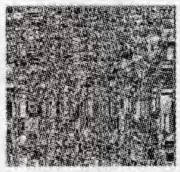
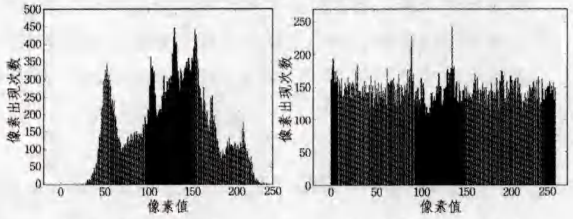


图 9 图 8 与图 6 图像像素值异或解密的图像

3)统计特性

通常来说,每张图片都有自己的统计特性,如果图像的像素置换效果不好,可通过像素的统计特性进行破解[13]。我们分析了原始图片和加密图片的统计特性(见图 10)。



(a) 原始图像的直方图 (b) 加密后图像的直方图

图 10 直方图分析

可以看出,经过加密后的像素能够被较均匀地转换,原图像的像素统计特性已经被完全改变,降低了原图像与加密后图像的相关性,增强了系统的抗破解能力。

结束语 本文在忆阻细胞自动机的基础上,提出了一种全新的细胞自动机模型,通过采用忆阻细胞自动机在响应激励的过程中产生的复杂的动力模型,设计了一个全新的加密矩阵。这种方法所产生的加密矩阵的混乱等级和扩散性较好,庞大的密钥空间也提高了蛮力破解的难度,加密后的密文图像像素也得到了近似均匀的置换。该方法是一种有应用前景的图像加密算法,不仅扩展了细胞自动机的研究内容,也为忆阻器在细胞自动机及神经网络中的应用提供了新的探索方向。

参 考 文 献

[1] Adamatzky A. Controllable transmission of information in excitable medium: the 2+medium[J]. Advanced Materials for Optics and Electronics, 1995, 5: 145-155

[2] Alonso-Sanz R. A structurally dynamic cellular automaton with memory[J]. Chaos, Solitons and Fractals, 2006, 32: 1285-1295

[3] Adamatzky A, Holland O. Phenomenology of excitation in 2D cellular automata and swarm systems[J]. Chaos, Solitons & Fractals, 1998, 3: 1233-1265

[4] Adamatzky A, Andrew W, Benjamin D L C. Glider-based computing in reaction-diffusion hexagonal cellular automata[J]. Chaos, Solitons & Fractals, 2006, 27(2): 287-295

[5] Wolfram S. Cryptography with cellular automat[J]. Advances in Cryptology, 1985, 218: 429-432

[6] Kuang T L. Information hiding based on binary encoding methods and pixel scrambling techniques[J]. Applied Optics, 2010, 49(2): 271-277

[7] Seredynski F, Bouvry P, Zomaya A Y. Cellular automata computations and secret key cryptography[J]. Parallel Computing, 2004, 30(5): 753-766

(下转第 168 页)

此外，从图中还可以看出与其它算法相比，Pair Copula 算法能在较少的存储空间下达到较高的查询精度。

结束语 由于数理统计中的 Pair Copula 方法可以准确快速地拟合高维随机变量的联合分布，且具有易于参数估计、模型构造灵活、可以全面捕捉维度间的线性与非线性关系等特点，本文首次将其引入到 OLAP 查询中，建立了基于“C 藤” Pair Copula 的高维 OLAP 查询模型。首先针对 OLAP 查询的特点设计了相应的 Pair Copula 查询模型，并同时给出了较为快捷的模型参数估计方法；接着结合 OLAP 操作的特点具体分析阐述了使用 Pair Copula 模型进行 OLAP 查询的具体过程，并给出了相应的算法；最后为了证明该算法的有效性，基于 4 组数据设计了对比试验，将本文提出的 Pair Copula 算法与经典 GENHist 算法、传统 Copula 算法进行了比较。实验结果显示相对于其它两种算法，本文提出的 Pair Copula 算法在同等条件下具有较低的平均查询误差以及较高的空间使用率，并且当数据维度较高时其查询效率要明显高于其它两种算法。

本文的研究是在传统 Copula 查询算法[14]上的进一步改进，取得了令人满意的研究结果。但仍然存在许多问题有待更深入的探讨。首先在数据挖掘方面，由于在使用 Copula 方法建立 OLAP 查询模型的同时建立了各维度样本间的联合分布，因此我们可以借此对维度间的关系进行挖掘，实现 OLAP 技术与数据挖掘的结合。其次，由于 Copula 方法同样可以用来拟合离散变量的联合分布，在今后的工作中，我们可以以此为出发点进行进一步的研究与实验，进一步扩大基于 Pair Copula 的 OLAP 建模方法的使用范围。

参 考 文 献

[1] Chaudhuri S, dayal U, Narasayya V. An overview of business intelligence technology [J]. Communications of the ACM, 2011, 54(8): 88-98

[2] Cuzzocrea A. Improving range-sum query evaluation on data cubes via polynomial approximation [J]. Data & Knowledge Engineering, 2006, 56(2): 85-121

[3] Barbará D, Wu X T. Loglinear-Based Quasi Cubes [J]. Journal of Intelligent Information Systems, 2001, 16(3): 255-276

[4] Chen Y, Dong G, Han J W, et al. Regression Cubes with Lossless Compression and Aggregation [J]. IEEE Transations on Knowledge and Data Engineering, 2006, 18(12): 1585-1599

[5] Poosala V, Ioannidis Y E. Selectivity estimation without the attribute value independence assumption [C]// Proceedings of the 23rd International Conference on Very Large Databases. Athens, Greece, August 1997: 486-495

[6] Gunopulos D, Kollios G, Tsotras V J, et al. Approximating Multi-Dimensional Aggregate Range Queries Over Real Attributes [C]// Proceedings of the 2000 ACM SIGMOD international conference on Management of data. Dallas, Texas, USA, May 2000: 463-474

[7] Rösch P, Lehner W. A Sample Advisor for Approximate Query Processing [C]// Proceedings of the 14th east European conference on Advances in databases and information systems. Novi Sad, September 2010: 490-504

[8] Li Xiao-lei, Han Jia-wei, Yin Zhi-jun, et al. Sampling cube: a framework for statistical OLAP over sampling data [C]// Proceedings of the 2008 ACM SIGMOD international conference on management of data. Vancouver, BC, Canada, June 2008: 779-790

[9] Chakrabarti K, Garofalakis M, Rastogi R, et al. Approximate Query Processing Using Wavelets [J]. The International Journal on Very Large Data Bases, 2001, 10(2/3): 199-223

[10] Heinen A, Valdesogo A. Asymmetric CAPM dependence for large dimensions: the canonical vine autoregressive model[M]. CORE discussion papers 2009069, Universit _ ecatholique de Louvain, Center for Operations Research and Econometrics (CORE), 2009

[11] Sklar A. Fonctions de répartition à n dimensions et leurs marges [M]. Publications de l'Institut de Statistique de l'Universite de Paris 8, 1959: 131-229

[12] Aas K, Berg D, Kurowicka D. Modeling Dependence Between Financial Returns Using Pair-Copula Constructions [M]. Dependence Modeling: Vine Copula Handbook. World Scientific, 2011: 305-328

[13] Bhat C R, Eluru N. A copula-based approach to accommodate residential self-selection effects in travel behavior modeling [J]. Transportation Research Part B: Methodological, 2009, 43(7): 749-765

[14] 高雅卓，倪志伟，倪丽萍. 连续属性上的 OLAP 查询建模方法研究[J]. 情报学报，2011，30(4)：372-379

[15] Aas K, Czado C, Frigessi A, et al. Pair-copula constructions of multiple dependence [J]. Insurance: Mathematics and Economics, 2009, 44(2): 182-198

[16] Shanmugasundaram J, Fayyad U, Bradley P S. Compressed Data Cubes for OLAP Aggregate Query Approximation on Continuous Dimensions [C]// Proceedings of the fifth ACM SIGKDD international conference on Knowledge discovery and data mining. San Diego, CA, USA, Aug. 1999: 223-232

[17] Acharya S, Gibbons P B, Poosala V, et al. The AQUA approximate query answering system [C]// Proceedings of the 1999 ACM SIGMOD international conference on Management of data. Philadelphia, Pennsylvania, USA, June 1999: 574-576

[18] Joe H. Families of m-variate distributions with given margins and m(m−1)/2 bivariate dependence parameters[J]. Lecture Notes-Monograph Series, 1996, 28: 120-141

[19] Patton A. Estimation of multivariate models for time series of possibly different lengths[J]. Journal of Applied Econometrics, 2006, 21(2): 147-173

(上接第 135 页)

[8] Itoh M, Chua L O. Advanced image processing cellular neural networks[J]. International Journal of Bifurcation and Chaos, 2007, 17: 1109-1150

[9] Itoh M, Chua L O. Memristor Cellular Automata and Memristor Discrete-Time Cellular Neural Networks[J]. International Journal of Bifurcation and Chaos, 2009, 19(11): 3605-3656

[10] Adamatzky A, Chua L O. Memristive excitable cellular automata [J]. International Journal of Bifurcation and Chaos, 2011, 21(11): 3083-3102

[11] 臧鸿雁，闵乐泉，吴春雪，等. 基于离散混沌系统广义同步定力的数字图像加密方案[J]. 北京科技大学学报，2007，29(1)：96-101

[12] 朱从旭，陈志刚，欧阳文卫. 一种基于广义 Chen's 混沌系统的图像加密新算法[J]. 中南大学学报：自然科学版，2006，37(6)：1142-1148

[13] Islam N, Puech W. Decryption of noisy encrypted images by statistical analysis[C]// 2011 3rd European Workshop on Visual Information Processing(EUVIP). Paris, 2011, 192-198