文章编号 1004-924X(2008)09-1781-06

基于有序细胞自动机的图像加密方案

张晓岩[1],王 超[2],孙志人[1],于 杨[3]
(1. 南京师范大学 数学与计算机学院,江苏 南京 210097;2. 南开大学 软件学院,天津 300071;
3. 南京师范大学 电气与自动化工程学院,江苏 南京 210097)

摘要:结合 Lafe 给出的基于细胞自动机变换的压缩技巧,提出了一个新的基于有序细胞自动机(CA)的图像加密方案。新的方案既利用了基于细胞自动机的变换对二维图像具有良好压缩效果的特点,又用有序细胞自动机的加密技术弥补了 Lafe 方案中加密效果不理想的缺点,使得密钥空间至少达到 $2^H\times2^{512}\times2^{33\,554\,432}$。模拟结果表明,该方案具有良好的细胞自动机雪崩效应的特性,即局部规则的微小改变将导致密文的大幅度变化,且具有易于实践、成本低等优点。由于有序细胞自动机具有平行结构简单、密钥量大和加密速度快的特点,所以这种加密技术非常适用于光学实现领域的应用。

关 键 词:细胞自动机;图像处理;图像加密;光学实现;密钥空间
中图分类号:TP309.7 **文献标识码**:A

An image encryption scheme based on sequential CA

ZHANG Xiao-yan[1], WANG Chao[2], SUN Zhi-ren[1], YU Yang[3]

(1. *School of Mathematics and Computer Science, Nanjing Normal University, Nanjing* 210097, *China*; 2. *College of Software, Nankai University, Tianjin* 300071, *China*; 3. *School of Electrical & Automation Engineering, Nanjing Normal University, Nanjing* 210097, *China*)

Abstract: Due to the universality of Cellular Automaton (CA) model, many applications have been found in traditional cryptography and image processing. Combined with Cellular Automaton Transform (CAT) compression technologies, an image encryption approach with enhanced security and more larger key space at least $2^H\times2^{512}\times2^{33\,554\,432}$ is proposed based on sequential CA. The simulation results show that the proposed scheme has the advantages of convenient realization, avalanche effect, confusion and diffusion properties, and low cost, which is suitable for optical realization based on the characteristics of simple parallelism structure of sequential CA, very large security key space and fast encryption speed.

Key words: cellular automata; image processing; image encryption; optical realization; key space

收稿日期:2008-01-30;**修订日期**:2008-03-21.
基金项目:国家自然科学基金资助项目(No. 10671095);中国博士后科研基金资助项目(No. 20070421028);江苏省博士后科研资助计划项目(No. 0602023C);南开大学科研创新基金资助项目(No. zlA2006019)

1 引　言

对图像进行光学处理与进行计算机处理比较起来，光学处理具有固有的优势。这是因为通过光学信息进行数据/图像加密不但具有可并行处理的优点而且还有利于提高安全性，是完全并行的、实时的，而且被认为是低廉开销的方法。如今它已被应用到图像处理的许多分支领域[1-3]。光学加密及安全应用[4-6]已经引起光学界相当的兴趣。近年来，由于基于细胞自动机的光学实现系统在大规模并行处理的全光学互联上的绝对优势越发地引人关注，用光学系统来实现细胞自动机算法也越来越方便。

虽然针对图像加密领域已经提出了很多算法，但是其中的很多加密方案仍然存在着潜在的缺陷。因此，为增加安全性，人们相继提出了许多新的技术和算法，例如在过去的几十年中混沌映射在图像加密中的应用[7-10]曾被广泛地研究过。近年来，人们发现将细胞自动机应用到密码系统和图像处理中具有越来越多的优点。Wolfram 给出了细胞自动机在密码系统中的第一个应用[11]，而且他还把细胞自动机引入到伪随机数的生成中，使它在流密码系统中得以应用。这种方法首先是用一个密钥通过伪随机数生成原来得到一个密钥流，然后对已经被依次分解为字节的密码流进行异或操作。其后，Nandi 等[12]给出了基于细胞自动机的块和流密码的应用；Madjarova 等[13]针对流密码的光学实现给出了不可逆的细胞自动机算法；Liang 等[14]提出基于混合加法细胞自动机的光学流密码系统，并对一维加法 CA 的同步系统进行了研究[15]，对 CA 在加密等方面的进一步应用具有参考价值；Chen 等[16]利用改进的细胞自动机变换代替像素点的值和基于 SCAN 方法进行图像像素点置换的技巧给出了一种图像加密的方法；文献[17]中概述了细胞自动机在密码学中的应用。

Lafe[18]介绍了基于细胞自动机变换(CAT)的数据压缩和加密方案，用细胞自动机变换的技术对数据进行编码和解码的操作。该方案从细胞自动机的进化状态集中生成一组基函数用于数据的压缩和加密。在 Lafe 的方案中，采用了最简单的 β-组基，参见文献[18]。在数据压缩过程中，用 CAT 揭示原始数据中的冗余信息，对图像的二维信息压缩时，细胞自动机变换的二维基函数可以很容易由一维基函数生成。Lafe 通过理论分析及与其它技术诸如 zero-tree 压缩方案[19]试验对比，证明了基于细胞自动机变换的图像压缩方案具有非常好的迭代速度和压缩率等。但是该方案对于图像的加密效果并不是很理想，其密钥空间并不是很大。本文结合 Lafe 给出的压缩变换原理，提出了基于有序细胞自动机的图像压缩加密方案，该加密方案没有继续流密码的原有思想以初值即初始配置作为密钥，而是利用基于有序细胞自动机的图像加密算法，以细胞自动机变邻域局部规则组合的有序排列为密钥，其变化空间远大于细胞配置的变化空间，进一步提高了密钥空间和安全性。细胞自动机变换对原始图像首先进行压缩变换以减少原始图像的冗余信息，有利于数据传输，其安全性又由基于有序细胞自动机加密方案所弥补，并且两类方法都具有细胞自动机雪崩效应的特性，即局部规则及密钥的微小改变将导致密文的大幅度变化。细胞自动机的简单平行结构非常适用于光学实现领域的应用。

2 基于有序细胞自动机的图像加密算法

细胞自动机是一个离散动力系统，它由被称为细胞的基本元素的配置及其局部变换规则 f 构成，并且细胞具有有限的状态，在局部规则的作用下同步更新。每个细胞都有 0 或 1 两个状态值，所有细胞状态的一个集合称为细胞自动机的一个配置。这里用二维细胞自动机作为一个具体描述的例子。Z^2 是二维细胞自动机的基本空间。以方点阵的格子图结构对细胞进行安排，细胞被放置在正方形的交叉点上。用(a,b)来代表一个在 z^2 上具有状态值为 0 或 1 的细胞，其包含 9 个点的邻域可表示为$(a\pm1,b)$，$(a,b\pm1)$，$(a\pm1,b\pm1)$和(a,b)。这种由(a,b)本身及距离它最近的 8 个特定的细胞构成的邻域称为 Moore 邻域。本文用 s_{ab} 表示细胞(a,b)的状态。那么 f 对这 9 个细胞的作用为

$$f(s_{a-1,b-1}\ s_{a-1,b}\ s_{a-1,b+1}\ s_{a,b-1}\ s_{ab}\ s_{a,b+1}\ s_{a+1,b-1}\ s_{a+1,b}\ s_{a+1,b+1}).$$

局部规则可以表示为：

$$f(000000000)=\varepsilon_1$$
$$f(000000001)=\varepsilon_2$$
$$\cdots$$
$$f(111111111)=\varepsilon_{512}$$

其中 $\varepsilon_i\in\{0,1\}$，且 $i\in\{1,2,\cdots,512\}$。f 被称为 1-邻域局部规则。为方便起见，把 f 写为 $\varepsilon_1\varepsilon_2\cdots\varepsilon_{511}\varepsilon_{512}$。例如 $f=0\mathrm{x}(06\ \mathrm{DB8}\ 3\mathrm{CA})^{16}$ 表示一个 128 位的十六进制数，即一个 512 位二进制数，由 16 个相同的十六进制数 06 DB8 3CA 的副本组合而成。一般地，把在 Z^2 上细胞 (x_i,x_j) 的 j-邻域记为

$$\{(y_1,y_2):|y_i-x_i|\leqslant j,1\leqslant i\leqslant 2,j\in Z^+\}。$$

对于 2-邻域来说，由于一个细胞的 2-邻域包含 25 个细胞，而且局部规则的独立变量的数目达到了 2^{25}，所以局部规则的集合将包含 $2^{2^{25}}=2^{33\ 554\ 432}$ 个元素。类似于 1-邻域的局部规则，把 2-邻域的局部规则 g 表示为 $\varepsilon_1\varepsilon_2\cdots\varepsilon_{33\ 554\ 431}\varepsilon_{33\ 554\ 432}$，例如

$g=(\mathrm{E\ 2A8\ 7F5\ 3C0\ 46B\ D19})^{524\ 288}$ 表示一个 8 388 608 位的十六进制数，即 33 554 432 位的二进制数，由 524 288 个十六进制数 E 2A8 7F5 3C0 46B D19 的副本构成。依此类推，一个 J-邻域的局部规则可以类似地去定义。

假设 $t=0$ 时的初始配置为 C_0，具有状态为 x_0 的细胞其 1-邻域集合的状态为 x_0，x_1，…，x_8。那么细胞在 $t=1$ 时状态为 $f(x_0,x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8)$。所有细胞的状态都可以用这个方法来得到。把这些状态合在一起就得到了一个新的配置 C_1，它可以认为是作用在 C_0 上的一个全局变换 ρ_f 作用的结果。进而可以得到 C_2，C_3，C_4 等等。

因为每一个图像在二维平面上都是有界的，所以必须解决二维细胞自动机的基本空间是无界二维平面的问题。为此，可以将图像的一组对边对应拼接，然后另外一组对边再拼接起来，形成一个胎面，这样每一个像素点都存在一个 9 个点的邻域。不失一般性，本文以高为 H，宽为 W 的黑白二值图 M 为例来说明如何用有序的细胞自动机来进行图像加密。所谓有序的细胞自动机即不同的局部规则按照一定顺序作用在细胞自动机的配置上。在黑白二值图 M 中，用 1 和 0 来表示细胞的黑白状态。图像 M 的每一行可以看作是长度为 W 的二进制字符串。

Alice 和 Bob 选择同样的一个 1-邻域的局部规则，记为 F_0，选择同样的一个 2-邻域的局部规则，记为 F_1，把 $S=\{1,2,\cdots,H\}$ 的子集记为 $I=\{i_1,i_2,\cdots,i_k\}$，其中 k 为预先给定的，且 $1\leqslant k\leqslant H$。

2.1　图像加密算法

(1) Alice 对原图 M 进行基于二维细胞自动机变换[18]的压缩编码操作，得到压缩图 C。

(2)由 Alice 生成一个初始的随机位图 R_C，使它与 C 具有相同的维数信息。R_C 具有 $t=0$ 时的配置。

(3)记 R_C 的第 i_j 行为 L_{ij}，其中 $1\leqslant j\leqslant k$。设 $L=L_{i1}\oplus L_{i2}\cdots\oplus L_{ik}$，那么 L 仍然是一个长度为 W 的二进制字符串。假设 $L=p_1p_2\cdots p_W$，其中 p_j $(1\leqslant j\leqslant W)$ 是 0 或者 1。经过有序的局部规则 $F_{p_1},F_{p2},\cdots,F_{pW}$ 作用后 Alice 得到了 R_C 的新的图像 $T_n(R_C)$。

(4)再经过 $T_n(R_C)$ 和 C 的异或操作，Alice 可以得到密图 $N=T_n(R_C)\oplus C$。

(5) Alice 将图像 (R_C,N) 发送给 Bob。

2.2　图像解密算法

(1) Bob 获取信息，将 R_C 经过有序的局部规则 $F_{p1},F_{p2},\cdots,F_{pW}$ 作用后，得到 $T_n(R_C)$。

(2)因为 $T_n(R_C)\oplus N=T_n(R_C)\oplus(T_n(R_C)\oplus C)=C$，所以 Bob 可以得到压缩图 C。

(3) Bob 利用基于细胞自动机变换的解码方案将压缩图恢复成原图 M。

3　光学加密系统及计算机模拟

3.1　光学系统结构简图

细胞自动机的计算体系目前是光学实现中最有前途的体系之一，这主要是因为它具有符合光学实践中的简单且鲁棒的结构，充分利用了固有的高度并行性和互联性。通过采用不同的方法来执行逻辑运算和互联，产生了许多光学细胞自动机实现体系[20-22]。使用这些方法和构造，很容易利用光学装置来实现基于有序细胞自动机的加密算法。

基于有序细胞自动机的图象加密方案的光学实现简单原理图如图 1 所示。

图中 I 和 II 两部分中的核心元件是空间光调制器(SLM)，以用来显示细胞的状态。对于实现

细胞阵列移位、叠加等操作可以用很多方法实现，如可采用可编程的 1/4 波带片来实现或计算机生成的不同散射命令控制强度的全息图来实现等。然后，通过分光器进化细胞自动机下一时刻的状态。I 和 II 两部分分别得到算法中的 C 和 $T_n(R_C)$，再通过分光镜进行异或操作，有关光探测器门限强度等选取的讨论可参见文献[20-22]。

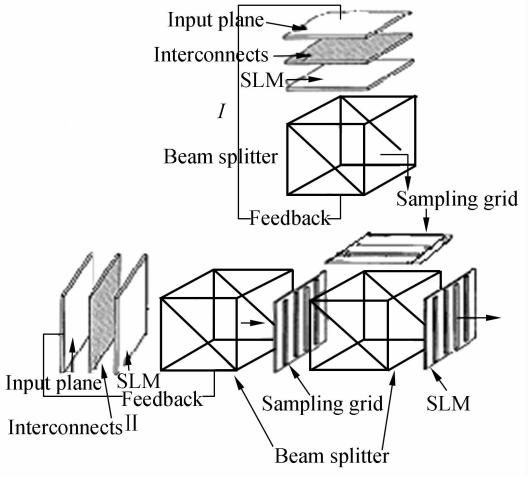


图 1　基于有序细胞自动机图像加密方案的光学实现原理图

Fig. 1　Block-scheme of optical image encryption scheme based on sequential CA

3.2　计算机模拟

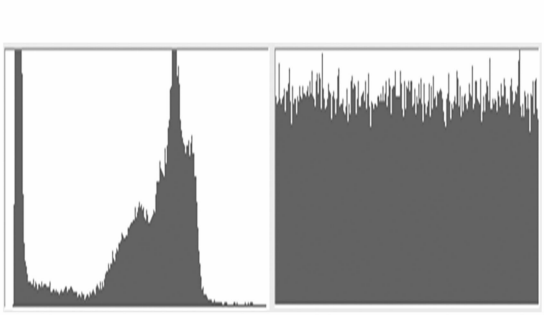
取一张 128×128 的 Lena 图像，选择一个 1-邻域的局部规则 $f=(06\ DB8\ 3CA)^{16}$ 和一个 2-邻域的局部规则 $g=(E\ 2A8\ 7F5\ 3C0\ 46B\ D19)^{524\,288}$。基于细胞自动机变换的压缩编码仍采用文献[18]中的 8-β 类二维 A_{ijkl} 基函数。实验结果如图 2 所示，图 2 的左边是原始图像 M，右边是压缩加密算法加密的结果 N。图 3 中对应地给出了 M 和 N 的直方图。密图 N 上均匀分布的像素说明被加密的图像的统计特征已经明显改变了。可见，加密图像的灰色区域具有很好的平衡性，说明了有序细胞自动机的加密算法满足了混淆特性，并可有力地抵抗已知明文攻击。

为了考察原始随机图像 R_C 和新的随机图像 $T_n(R_C)$ 之间的相关性，通过求两个图之间的相关系数来验证。利用实验中选择的规则，一共做了 8 次实验，每次产生一个原始随机图像 R_C，然后经过有序 CA 变换后得到的相应新的随机图像

(M)　　(N)

图 2　原始图片 M 和密图 N

Fig. 2　Original image M and secret image N



(M)　　(N)

图 3　原始图片 M 和密图 N 的直方图

Fig. 3　Histograms of image M and image N

$T_n(R_C)$，计算两者的相关系数 ρ，结果如表 1。

表 1　两随机图像之间的相关系数

Tab. 1　Correlation coefficients of two random images

No.	1	2	3	4
ρ	0.001 3	−0.002 1	0.001 1	0.003 5
No.	5	6	7	8
ρ	−0.002 4	−0.003 2	−0.005 0	0.004 6

可以看出，大多数情况下，两个图像的相关系数的绝对值都＜0.005，并且在所有实验的结果中，没有任何一次相关系数的绝对值＜0.01，从而说明两个图像之间的相关性非常弱。

4　结　论

如果用 3-邻域来代替 2-邻域，那么局部规则的集合将包含 $2^{2^{49}}=2^{562\,949\,953\,421\,312}$ 个元素。3-邻域的局部规则比 2-邻域的局部规则具有更强的雪崩效应。但是存储 2-邻域的局部规则只需要

不到 4 M(33 554 432 bit)的空间，而 3-邻域的局部规则要存储起来需要 65 536 G 的空间，所以，从可行性的角度来考虑，2-邻域是一个最佳选择，仅需要($H+4M+512$) B 的空间来存储有序的局部规则。对于窃听者必须要在$\{1,2,\cdots,H\}$的所有子集中寻找所有可能的 2^{512} 个 1-邻域局部规则和所有可能的 $2^{33\,554\,432}$ 个 2-邻域局部规则。因为 CAT 压缩编码还具有一定的密钥量[18]，因此本文所提出的这个加密方案的密钥量至少为 $2^H\times 2^{512}\times 2^{33\,554\,432}$。这个密钥量不仅远远大于文献[16]中所采用的改进的细胞自动机的密钥量 $10^{9\,536}$，而且还大于文献[8-10]中所采用的二维混沌映射的密钥量 1.84×10^{19} 及合成的离散混沌系统的密钥量 10^{32} 和基于 3-D Lorenz 系统的混沌图像加密算法的密钥量 2^{158}。综上，该方案是一种密钥量大、高效率和具有发展潜力的图像加密算法，而且该方案适合用光学元件实现，可有效应用于光学图像加密。

参考文献：

[1] 田岩，柳健，田金文. 一种光学图像的快速超分辨率重建方法[J]. 红外与毫米波学报，2004，23(3)：237-240.
TIAN Y，LIU J，TIAN J W. Fast super resolution method applied to optical image[J]. *Infrared Millim. Waves*，2004，23(3)：237-240. (in Chinese)

[2] WANG ZH，JIA SH H，ZHANG X H，*et al*.. Multiframe postprocessing algorithm of laser active imaging images [J]. *Opt. Precision Eng.*，2007，15(4)：615-621.

[3] 王玉荣，王青圃，徐鹏，等. 用两次曝光相移全息干涉实现光学幅相转换[J]. 光电子·激光，2005，16(7)：858-861.
WANG Y R，WANG Q P，XU P，*et al*.. Optical amplitude-phase conversion by using double-exposure phase-shifting holographic interferometry[J]. *Journal of Optoelectronics·Laser*，2005，16(7)：858-861. (in Chinese)

[4] GUO Y，HUANG Q，DU J，*et al*.. Decomposition storage of information based on computer-generated hologram interference and its application in optical image encryption[J]. *Applied Optics*，2001，40(17)：2860-2863.

[5] HENNELLY B，SHERIDAN J T. Optical image encryption by random shifting in fractional fourier domains[J]. *Opt. Lett.*，2003，28(4)：269-271.

[6] LI Y，KRESKE K，ROSEN J. Security and encryption optical systems based on a correlator with significant output images[J]. *Appl. Opt.*，2000，39(29)：5295-5301.

[7] 丁文霞，卢焕章，谢剑斌. 混沌二值序列对异或运算构成群的理论和实验证明[J]. 系统工程与电子技术，2006，28(9)：1420-1422.
DING W X，LU H ZH，XIE J B. Theoretical and experimental proof that chaotic binary sequences are groups about XOR operation[J]. *Systems Engineering and Electronics*，2006，28(9)：1420-1422. (in Chinese)

[8] 杨华千，张伟，韦鹏程，等. 一种基于复合离散混沌系统的对称图像加密算法[J]. 计算机科学，2006，33 (12)：86-91.
YANG H Q，ZHANG W，WEI P CH，*et al*.. A symmetric image encryption scheme based on composite discrete chaotic system[J]. *Computer Science*，2006，33 (12)：86-91. (in Chinese)

[9] FU C，ZHANG Z，CAO Y. An improved image encryption algorithm based on chaotic maps[C]. *Natural Computation，ICNC* 2007，*Third International Conference*，2007，3：189-193.

[10] 黄峰，冯勇. 利用图像分割思想的二维混沌映射及图像加密算法[J]. 光学 精密工程，2007，15(7)：1096-1103.
HUANG F，FENG Y. Novel 2D chaotic map based on image segmentation and image encryption approach[J]. *Opt. Precision Eng.*，2007，15(7)：1096-1103. (in Chinese)

[11] WOLFRAM S. Cryptography with cellular automata[C]. *Advances in cryptology-CRYPTO* 85，*Lecture Notes in Computer Science*，1985，218：429-432.

[12] NANDY S，KAR B K，CHAUDHURI P P. Theory and applications of cellular automata in cryptography[J]. *IEEE Trans. Comput.*，1994，43(12)：1346-1356.

[13] MADJAROVA M，KAKUTA M，YAMAGUCHI M，*et al*.. Optical implementation of the stream cipher based on the irreversible cellular automata algorithm[J]. *Optical Letters*，1997，22 (21)：1624-1626.

[14] 梁士利,张占新,郭景富,等. 基于混合加法CA的光学流密码系统[J]. 光电子·激光, 2003, 15(4):615-621.
LIANG SH L, ZHANG ZH X, GUO J F, *et al*.. Optical system of the stream cipher based on the hybrid additive cellular automata[J]. *Journal of Optoelectronics · Laser*, 2003, 14(5):615-621. (in Chinese)

[15] 梁士利,张玲,王广,等. 一维加法CA的同步系统研究[J]. 光学 精密工程,2006,14(3):495-497.
LIANG SH L, ZHANG L, WANG G, *et al*.. Study on synchronization of 1D-k3 additive cellular automata[J]. *Opt. Precision Eng.*,2006,14(3):495-497. (in Chinese)

[16] CHEN R, LU W, LAI J. Image encryption using progressive cellular automata substitution and SCAN[C]. *Circuits and Systems, ISCAS 2005. IEEE International Symposium*, 2005,2:1690-1693.

[17] CHAUDHURI P P, CHAUDHURI D R, CHAUDHURI D R, *et al*.. *Additive Cellular Automata: Theory and Applications*[M]. New York: IEEE Press, 1997.

[18] OLU L. Data compression and encryption using cellular automata transforms[J]. *Engng. Applic. Artif. Intell.*, 1997, 10(6):581-591.

[19] SHAPIRO J M. Embedded image coding using zerotrees of wavelet coefficients[J]. *IEEE Trans. on Signal Processing, Special Issue on Wavelets and Signal Processing*, 1993,41:3445-3463.

[20] YATAGAI T. Cellular logic architectures for optical computers[J]. *Appl. Opt.*, 1986, 25(10): 1571-1577.

[21] TABOURY J, WANG J M, PIERRE C, *et al*.. Optical cellular processor architecture. 1:principles[J]. *Applied Optics*, 1988, 27(9): 1643-1650.

[22] TABOURY J, WANG J M, PIERRE C, *et al*.. Optical cellular processor architecture. 2:illustration and system considerations[J]. *Appl. Opt.*, 1988, 28: 3138-3147.

作者简介:张晓岩(1978—),男,讲师,博士后,主要从事图论优化与信息安全、图像处理等方面的研究。E-mail: royxyzhang@yahoo.cn

●下期预告

基于电子倍增CCD噪声特性的最佳工作模式研究

张闻文,陈　钱
(南京理工大学 电子工程与光电技术学院,江苏 南京 210094)

对电子倍增CCD的噪声特性进行了研究,在此基础上选择最佳工作模式。首先,介绍了反转和非反转模式的工作原理,分析了不同工作模式下暗电流与时钟感生电荷的表现并进行了对比。接着,以工作温度、积分时间和垂直转移次数为参量,建立了最佳工作模式的数学模型。然后,求解出最佳工作模式的积分临界点,确定了电子倍增CCD的最佳工作模式。最后,结合具体器件参数模拟了最佳工作模式下电子倍增CCD的噪声特性曲线。仿真结果表明:室温下(293 K),积分临界点为1.6 μs。当积分时间大于1.6 μs时,最佳工作模式为反转模式;当积分时间小于1.6 μs时,最佳工作模式为非反转模式。研究结果为电子倍增CCD工作模式的选取提供了切实可靠的理论依据。