基于 2 维元胞自动机的图像置乱和水印技术

李辉亮 叶瑞松
(汕头大学数学系,汕头 515063)

摘 要 为了对图像进行鲁棒的加密,在对一些规则号的 2 维元胞自动机进行混沌性质简单分析的基础上,计算了 2 维元胞自动机的分形维数,并将其运用到图像的加密和图像水印技术中。攻击实验证明了元胞自动机的混沌性质在图像加密和水印技术上的应用有较好的鲁棒性。

关键词 元胞自动机 混沌 图像加密 水印技术
中图法分类号:TP309 **文献标识码**:A **文章编号**:1006-8961(2008)11-2076-05

Image Scrambling and Watermarking Technique Based on 2D Cellular Automata

LI Hui-liang, YE Rui-song
(*Department of Mathematics, Shantou University, Shantou* 516063)

Abstract The chaotic characteristics of Cellular Automata are analyzed simply and the definition of fractal dimension is constructed. Cellular Automata are applied to image encryption and image watermarking technique. The attacking examinations show that the characteristics of Cellular Automata are rather well in the application field of images.

Keywords cellular automata, chaos, image encryption, watermarking technique

1 引 言

元胞自动机(cellular automata)是一种自然界中的复杂系统的完全离散化的数学模型。该系统是一个时间、空间和状态变量取值均是离散的动力系统。元胞自动机刻画了具有大量离散自由度的动力系统,其结构简单,但行为却异常复杂。元胞自动机最早是由现代计算机之父——冯·诺伊曼(Von Neumann)等人提出的构想[1],用于模拟生物的自复制过程。1970 年,Conway 等人提出了著名的"生命游戏"(game of life)模型,引起了一时的轰动。生命游戏是一种单人玩的计算机游戏[2]。它与现代的围棋游戏在某些特征上略有相似:围棋中有黑白两种棋子,黑白两子在空间的分布决定了双方的死活。而生命游戏中的元胞也有{"生","死"}两个状态{0, 1},只不过规则更为简单。目前元胞自动机已成为一个应用广泛的研究领域。其在图像处理、加密、压缩、计算机模拟仿真等方面都有广泛的应用[3~5]。分形学的产生,给人们研究元胞自动机的内在混沌性质提供了方便。分形维数的计算可以描绘系统的混沌性,其中包括 Hausdorff 维、分形维、盒维等,本文给出了 2 维元胞自动机的盒维计算方法,同时根据维数对 2 维元胞自动机进行了分类,并将其进一步应用到图像的置乱与水印处理。

随着多媒体技术和网络技术的迅速发展,越来越多的数字图像和影像作品在网络上传输,如何保证信息的安全传输、存储已成为目前面临的重大问

基金项目:国家自然科学基金数学天元基金项目(A0324649)
收稿日期:2006-11-20;**改回日期**:2007-05-08
第一作者简介:李辉亮(1980~),男。现为汕头大学数学系硕士研究生。主要从事分形混沌在图像处理中的应用。E-mail: g_hlli@stu.edu.cn;
通讯作者:叶瑞松(1968~),男。博士,教授。主要研究方向为分叉理论及其数值计算、分形混沌及其计算机应用、图像加密和水印等。E-mail:rsye@stu.edu.cn

题。信息隐藏加密、水印技术是解决此类问题的一个重要,且很活跃的研究领域。在数字信息加密隐藏、数字图像水印技术中,置乱作为一种数字信息的预处理和后处理技术,在这些方面有着广泛的应用。置乱的目的是将有意义的可读信息变换成杂乱无章的信息,以便实现信息的加密或隐藏。目前已经有了很多种有效的方法,基本上可以分为以下 3 大类:第 1 类是通过改变图像像素的位置来达到置乱的目的;第 2 类是通过改变图像像素的灰度值来达到置乱的目的;第 3 类是同时兼有第 1、第 2 类方法的特点[6~10]。文献[9]提出了一种基于生命游戏的数字图像置乱与数字水印技术,它成功地将规则号 $C=224$ 的 2 维元胞自动机应用到图像置乱和水印嵌入中。本文将对几个 2 维元胞自动机进行混沌性质的简单分析,同时计算 2 维元胞自动机的分形维数,并利用 2 维元胞自动机的混沌性质来对数字图像进行置乱加密和数字水印嵌入。攻击实验证明了元胞自动机的混沌性质在图像加密和水印技术上的应用有较好的鲁棒性。

2　2 维元胞自动机和分形盒维

元胞自动机是空间、时间和状态的取值都是离散的动力系统,也是离散动力系统研究领域的一个极端代表。元胞自动机的空间是由一系列格栅状分布的元胞构成的,可以是 1 维、2 维或者更高维(n 维)的,其可用欧氏空间的整数格点 $\mathbf{Z}^n$($\mathbf{Z}$ 为自然数集合)来表示;除此之外,元胞自动机还包括元胞状态集 $\boldsymbol{S}=\{0,1,\cdots,k-1\}$、元胞邻域 $\boldsymbol{N}$、局部规则 $f:\boldsymbol{S}^N\to\boldsymbol{S}$、构形集 $\boldsymbol{A}$ 和全局映射 $G_f:\boldsymbol{A}\to\boldsymbol{A}$。元胞自动机的动态过程由局部的规则号来确定,而局部规则则确定了元胞的当前状态映射到下一时刻的状态值的更新规则。设一个 2 维元胞自动机的状态集为 2 态,邻域 $\boldsymbol{N}$ 为 Moore 邻域,其由围绕 $\boldsymbol{N}$ 的周围 8 个元胞和它本身一共 9 个元胞构成,即

$$\boldsymbol{N}_{i,j}=\{S_{i-1,j-1},S_{i-1,j},S_{i-1,j+1},S_{i,j-1},S_{i,j},S_{i,j+1},S_{i+1,j-1},S_{i+1,j},S_{i+1,j+1}\}$$

局部规则为外全加规则,即规则号与元胞 $S_{i,j}$ 周围的 8 个元胞的状态值的和有关:

$$S_{i,j}^{(t+1)}=f(S_{i,j},S_{i-1,j-1}+S_{i-1,j}+S_{i-1,j+1}+S_{i,j-1}+S_{i,j+1}+S_{i+1,j-1}+S_{i+1,j}+S_{i+1,j+1})$$

与不同的映射规则对应的不同的规则编号为

$$C=\sum_{m=0}^{1}\sum_{n=0}^{8}f(m,n)2^{2n+m}\tag{1}$$

式中,m 有两种取法,n 可以是 0 ~ 8 的 9 个数中的一个,有 9 种取法。根据它们的组合方式,共有 $2^{2\times9}=2^{18}=262\ 144$ 种不同的规则号。这给选取规则号进行图像处理实验提供了非常丰富的选取方法。本文选取具有混沌性质的那些 2 维元胞自动机作为图像置乱和水印的选择结果。如何判断与哪些规则号对应的 2 维元胞自动机具有混沌性,可选取其分形维数作为判断的根据。下面给出了 2 维元胞自动机盒维数的计算方法。

定义 1　设构形集 $\boldsymbol{A}$ 属于欧氏空间 $\mathbf{R}^2$,$\mathbf{R}^2$ 被边长为 $\frac{1}{2^n}$ 的方盒子所覆盖,记 $N_n(\boldsymbol{A})$ 表示覆盖图形的方盒子个数。则 $\boldsymbol{A}$ 的分形盒维数为

$$D=\lim_{n\to\infty}\frac{\ln N_n(\boldsymbol{A})}{\ln 2^n}\tag{2}$$

举一个例子,设 $\boldsymbol{A}$ 为 Sierpinski 三角形,则 $N_1(\boldsymbol{A})=3,\cdots,N_n(\boldsymbol{A})=3^n$(见图 1),Sierpinski 三角形的分形盒维数为

$$D=\lim_{n\to\infty}\frac{\ln N_n(\boldsymbol{A})}{\ln 2^n}=\frac{\ln 3^n}{\ln 2^n}=\frac{\ln 3}{\ln 2}$$

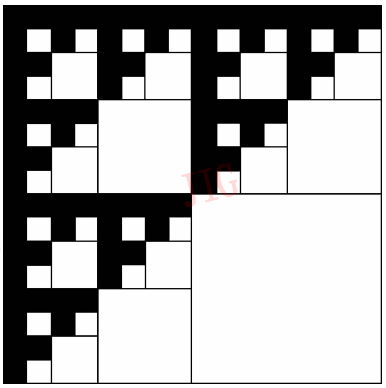


图 1　覆盖 Sierpinski 三角形的方盒子个数

Fig. 1　The box number covering the Sierpinski triangle

本文先把平面网格分割成 2^n 份,然后对 2 维元胞自动机的演化图进行计算处理。由于像素数量问题,n 不能取得太大,只能近似地求它的分形维数。例如 256 × 256 大小的演化图,可通过取 4 × 4 大小的小盒子去覆盖整个状态值为 1 的格点来求出所有的覆盖盒子数目 $N_n(\boldsymbol{A})$,代入式(2)即可求得它的近似分形维数。本文通过具体选取一些不同的规则号进行计算来得到表 1 的结果。

表 1 2 维元胞自动机演化图的分形盒维数

Tab. 1 The fractal box dimensions of the 2D CA evolving patterns

规则号 C	迭代 7 次	迭代 12 次	迭代 13 次	结构类型
261 100	1.99	2.0	2.0	均等态
8 189	1.998	1.26	1.998	波动稳定
4 093	1.997	1.305	1.997	波动稳定
816	1.84	1.842	1.843	混沌态
35 853	1.796	1.810	1.811	混沌态
534	1.78	1.831	1.799	混沌态

表 1 分别给出了不同类型的元胞自动机的近似分形盒维数,在利用规则号 $C=261\ 100$ 进行迭代后,演化图的元胞出现了全部元胞成活的状态;当采用 $C=8\ 189$ 时,则出现了两种极端状态来回波动的状态,即奇数次时刻为基本全部成活,偶数次时刻为基本死亡。而当采用 $C=816$, $C=35\ 853$ 等其他规则号时,则算得的数据大概出现在 1.7 到 1.9 之间,这样的情况说明元胞自动机的动力行为出现了混沌的性质。因此本文将元胞自动机的动力行为分为以下 3 大类:(1)演化到空间的均等态;(2)在空间趋向简单稳定或者周期性结构;(3)趋于混沌的非周期行为。其中第 3 类就是具有混沌性质的、能较好地被利用到图像加密和水印技术中去的一大类,并且属于这类的元胞自动机的不同规则号有不同的效果,下面将具体地应用该类元胞自动机来对数字图像进行置乱和水印的处理。

3 数字图像的置乱

随着数字图像的广泛应用、计算机技术的发展和网络传输速度的提高,让更多的音频视频文件能够迅速地传递,图像更是各式各样,有天文、地理等相关图像,也有些涉及到国家军事等安全问题的图像。这都需要用加密技术来保证信息在传送过程中不外泄。一般地,可采取置乱的方法来保证图像信息的安全性。而判断置乱图像的效果,则可以用置乱度来评价。

定义 2 设图像大小为 $M\times N$,用 $I(i,j)$ 表示图像 $\boldsymbol{I}$ 在 (i,j) 处像素点的灰度值,则该像素与其相邻像素的相邻灰度差为

$$d_{\text{gray}}(I(i,j))=\frac{\sum\left[I(i,j)-I(\hat{i},\hat{j})\right]^2}{4} \tag{3}$$

其中,$(\hat{i},\hat{j})=\{(i-1,j),(i+1,j),(i,j-1),(i,j+1)\}$。

式(3)表示图像中某像素点的灰度值与周围上下左右相邻的 4 个像素的平均灰度差。除了图像边缘上的像素点外,都可通过计算图像中其余各像素点与周围点的灰度差,然后进行相加平均来得到整个图像 $\boldsymbol{I}$ 的灰度差

$$\bar{d}_{\text{gray}}(\boldsymbol{I})=\frac{\sum_{i=2}^{M-1}\sum_{j=2}^{N-1}d_{\text{gray}}(I(i,j))}{(M-2)\times(N-2)}$$

因此,定义灰度差置乱度为[10]

$$D_{\text{gray}}(\boldsymbol{I},\hat{\boldsymbol{I}})=\frac{\bar{d}_{\text{gray}}(\hat{\boldsymbol{I}})-\bar{d}_{gray}(\boldsymbol{I})}{\bar{d}_{\text{gray}}(\hat{\boldsymbol{I}})+\bar{d}_{\text{gray}}(\boldsymbol{I})} \tag{4}$$

其中,$\bar{d}_{\text{gray}}(\boldsymbol{I})$,$\bar{d}_{\text{gray}}(\hat{\boldsymbol{I}})$ 分别表示置乱前后图像 $\boldsymbol{I}$、$\hat{\boldsymbol{I}}$ 的相邻像素的平均灰度差。D_{gray} 的取值范围为 $(-1,1)$。若它小于 0,则表示置乱后比置乱前的效果还差,若它大于 0,则表示置乱效果比原图好,而且越接近 1 越好。

本文把平面的网格点对应到二值图像的像素点去,首先取一个随机分布的 0,1 矩阵,设为初始矩阵 $\boldsymbol{A}_0$。具体置乱步骤如下:

(1)将 $\boldsymbol{A}_0$ 的状态值为 1 的点对应到要置乱图像 $\boldsymbol{I}$ 的像素点上去,并且按行顺序取出放到新建的图像像素矩阵 $\hat{\boldsymbol{I}}$ 中去;

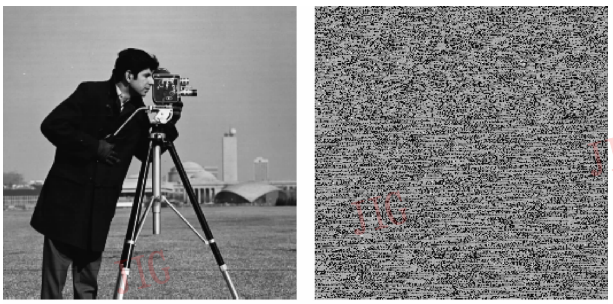
(2)用规则号 C 的映射函数 f 对 $\boldsymbol{A}_0$ 进行连续迭代 k 次来得出一序列 $\{\boldsymbol{A}_1,\boldsymbol{A}_2,\boldsymbol{A}_3,\cdots,\boldsymbol{A}_k\}$;

(3)取与 $\boldsymbol{A}_1$ 上状态值为 1,且 $\boldsymbol{A}_0$ 上相同位置的状态值不为 1 的点对应的图像 $\boldsymbol{I}$ 上的像素灰度值,并按顺序取出放到 $\hat{\boldsymbol{I}}$ 的后面去。

继续迭代到第 k 步,取出 $\boldsymbol{A}_k$ 状态值为 1 而在所有的 $\boldsymbol{A}_{k-1},\boldsymbol{A}_{k-2},\cdots,\boldsymbol{A}_0$ 的相同位置状态值全不为 1 的点所对应的图像 $\boldsymbol{I}$ 上的像素灰度值,依次放到 $\hat{\boldsymbol{I}}$ 中去。最后,将图像 $\boldsymbol{I}$ 中剩下的点也依次放到 $\hat{\boldsymbol{I}}$ 中去。这样所得到的 $\hat{\boldsymbol{I}}$ 就是进行置乱后的图像。解密用此算法的逆过程,需要用的密钥是随机生成的种子整数 E、迭代次数 k 和规则号 C。其丰富的密钥足够保证置乱的安全性。

现在具体选取几个规则号的元胞自动机来对图像进行置乱。取 $f(1,2)=1$,$f(0,3)=1$,$f(1,3)=1$,其他状态值为 0,代入式(1),可得规则号 $C=2^3+2^6+2^7=224$。对于初始随机种子数 E 为 100

产生的0,1 矩阵,迭代次数 k 为 2 次,其置乱后的图像如图 2(b)所示。同样地,取 $f(p,q)=1$,当 $q=2$ 或 4,且 $p=\{0,1\}$ 时,其他状态值为 0,则算得的规则号 $C=2^4+2^8+2^5+2^9=816$,其置乱后的图像见图 2(c)。取 $f(p,q)=1$,当 $q=2$ 或 5,$p=\{0,1\}$,而 $f(1,7)=1$,其他状态值为 0 时,则算得的规则号 $C=2^2+2^3+2^{10}+2^{11}+2^{15}=35\ 852$,其置乱后的图像如图 2(d)所示。由此可以看出,用元胞自动机算法不仅置乱的效果很好,而且运算速度快,每次加密过程只需要用映射函数迭代 2 到 3 次就能满足置乱的要求。



(a)原始图像　(b)C=224,D_{gray}= 0.892 6

(c) C=816,D_{gray}= 0.886 5　(d)C=35 852,D_{gray}= 0.888 4

图 2　原始图像和用不同规则号置乱后的图像

Fig. 2　The original image and the encrypted images

根据式(4)得到的规则号为 $C=224$ 的置乱度 $D_{gray}=0.892\ 6$ 和规则号为 $C=816$ 的置乱度 $D_{gray}=0.886\ 5$,以及规则号为 $C=35\ 852$ 的置乱度 $D_{gray}=0.888\ 4$,都远远大于 0,接近 1,且置乱效果都很好,在直观上也很容易看出。根据本文定义的算法的逆算法,只要输入正确的密钥,就可以还原图像。

4　2 维元胞自动机的水印算法

数字水印技术分为可见水印和不可见水印技术两类,一般隐藏图像水印信息的算法都是不可见水印算法。本文提出了一种 2 维元胞自动机的不可见水印算法,该算法步骤如下:

(1)在第 3 类元胞自动机的具有混沌性质的规则号中任意选取一个,根据上述的置乱方法,对原始图像 $\boldsymbol{I}$(大小为 $m_1\times n_1$)进行置乱,设得到置乱后的图像为 $\hat{\boldsymbol{I}}$。

(2)设水印图像为 $\boldsymbol{W}$(大小为 $m_2\times n_2$),在置乱后的图像 $\hat{\boldsymbol{I}}$ 的左上角建立一个与水印大小一致的矩阵区域,即

$$\tilde{\boldsymbol{I}}=\{\hat{I}(i,j)\mid 0<i\leqslant m_2,0<j\leqslant n_2\}$$

然后利用线性关系来建立新的加入水印后的图像块 $\bar{\boldsymbol{I}}_w=(1-t)\boldsymbol{W}+t\tilde{\boldsymbol{I}}$,$t\in(0,1)$。

(3)先把 $\bar{\boldsymbol{I}}_w$ 放回到图像中对应的左上角,再利用置乱的逆算法来恢复图像,即可得到一幅嵌入水印的图像 $\boldsymbol{F}$。

在步骤(2),必须把 t 的值取得恰当,t 过小会使图像出现花点和原图不一致;而 t 过大时,则又使水印的信息保留较少,难于提取水印,从而导致加入水印后的图像经受不起攻击。而为了保证图像的清晰性,一般地 t 值取 0.1 ~0.3 之间。按原算法的逆算法很容易得到水印提取算法,即将嵌有水印的图像 $\boldsymbol{F}$ 用同样的规则号和其他相同条件进行置乱,再用另一公式计算左上角的水印图像块:$\boldsymbol{W}=(\bar{\boldsymbol{I}}_w-t\tilde{\boldsymbol{I}})/(1-t)$,这样就可以把水印 $\boldsymbol{W}$ 提取出。图 3 左边为利用规则号为 816 号的元胞自动机算法嵌入水印后的图像,右边为提取出的水印图像。

图3　加入水印的图像(t=0.1)和原始水印图像

Fig. 3　The image embedded watermark and the original watermark image

5　攻击实验

为了检验算法的鲁棒性,还对利用规则号为 816 号的 2 维元胞自动机水印算法得到的图像进行了人为攻击实验。例如在图 4(a)中,对加入水印的图像大面积的切割,其恢复的水印结果较好;图

4(b)中,对图像进行加上不同灰度的污点,而且是大面积的涂抹,其恢复的水印还是得到令人满意的效果,恢复出的水印基本能辨认出“汕头大学”4 个字。在图 4(c)中,对嵌入水印的图像进行了覆盖攻击,覆盖面积接近整体面积的四分之一,其恢复的水印一样令人满意;图 4(d)中,对图像进行无规则切割,由于在嵌入水印的过程中运用了较好的置乱方法,水印的信息已经无规则地遍布在水印载体上,由各图右边的水印恢复结果也可以看出,算法具有较好鲁棒性。在图 4(e)和图 4(f)中,分别用品质因子为 50 和 80 对图像进行 JPEG 压缩。原图像大小是压缩后的图像大小的 8.16 倍和 4.78 倍,用本文算法提取出的水印依然清晰可见,这说明了算法的抗攻击能力是比较强的。

图 4 一些攻击实验的效果

Fig. 4 The attacking tests and their results

6 结 论

本文通过计算 2 维元胞自动机的分形盒维数,首先对它们的动力行为做了具体分类,并将具有混沌性质的一类元胞自动机应用到图像的置乱加密和图像水印嵌入。对规则号为 $C=224$, $C=816$, $C=358$ 5 的元胞自动机实现了图像置乱和图像水印,并分别计算了它们的置乱度。在原有的置乱基础上,进行了水印的嵌入和提取,并且对规则号为 $C=816$ 的水印图像进行了破坏攻击实验,实验取得了满意效果。

参考文献(References)

1 Neumann J V. Theory of Self Reproducing Automata [M]. Urbana, Illionois, USA: University of Illionois Press, 1966.

2 Gardner M. On cellular automata self-reproduction the garden of eden and the game “life” [J]. Scientific American, 1971, **224**(2): 112~117.

3 Hernandez Gonzalo, Herrmann Hans J. Cellular automata for elementary image enhancement [J]. Graphical Models and Image Processing, 1996, **58**(1): 82~89.

4 Veronique Terrier. Two-dimensional cellular automata and their neighborhoods [J]. Theoretical Computer Science, 2004, **312**: 203~222.

5 Lafe O. Data compression and encryption using cellular automata transforms [J]. Engineering Applications of Artificial Intelligence, 1997, **10**(6): 581~591.

6 Ding Wei, Qi Dong-xu. Digital image transformation and information hiding and disguising technology [J]. Chinese Journal of Computers, 1998, **21**(9): 839~843. [丁玮,齐东旭. 数字图像变换及信息隐藏与伪装技术[J]. 计算机学报,1998, **21**(9): 839~843.]

7 Wu Min-sheng, Wang Jie-sheng, Liu Shen-quan. Permutation transform of images [J]. Chinese Journal of Computers, 1998, **21**(6): 514~519. [吴旻升,王介生,刘慎权. 图象的排列变换[J],计算机学报,1998, **21**(6): 514~519.]

8 Li Nan, Shang Yan-hong, Zou Jian-cheng. An audio phase coding watermark method based on Fibonacci transformation [J]. Journal of North China University, 2005, **17**(3): 1~5. [李南,商艳红,邹建成. 基于 Fibonacci 变换的音频相位水印技术算法[J],北方工业大学学报, 2005, **17**(3): 1~5.]

9 Ding Wei, Yan Wei-qi, Qi Dong-xu. Digital image scrambling and digital watermarking technology based on Conway's game [J]. Journal of North China University, 2000, **12**(1): 1~5. [丁玮,闫伟齐,齐东旭. 基于生命游戏的数字图像置乱与数字水印技术[J],北方工业大学学报, 2000, **12**(1): 1~5.]

10 Xiang De-sheng, Xiong Yue-shan. Digital image scrambling based on Josephus traversing [J]. Computer Engineering and Applications, 2005, **41**(10): 44~46. [向德生,熊岳山. 基于约瑟夫遍历的数字图像置乱算法[J]. 计算机工程与应用, 2005, **41**(10): 44~46.]