基于混沌序列的数字水印信号研究

纪 震,李慧慧,肖薇薇,张基宏
(深圳大学信息工程学院,广东深圳 518060)

摘 要: 本文针对当前数字水印算法中提出的各种数字水印信号进行分析,综合了数字水印信号应满足的特性,并且提出了基于混沌序列的数字水印信号算法. 与目前存在的数字水印信号相比,混沌数字水印信号具有三方面的优点:易于产生,仅需采用一维混沌映射方程,水印信号生成速度快;数量众多,混沌系统模型、参数和初值的选择不同即可得到互不相关的两序列;保密性好,在不知道混沌模型及相关参数的前提下,几乎不可能破译. 因此可以有效地解决实际应用中大量数字水印产生的问题及数字水印标准化问题,有利于数字水印技术走向实际应用.

关键词: 数字水印; 混沌; 扩频; 水印信号; 水印标准化
中图分类号: TP391.41 **文献标识码**: A **文章编号**: 0372-2112 (2004) 07-1131-04

The Research of Digital Watermark Signal Based on Chaotic Sequences

JI Zhen, LI Hui-hui, XIAO Wei-wei, ZHANG Ji-hong
(Faculty of Information Engineering, Shenzhen University, Shenzhen, Guangdong 518060, China)

Abstract: Various digital watermark signals involved in digital watermarking algorithms are discussed and the requisite characteristics of a watermark signal are summarized. The chaotic watermark signal based on chaotic sequences is proposed. This chaotic watermark signal has some promising characteristics in comparison with other watermark signals. Firstly, it is easy to be created by using 1-D chaotic maps only. Secondly, it can create numerous chaotic watermark signals whose auto correlation is strong and cross correlation is weak. Finally, the chaotic watermark signal is difficult to be decoded if the chaotic map model and its parameters are unknown. Chaotic watermark signal can meet the tremendous demand in the applications and the standardization of watermark signals will help watermarking technology to come into realization.

Key words: digital watermarking; chaotic; spread spectrum; watermark signal; watermark standardization

1 引言

近年来,数字水印技术在电子产品版权保护领域得到广泛关注. 一般认为,数字水印算法由数字水印信号的构造算法,嵌入算法和检测算法三部分组成[1]. 本文将重点研究数字水印信号的构造算法. 由于人类视觉系统对纹理具有极高的敏感性,所以水印信号不能构成纹理,而应该具有不可预测的随机性以及与噪声相同的特性. 水印序列宜采用(0,1)或(-1,1)数据流,在嵌入宿主信号前应进行扩频处理[1],以增强水印的鲁棒性. 作为数字水印信号,必需满足如下的特性[2]:(1)视觉不可见性:$X_0 \sim X_w$. 加数字水印信号后的图像 X_w 与宿主图像 X_0 在视觉上难以感知差别. (2)密钥 K 的唯一性:如 $K_1 \neq K_2$,则 $W_1 \neq W_2$. (3)数字水印的不可逆性. (4)数字水印的鲁棒性. 随着数字水印技术研究的进展,如何将水印技术推向应用受到广泛关注. 为满足不同的版权所有者及不同作品的需要,在实际应用中需要大量相互独立(统计意义上)的数字水印信号. 这些水印信号应具有相似性,即结构上或统计意义上的相似. 而大量水印信号还应满足自相关性强,互相关性弱的特性. 这样在大规模应用中,正确的水印信号才能够易于被检测到;而且大量水印信号在应用中不会相互影响,如一个水印信号被攻击者解密,而不会影响其它水印信号. 因此数字水印技术走向实用需要大量易于产生、具有良好统计特性的水印信号.

目前文献中采用的数字水印信号多种多样,具体可归纳如下:(1)伪随机序列. (2)高斯白噪声序列. (3)有特定含义的数字水印信号:通常是选取具有特定意义的字符串作为水印信号,把每个字符作为产生随机序列的种子,最后对所产生的伪随机序列按一定的操作(异或、与操作等)加入到图像数据中. (4)采用一幅二值图像作为数字水印信号. (5)将一幅二值图像进行小波分解,小波系数作为数字水印信号[3]. (6)将灰度级的数字图像分成不同的位面图像,一部分作为数字水印信号,另一部分用作密钥[4]. (7)取一幅彩色图像作为水印图像,对该图像进行 JPEG 压缩,以压缩后的数据流作为数字水印信号[5]. (8)采用具有自相似特性的图像作为水印信号[6].

收稿日期:2002-11-03;修回日期:2004-04-20
基金项目:国家自然科学基金(No. 60172065 和 No. 60373084);广东省"千、百、十"工程优秀人才基金

其中最常用的方法是采用伪随机序列作为数字水印信号. 伪随机序列具有类似白噪声的性质,但又具有周期性和规律性,可以人为地加以产生和复制. 由于移位寄存器的输出是由初始状态和反馈逻辑直接决定的,而且任取一段输出不可能预测其它的输出,因此常选用 m 序列或 M 序列作为数字水印信号. m 序列的自相关性很好,互相关性却不够好,因此不利于水印的正确检测;且 m 序列数量有限,不利于大规模应用. 而采用二值图像,灰度图像及彩色图像作水印信号的方法过于复杂,且图像本身的特性多样化,难以形成统一的标准,也无法分析其序列的相关性,因此同样不适于大规模的应用.

本文针对这些问题,结合了水印信号应满足的特性. 在分析混沌序列特性的基础上,提出基于混沌序列的数字水印信号. 通过本文的研究,表明与目前存在的数字水印信号相比,混沌数字水印信号具有三个明显的优势:易于产生,仅需采用一维混沌映射方程,水印信号生成速度快;数量众多,混沌系统模型、参数和初值的选择不同即可得到互相关性为 0 的两序列;保密性好,如果不知道混沌模型及相关参数,几乎不可能破译. 因此,混沌数字水印信号可以有效地解决实际应用中大量数字水印的产生问题. 同时在水印嵌入时引入扩频通信原理[1],水印的鲁棒性可以得到明显的增强. 数字水印技术的发展最终是走向应用,解决电子产品的版权保护问题,因此数字水印信号采用统一的标准信号才能促进数字水印技术走向应用.

2 混沌数字水印信号

2.1 一维混沌映射的统计特性

一维离散映射 $F: U \to U$,为一实值序列轨迹. 方程可表示为:

$$Z(n+1) = F(Z(n), \lambda),\ Z(n) \in U, \lambda \in R \qquad (1)$$

式中 $n = 0, 1, 2, \cdots$ 表示迭代次数,λ 为控制参数. 对于 λ 的一个特定值,有限空间 U 由两个子集 U_{reg} 和 U_{cha} 组成,即周期序列和混沌序列. 恰当地选取 λ 值,$Z(n)$ 就能形成混沌序列. 常用的一维混沌映射有 Logistic、Kent、Chebyshev 映射[7~10]等等,本文以一维 Logistic 映射生成的混沌序列为例,分析其相关特性. 一维 Logistic 映射方程为:

$$x_{n+1} = 1 - ux_n^2,\ x \in (-1, 1),\ u \in [0, 2] \qquad (2)$$

u 为分叉参数. 当 $u \in [1.40115, 2]$ 时系统进入混沌状态.

当 Logistic 映射在参数 $u = 2.00000$ 时产生的混沌序列均值为 0,自相关性是 δ 函数,互相关性为 0,其概率统计特性与白噪声一致. 混沌系统中参数和初始条件的微小变化都对混沌信号有很大影响. 如图 1 所示的初值相差仅 0.001 的两混沌序列,经过几次迭代后迅速分离,成为两个不相关的序列. 因此混沌序列资源丰富,易于大量产生,可以满足实际应用中数字水印信号的需求量. 图 2 和图 3 分别说明了 Logistic 混沌序列的自相关和互相关特性,图中共有 600 个不同的 Logistic 混沌序列. 混沌序列很强的自相关性使得其作为水印信号易于检测,而很弱的互相关性则说明其可大量用作数字水印信号而互不干扰. 由以上分析可知,混沌序列用作数字水印信号具有下列特性:易于产生,仅需采用一维混沌映射方程,运算量小,因此水印信号生成速度快;数量众多,混沌系统模型、参数和初值的选择不同即可得到互不相关的两序列;密钥(混沌模型、参数及初始值)具有唯一性;水印检测具有可靠性.

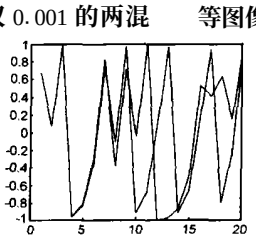

图 1 初值相差 0.001 的两混沌序列

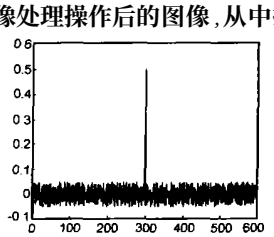

图 2 Logistic 映射序列的自相关函数

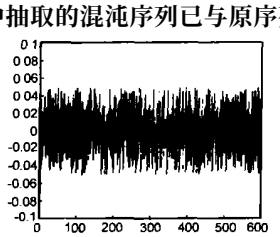

图 3 Logistic 映射序列的互相关函数

2.2 二值混沌序列的构造

根据公式(2)产生的混沌序列是非周期且长度无限的实数序列,但作为水印信号仅需根据需要从中截取合适的长度,进而生成二值序列作为数字水印信号. 由实值序列生成二值序列的方法有很多种,如阈值门限法,多种量化方法等. 本文采用以二进制小数表示一个 0～1 之间的数[11],首先对混沌实值序列 $w_k (k = 0, 1, 2, \cdots, -1 < w_k < 1)$ 取绝对值,即 $0 < |w_k| < 1$,把区间 $(0, 1)$ 上的数 w_k 写成二进制数表达形式

$$w_k = \sum_{v=0}^{\infty} a_{k,v} 2^{-(v+1)},\ a_v = 0 \text{ or } 1 \qquad (3)$$

截取前 L 位,则有

$$\tilde{w}_k = \sum_{v=0}^{L-1} a_{k,v} 2^{-(v+1)} = 2^{-L} \sum_{v=0}^{L-1} a_{k,v} 2^{(L-1)-v} = 2^{-L} B_k \qquad (4)$$

因此,混沌实值序列 w_k 中每一个由一个 L 位的二值序列 B 表示. 文献[11]证明了由混沌实值序列得到的混沌二值序列的统计特性. 混沌二值序列仍具有良好的自相关及互相关特性. 在一些特定条件下混沌实值序列可由穷尽搜索法逆推出来,而二值化后的混沌序列丢失了部分信息,增强了其保密性,更加难以破译. 因此采用混沌二值序列作为数字水印信号,又满足了数字水印信号需具备的另一特性:不可逆性.

2.3 基于混沌序列的数字水印信号

由以上对混沌序列的特性分析可知,混沌序列易于产生,数量众多,不同码元的数目平衡,具有良好的自相关性和互相关性,且可根据需要生成相应长度的混沌序列. 与高斯序列,伪随机序列等相比,更适合用作数字水印信号. 数字水印技术的最终目的是走向应用,解决电子产品版权保护问题,因此对数字水印结构建立一个通用的标准是必要的,而混沌序列恰能满足数字水印标准化所要求的各项特性. 在版权认证机构,登记作者及版权信息的同时,记录下嵌入的数字水印信号信息,即仅需记下混沌序列的产生模型,参数和初值(密钥)即可. 混沌序列数量众多,且水印信号仅需从中截取 3000～6000 个比特,因而可满足实际应用的需要.

数字水印信号应具有较强的鲁棒性,以抵抗一系列的图像处理操作及有意无意的攻击. 经过诸如压缩、扭曲、去噪等等图像处理操作后的图像,从中抽取的混沌序列已与原序列

有了不同,而混沌序列的特点是自相关性很强,而互相关性很弱,遭受一系列有意或无意的攻击后,就给混沌序列的正确检测带来困难.因此应将扩频通信的概念应用到数字水印技术中[1].本文采用 15 位的 m 序列对生成的二值混沌序列直接扩频调制.实验表明可有效提高水印的鲁棒性.

Logistic、Kent、Chebyshev 映射都可用于混沌数字水印信号的产生.在实际应用中,可采用两种方法生成混沌数字水印信号.一种方法是直接利用混沌映射生成二值序列,再经 m 序列扩频后作为数字水印信号嵌入宿主信号.另一种方法是将

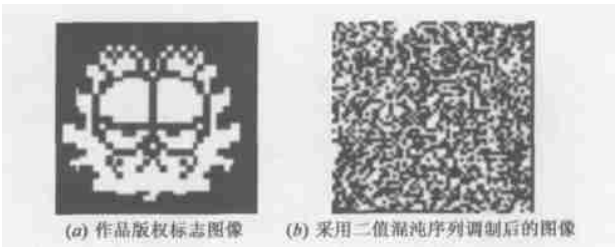

图 4　一种混沌水印信号的生成

用作版权标记的二值图像(如商标等)用混沌二值序列调制后(如图 4 所示),再经 m 序列扩频作为水印信号嵌入宿主信号.即可有效地解决版权争议问题.表 1 中列出了混沌水印信号与其它一些水印信号在水印生成速度,复杂度,水印数目方面的比较,可知混沌水印信号在这些方面具有明显的优势.在水印长度方面,由于 m 序列具有固定周期,因此易于破译,而混沌水印信号是非周期信号,在不知道混沌系统模型及参数的情况下难以破译.由于 m 序列的数量有限,如果作为数字水印信号大规模使用,必然要大量重复使用,不适合用作公钥.而数字水印信号的发展是要建立公共密钥.另外,一维混沌映射方程极其简单,用来产生水印信号极为方便,运算复杂度低.这些特点使得混沌水印信号在大规模应用中具有独特的优势.

表 1　本文的混沌水印信号与其它水印信号的比较

水印信号产生方法	序列长度	水印生成时间	水印数量	水印生成复杂度	保密性
m 序列	固定周期	秒级	有限	低	弱
图像数据	几百～几千	分钟级	有限	高	中等
混沌序列	任意长度	秒级	无数	低	强

3　实验结果

仿真实验采用的宿主图像为 512 ×512 大小的灰度图像,数字水印信号采用图 4 中生成的二值混沌序列.利用不同的初值,产生 600 个不同的 Logistic 混沌序列,分别对图 4(a)中的图像进行调制,并且采用 15 位的 m 序列对生成的二值混沌序列直接扩频调制,形成长度为 4096 比特的混沌水印信号.从产生的 600 个混沌水印信号中,取其中 5 个作为多重数字水印嵌入到宿主图像中[12].

采用峰值信噪比(PSNR)来评价宿主图像和加水印后图像之间的差别.误码率衡量的是扩频后的混沌水印信号与检测到的水印信号的误差程度.相似度指标分析的是,从扩频信号中恢复出的水印 $\tilde{W}(i,j)$ 和原水印 $W(i,j)$ 的相似性,进而判断水印信号是否存在.相似度如下定义:

$$\text{Normalized Correlation}(NC)=\frac{\sum_i\sum_j W(i,j)\,\tilde{W}(i,j)}{\sum_i\sum_j |W(i,j)|^2} \qquad (5)$$

一般情况下,当 $NC>0.5$,就可以判断水印存在.

实验中,攻击手段以 JPEG 压缩为例.图 5 中,5 条直线示出了经 JPEG 压缩后(压缩比为 17.1:1)提取出的 5 个水印信号与原信号的相似度.与不同初值的其它混沌水印信号相比,这些水印信号可明显区分.由图 5 可以得知,混沌水印信号具有较强的鲁棒性,已达到目前文献中一般水印算法所能达到的抗攻击性能.

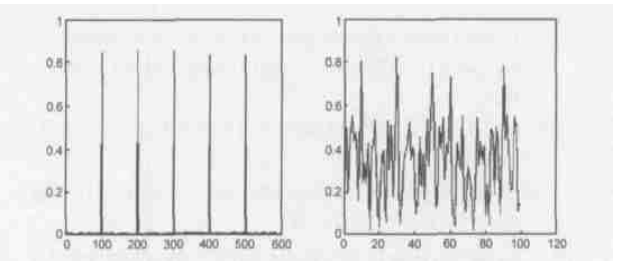

图 5　JPEG 压缩攻击后的水印检测结果(混沌水印信号)　　图 6　JPEG 压缩攻击后的水印检测结果(m 序列水印信号)

水印信号如果采用其它伪序列,以 100 个不同的 31 位 m 序列为例.将这 100 个信号扩频为长度为 4096 位的水印信号,选择其中 5 个水印信号嵌入到宿主图像中,采用与上述相同的 JPEG 压缩攻击,得到的检测结果见图 6.从图中,可以看出,m 序列的自相关性较好,5 个水印的相似度能够大于 0.75.但是,相比于混沌水印信号,m 序列的互相关性却不够好,这非常不利于水印的正确检测.在攻击强度加强的情况下,比较容易导致水印信号的错误识别.

表 2　加水印(水印信号 1)图像经 JPEG 有损压缩处理后提出水印的误码率及相似度

JPEG 压缩比	峰值信噪比(dB)	误码率(%)	相似度
5.59:1	36.43	0.55	0.999
6.43:1	36.04	0.73	0.992
9.18:1	34.65	0.82	0.983
13.5:1	32.16	4.3	0.901
17.1:1	30.88	28.1	0.831

表 2 中给出在宿主图像中只嵌入混沌水印信号 1,经过不同强度的 JPEG 压缩攻击后的检测结果.由表 2 可知,在较低的压缩比情况下,误码率可以忽略,相似度可以接近 1.加大压缩比,误码率急剧增加,而水印的相似度保持比较好,这也说明了扩频处理可能增强水印算法的鲁棒性.

4　结论

本文对数字水印信号需满足的条件,以及混沌序列的特性进行了分析,并与目前出现的数字水印信号进行了比较.由混沌映射产生的混沌序列的自相关和互相关特性都较好,而且用作数字水印信号还具有三个明显的优势,一是易于产生,仅需采用一维混沌映射,如 Logistic、Kent、Chebyshev 映射等等,方程简单,水印信号生成速度快;二是数量众多,混沌系统模

型不同,参数和初值的选择不同即可得到互相关性为 0 的序列,如初值仅相差 0.001 亦可得到完全不同的两序列,可满足数字水印信号大规模应用的需求量;三是保密性好,如果不知道混沌模型及相关参数,几乎不可能破译.因此混沌数字水印信号具有不可逆性.因此,混沌序列是最适合用作数字水印信号的序列.为增强水印的鲁棒性,在嵌入水印过程中引入扩频通信原理.本文提出的基于混沌序列的数字水印信号,有利于数字水印信号的标准化,进而推动数字水印技术走向实用.下一步的工作是根据混沌序列的统计特性,研究最优的混沌水印信号检测算法.

参考文献:

[1] I J Cox, J Kilian, T Shamoon. Secure spread spectrum watermarking for multimedia[J]. IEEE Trans on Image Processing, 1997, 6(12): 1673 - 1687.

[2] 陈明奇,钮心忻. 数字水印的研究进展和应用[J]. 通信学报, 2001, 5(22): 71 - 79.

[3] 韦志辉. 基于小波域中视觉门限模型的数字水印技术[J]. 东南大学学报, 1998, 9(28): 44 - 48.

[4] Xia-mu Niu, Sheng-he Sun. Adaptive gray-level digital watermark[A]. In ICSP'2000[C]. Beijing, 2000. 1293 - 1298.

[5] 易开祥. 自适应二维数字水印系统[J]. 中国图像图形学, 2001, 5(6): 444 - 449.

[6] Cao Hanqiang. A watermarking method based on fractal self-similarity [A]. In ICSP'2000[C]. Beijing, 2000. 99 - 103.

[7] 刘文波. 混沌信号的一种简单设计方法及应用[J]. 南京航空航天大学学报, 1998, 6(30): 288 - 292.

[8] 郭杰. Chebyshev 混沌序列和 m 序列的特性比较和分析[J]. 重庆邮电学院学报, 1999, 12(11): 30 - 33.

[9] H Bateni, C D Mcgillem. A chaotic direct-sequence spread-spectrum communication system[J]. IEEE Trans on Communication, 1994, 42: 1524 - 1527.

[10] G M Bernstein, M A Lieberman. Secure random number generation using chaotic circuit [J]. IEEE Trans on CAS, 1990, 37(9): 1157 - 1164.

[11] T Kohda, A Tsuneda. Statistics of chaotic binary sequences[J]. IEEE Trans on Information Theory, 1997, 6(43): 104 - 112.

[12] 纪震,肖薇薇. 基于混沌序列的多重数字图像水印算法[J]. 计算机学报, 2003, 26(11): 1555 - 1561.

作者简介:

纪 震 男,1973 年 8 月出生于江苏省溧阳市,工学博士,副教授,主要研究方向:医学图像处理,数字水印以及数字信号处理硬件系统.

李慧慧 女,1980 年 9 月出生于广东省廉江市,硕士研究生,主要研究方向:数字信号处理硬件实现以及混沌理论.

肖薇薇 女,1973 年 6 月出生于安徽省合肥市,硕士,讲师,主要研究方向:数字水印以及混沌理论.

张基宏 男,1964 年 8 月出生于江苏省海安县,工学博士,教授,主要研究方向:数字图像处理以及图像压缩技术.