

基于混沌与细胞自动机的数字水印模式

王丽娜^{1,3}, 杨景辉², 张焕国¹, 于戈²

(1. 武汉大学软件工程国家重点实验室, 湖北武汉 430072; 2. 东北大学计算机软件与理论研究所, 辽宁沈阳 110004;
3. 中国科学院自动化所模式识别国家重点实验室, 北京 100080)

摘要: 本文提出了基于混沌与细胞自动机的数字自动转化为灰度图像的方法. 数字作为密钥, 不同数字能产生不同的灰度图像, 其实现过程为数字作为种子, 使用混沌迭代产生随机序列, 然后转化成二值图像, 经细胞自动机处理, 再使用平滑过程, 这样就产生了灰度图像. 灰度图像作为嵌入宿主信号的数字水印模式, 该水印模式的能量集中在低频. 实验结果显示该水印模式有好的特性, 使用该水印模式的水印算法能抵抗一些常见的攻击.

关键词: 混沌; 细胞自动机; 数字水印模式; 数字水印

中图分类号: TN918.91 **文献标识码:** A **文章编号:** 0372-2112(2004)04-0580-03

Digital Watermarking Pattern Based on Chaos and Cellular Automata

WANG Li-na^{1,3}, YANG Jing-hui², ZHANG Huan-guo¹, YU Ge²

(1. State Key Laboratory of Software Engineering, Wuhan University, Wuhan, Hubei 430072, China;
2. School of Information Science and Engineering, Northeastern University, Shenyang, Liaoning 110004, China;
3. National Laboratory of Pattern Recognition, Chinese Academy of Science, Beijing 100080, China)

Abstract: In this paper, an algorithm which automatically transforms number to gray-image using the number as key is proposed, distinct number leading to distinct gray-image. Its implementation is that random sequence is made by chaotic iterations using number as seed, then the sequence is transformed to two-value image. By cellular automata processing and after smoothing operation the gray-image is generated. The gray-image is regarded as a digital watermarking pattern and the pattern has most of its power concentrated in low frequencies. The watermarking is embed into original image in spatial apace, and it is detected by using DCT. The experiment results show that the pattern has good property. The watermarking algorithm based on the pattern can resist some usual attacks.

Key words: chaos; cellular automata; digital watermarking pattern; digital watermarking

1 引言

近年来提出的向数字作品加入不易察觉但可以鉴别版权的版权标记技术是一种有效的技术手段, 我们称之为数字水印^[1], 数字水印技术能保护所有的数字作品, 包括音频、视频、图形、图像、文本和软件等. 文献[1]提出的一种方法, 将 m 序列的伪随机信号编码形式作为水印的模式, 然后嵌入到 LSB (Least Significant Bit). 最简单的方法通过一个密钥来初始化一个伪随机数发生器, 这个伪随机数发生器将产生嵌入宿主信号的位置, 并在此基础上改进的一些方法^[2], 文献[3]提出了同时取 1 和 -1 二个值作为数字水印的模式, 对选择的像素对进行修改. 同时有很多的水印方法提到用二进制编码(取值为 0 和 1)作为水印的模式. 文献[4]提出了把二值水印经混沌置乱之后作为水印模式. 本文讨论基于混沌与细胞自动机的数字自动转化为灰度图像的方法, 以此灰度图像作为数字水印模式, 该数字水印模式有比较好的健壮性, 能抵抗一些常见的攻击.

2 基于混沌与细胞自动机数字转化为灰度图像

2.1 混沌产生随机序列

混沌区的数据有两个特性: 迭代不重复性和初值敏感性. 当选定适当系数使方程进入混沌状态时, 方程将进行无限不循环迭代, 因此不会出现重复的迭代值. 任何人如果得不到其初值 x_0 都无法预测下一个迭代值, 这种迭代的结果可以用来产生随机序列^[5].

对于一维映射: $X_{n+1} = f(X_n; \mu_i)$

由初始条件敏感性可知, 当初始条件 x_0 稍微出现一些偏差 δx_0 , 则经过 n 次迭代后, 结果就会呈指数分离.

混沌产生随机序列采用了混合光学双稳模型作为混沌源, 它是能生成奇妙吸引子的函数. 下面的方程为混合光学双稳模型的迭代方程:

$$X_{n+1} = A \sin^2(X_n - X_B)$$

A 和 X_B 是方程的系数, 随着参数 A , X_B 的变化, 系统将 from

收稿日期: 2002-08-05; 修回日期: 2004-01-15

基金项目: 国家自然科学基金重大研究计划项目(No. 90104005); 国家自然科学基金(No. 60173051); 教育部高等学校优秀青年教师教学和科研奖励基金

定点失稳,经周期分岔进入混沌.这里取 $A = 4, X_B = 2.5$,此时方程处于混沌状态.给定该方程的初值 X_0 ,进行迭代运算,判断迭代值 X_i 的大小,当 $X_i > (2.5) * A/3$ 时取 1,否则取 0.图 1 是选择三个不同的初值(种子)产生的随机序列,然后转变成 128×128 的矩阵.

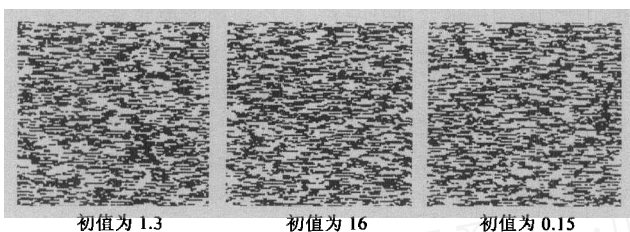


图 1 混沌产生随机序列(转化成 128×128 矩阵)的随机模式

2.2 基于投票规则的细胞自动机

细胞自动机 (Cellular Automata)^[6,7] 是能和其他细胞 (automata/cell) 相互作用具有相同的可计算功能的细胞的数组.这个数组可以是一维的串 (String), 二维的格子 (Grid), 三维的立体 (Solid). 大部分细胞自动机被设计为简单的方形的格子 (Rectangular Grid), 也有一些设计成蜂窝状. 描述细胞自动机必要的特征包括: 状态 (State)、邻居关系 (Neighbourhood) 和规则 (Rules).

基于投票规则的细胞自动机^[8] 设计为: 状态: 0 或 1; 邻居关系: 以自己为中心的 3×3 邻居; 规则: 计算以自己为中心 3×3 邻居(包括中心)1 的个数 P , 如果 $P < 5$, 中心的状态为 0, 否则状态为 1.

图 1 中三个不同初值得到的随机模式经过基于投票规则的细胞自动机四次处理后得到的模式如图 2 所示.

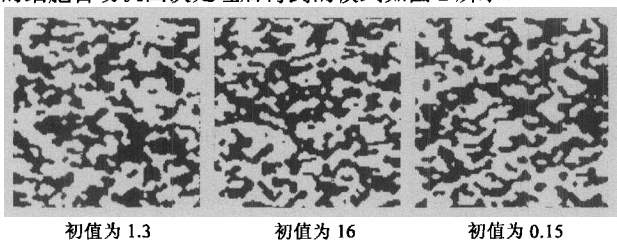


图 2 经过四次细胞自动机处理后得到的模式

从处理以后的结果可以看出, 给定一个初值(种子)使用混沌迭代产生的随机序列经过细胞自动机处理以后得到的模式具有“初值敏感性”, 不同的初值产生的模式完全不一样, 利用这一点具有单向 Hash 函数的作用.

2.3 灰度图像产生过程

在这里, 我们利用 7×7 的均值滤波器来平滑 (Smoothing) 经过细胞自动机处理后的模式. 图 2 的三个模式经过平滑八次处理得到图 4 的图像, 如图 4 所示.

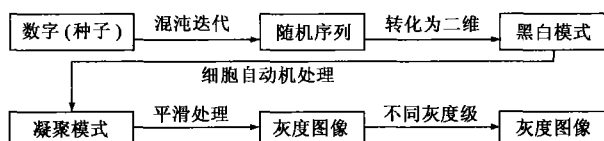


图 3 数字自动转化灰度图像的过程

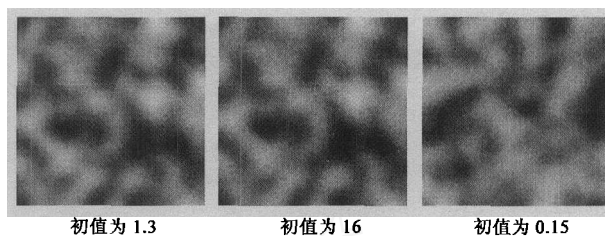


图 4 平滑 8 次的结果

经过以上处理的灰度图像(水印模式), 同时兼顾初值敏感性和不可逆性, 也即不能通过水印模式来计算出初始种子的值, 提高了整个水印系统的安全性.

图 3 可以很直观地看出, 数字作为混沌迭代的初值, 产生随机序列, 然后转化为二维矩阵, 经过细胞自动机处理, 平滑以后得到灰度图像. 应用细胞自动机有以下优点: (1) 得到视觉感知变化平滑的水印模式; (2) 细胞自动机运算具有不可逆性, 提高了安全性; (3) 水印模式的产生过程中, 得到凝聚模式, 为后续步骤产生条件.

如果图像比较小, 细胞自动机和平滑处理的运算都是简单的关系运算和加减运算, 运算速度很快, 没有大的运算量. 如果图像很大, 可以通过相应的频域处理, 运算量也很小, 整个生成水印模式的过程能很快的完成, 加之我们的嵌入算法是在空域下直接进行, 相比一些在频域下嵌入水印的算法快得多. 因此不会增加算法的复杂性.

经过以上处理, 种子不一样, 所得的灰度图像完全不一样. 我们知道, 根据混沌的特性初值敏感性, 每个初值所产生的随机序列不同, 细胞自动机处理以后不同的种子所产生的黑白图像也不同, 而且以上两步都是不可逆的, 我们可以认为最后得到的灰度图像对初值是敏感的, 具有不可逆性, 有密码学当中的一些安全特性, 类似密码学当中的 Hash 函数. 并且该灰度图像的大部分能量集中在低频.

3 水印嵌入及实验结果讨论

细胞自动机和平滑处理之后产生的水印模式的能量主要集中在低频, 嵌入过程在空域下, 也即直接对空域进行迭加, 根据信号变换的性质, 空域上的迭加和频域迭加是对应的, 在低频中嵌入水印, 即在感觉重要的成分嵌入水印, 有利于提高抗攻击能力.

我们使用文献[10]介绍的嵌入算法时, 把得到的灰度图像灰度级降到 16, 把每个像素的灰度值减去 8, 然后在空域下加到要嵌入水印的原图像, 这样对没有加入水印图像每个像素的修改不超过 ± 8 个灰度级. 在空域下嵌入该水印模式, 嵌入以后的图像与原图像视觉感觉差别很小.

水印检测算法通过计算相关系数决定是否有水印的存在. 实验采用频域下求相关系数, 频域求相关系数比在空域性能更好. 设没有嵌入水印的原图像用 I 表示, 嵌入水印的图像用 I' 表示, 嵌入水印并遭到修改的图像用 I^* 表示, 下面的函数用来计算相关系数:

$$sim(I^*, I') = \frac{D^* \cdot D}{\sqrt{D^* \cdot D^*} \sqrt{D \cdot D}},$$

$$D = X' - X, D^* = X^* - X$$

X, X', X^* 分别对应 I, I', I^* 的最低 1024 离散余弦变换 (DCT) 系数. 从检测的角度来看, 检测过程只取相应的图像的最低 1024 个离散余弦变换 (DCT) 系数

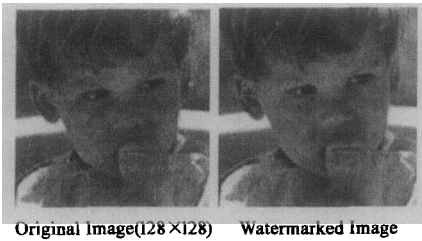


图 5 嵌入初值为 3.4 水印模式

值, 用于检测水印的标志空间的维数大大地减少了, 与直接使用混沌迭代序列直接作为水印模式然后检测几乎没有检测上的区别.

(1) 抵抗 JPEG 压缩检测

表 1 给出经过 JPEG 压缩后检测的相关系数

表 1 JPEG 压缩相关系数表

Quality	80%	50%	40%	30%	20%	10%
Sim	0.9692	0.8259	0.7999	0.7643	0.6842	0.4778

通过实验显示, 不同水印嵌入不同图像, 检测到的相关系数不超过 0.3, 因此判断是否嵌有该水印的阈值为 0.3. 表 1 显示, 压缩到 10% 都能很好的检测到水印的存在.

(2) 抵抗中值滤波检测

中值滤波: 采用 Stirmark 软件, 分别进行 $2 \times 2, 3 \times 3, 4 \times 4$ 中值滤波.

(3) 抵抗 Cropping 检测

Cropping: 嵌入水印以后的图像被删除 20%, 50% 的边界来剪切图像 (Stirmark), 删除的部分被原图像相应的部分补上, 然后再检测相关系数, 相关系数如下面表 3 所示.

表 2 “中值滤波”相关系数表

Median filter	2×2	3×3	4×4
Sim	0.3570	0.2296	0.1450

表 3 “剪切图像”相关系数表

Cropping	20%	50%
Sim	0.7889	0.5074

(4) 抵抗信号增强检测

信号增强: 采用 Stirmark 软件, 分别进行频域拉普拉斯去除 (FMLR)、高斯滤波和采用 Paintshop 7.04 软件 Sharp 和 Sharpmore 项进行操作.

表 4 “信号增强”相关系数表

信号增强	FMLR	Gaussian	Sharp	Sharpmore
Sim	0.5067	0.3745	0.8242	0.4967

(5) 峰值信噪比 (PSNR)

测试以图 5 的图像为例, 得到一组峰值信噪比见表 5.

表 5 不同的初值 X_0 所对应的峰值信噪比

初值 X_0	3.4	1.2	18	0.5	32	2.4
PSNR	46.95737	40.9669	42.4782	42.2801	42.2728	46.7694

实验结果显示本文讨论的水印模式能抵抗 JPEG 压缩、剪切、一些滤波和一些信号处理.

4 结论

本文重点讨论了基于混沌与细胞自动机的数字转化为灰

度图像的方法, 并以该灰度图像作为数字水印模式. 该水印模式的特点是最后得到的灰度图像对初值是敏感的, 具有不可逆性, 有密码学中的一些安全特性, 类似密码学当中的 Hash 函数. 同时, 该水印生成形式的大部分能量集中在低频.

本文不足之处是没有讨论分析数据有效载荷. 未来的工作应该对该水印模式进行分析, 讨论使用该模式算法的数据有效载荷. 研究在该水印生成形式基础上的盲检测水印算法. 下一步我们将确定目标, 使用优化算法优化产生混沌序列的一个参数及细胞自动机处理次数等参数, 在水印模式产生过程中根据被嵌入对象的特点得到性能更好的水印模式. 对产生的灰度图像进行分析, 使水印信息调制于灰度图像中, 结合密钥控制的优点, 发展健壮的盲检测水印算法.

参考文献:

- [1] Schyndel R G, Tirkel A Z, Osborne C F, A Digital Watermark [A]. Proc of IEEE Int Conf Image Processing [C], Austin Texas, USA, 1994, II, 86-90.
- [2] Stefan Katzenbeisser, Fabien A P Petitcolas, 吴秋新, 等译. Information Hiding Techniques for Steganography and Digital Watermarking [M]. 北京: 人民邮电出版社, 2001. 35-36.
- [3] Bender W, Gruhl D, Morimoto N, Techniques for Data Hiding [A]. Proceeding of the SPIE, Storage and Retrieval for Image and Video Database III [C]. San Jose, Feb, 1995, 2420, 164-173.
- [4] 张军, 王能超, 施保昌. 基于混沌映射和遗传算法的公开数字水印技术 [J]. 模式识别与人工智能, 2002, 15(1): 42-47.
- [5] 王丽娜. 基于混沌特性改进的小波数字水印算法 [J]. 电子学报, 2001, 29(10): 1424-1426.
- [6] David G Green. Cellular Automata [OL]. <http://life.csu.edu.au/complex/tutorials/tutorial1.html>.
- [7] Rucker R, John W [OL]. <http://www.ifs.tuwien.ac.at/~aschatt/info/ca/ca.html>.
- [8] Alexander S. Cellular Automata [OL]. <http://www.fourmilab.ch/cellab/>.
- [9] Jiri Fridrich, etc, Secure Encryption and Hiding of Intelligence Data, AFRL-IF-RS-TR, Mission Research Corporation, Final Technical Report [OL]. 1998, 9. at <http://www.rl.af.mil/programs/shid/>

作者简介:



王丽娜 女, 1964 年 10 月生于辽宁省营口市, 博士, 现为武汉大学计算机学院教授, 主要研究领域为计算机网络安全, 信息隐藏与数字水印, 发表论文 30 余篇, 编著 3 部. E-mail: lnawang@163.com.

杨景辉 男, 1980 年 10 月生于江西省临川市, 东北大学软件与理论专业在读硕士研究生, 主要研究方向为多媒体信息的安全与保护技术. E-mail: Jinghuiyang@hotmail.com.

张焕国 男, 1945 年 6 月生于河北省, 现为武汉大学计算机学院教授, 博士生导师, 主要研究领域为密码学与信息安全理论与技术.