一种基于共轭混沌映射的数字水印算法研究

张 伟[1,2] 廖晓峰[1] 韦鹏程[1,2] 杨华千[1,2] 黄 松[1,2]
(重庆大学计算机科学与工程学院 重庆 400044)[1]
(重庆教育学院计算机与现代教育技术系 重庆 400067)[2]

摘 要 数字水印技术在多媒体方面有着广泛的应用,其中最受关注,同时也是要求最高的应用是用于版权保护的数字水印技术。本文提出了一种基于共轭的抗剪切鲁棒水印算法,运用一类标准混沌映射,构造了一种具有强非线性耦合的置换方式,从而改变水印图像像素点的位置,利用共轭映射产生密钥流改变载体图像的灰度值,然后对水印进行嵌入。实验结果证明该方案具有可行性、鲁棒性和安全性。

关键词 混沌,共轭映射,数字水印

A Novel Watermarking Algorithm Based on Coupled Chaotic Map

ZHANG Wei[1,2] LIAO Xiao-Feng[1] WEI Peng-Cheng[1,2] YANG Hua-Qian[1,2] HUANG Song[1,2]
(Department of Computer Science and Engineering, Chongqing University, Chongqing 400044)[1]
(Department of Computer and Modern Education Technology, Chongqing Education College, Chongqing 400067)[2]

Abstract Digital watermarking is widely used for a variety of multimedia applications, of which technique aiming at copyright protection is the most difficult as well as attractive. In this paper, a robust digital watermark algorithm based on coupled chaotic map is proposed. First, the original binary watermark is permuted by standard chaotic map, and the grey value of original image is masked according the coupled map. Then, the permuted watermark is embedded in the masked original image. Simulation results have demonstrated that this scheme is practical, secure and robust.

Keywords Chaos, Coupled map, Digital watermarking

1 引言

目前,数字水印技术在多媒体数字产品的版权保护上已经有了广泛的应用。对它的研究涉及领域很多,其理论与图像隐藏、信号处理、密码学、通信理论、视觉感知理论等密切有关;其应用与网络信息安全、数字多媒体版权保护等联系紧密。尽管它还比较年轻,但却按指数速率成长。目前,对该领域的研究主要集中在水印算法的设计上,大致可分为三类:其一是水印生成技术,研究如何产生一个与作者和作品直接有关的信息(一般是一个随机信号);其二是水印嵌入技术,研究如何在空域、变换域、混合域等嵌入水印信息而获得好的水印特性。其三是水印检测技术,研究如何有效地从含水印载体中提取出水印信息(或检测到水印的存在)。

经过十余年的研究,国内外所提出的水印算法很多,不同的嵌入算法和检测算法以及嵌入强度的不同,必定会有不同的性能,有的抗滤波能力较强,有的抗压缩能力较好。从目前的水印算法来看,大多数算法的抗几何变换的能力都比较弱,当载体图像被旋转、伸缩变换,尤其是空域水印在被剪切掉一半以后,所提取的水印信息已非常模糊[1],不满足水印的保真性要求。因此,抗几何变换的鲁棒水印算法是目前水印算法研究中的一个热点[1,2]。为提高水印系统的抗几何变换的能力,目前的算法都是基于变换域的嵌入方法[3,4]。由于这种方法需要对图像进行 DCT 或 DWT 变换,影响算法的速度。本文应用离散混沌动力系统,针对图像数据的存储特点,设计了一种基于共轭混沌映射 Logistic 映射和 Tent 映射的数字水印算法,在空域内对载体图像和水印信号进行变换处理,以提高水印系统的保密性和抗剪切能力。MATLAB 实验结果表明,在受到剪切 3/4 的强攻击情况下,所提取出的水印图像仍然比较清晰。因此,该算法具有较好的保密性和保真性,有很高的实用价值。

2 混沌映射的拓扑共轭

混沌现象是一种有界的内在的随机过程,具有时间遍历性,这种过程既非周期性,又不收敛。任意相近的两点经过若干次混沌迭代之后,就会呈现指数发散,所以根据混沌序列很难确定混沌系统的初值和参数。另外,混沌轨道极其不规则,经过系统局部扩展、压缩、折叠之后,系统的输出类似于随机噪声。这些特点,都使得混沌映射很适合用来设计密码系统。

由于很多混沌映射具有拓扑共轭性质[5],比如 Logistic 映射就与改进的 Logistic 映射、Tent 映射以及 Chebyshev 映射等具有拓扑共轭关系。而这种拓扑共轭关系是一种等价关系,因此就可以重点地研究和分析其中的某几类混沌映射的性能。

定义 1 设 $x=h(\theta)$是连续、可逆的函数。对映射 $f(x)$作变换

$$g(\theta)=h^{-1}(f(h(\theta))) \tag{1}$$

或简记为 $g=h^{-1}\circ f\circ h$,则称(1)式为映射 $f(x)$到 $g(\theta)$的拓扑共轭变换。

当 f 与 g 拓扑共轭时,记为 $f\sim g$。拓扑共轭关系是一种等价关系,满足下面三条性质:

*)基金项目:中国博士后基金一等资助项目(No. 20060390175),重庆市科委自然科学基金资助项目(No. CSTC,2005BB2286,2006BB2254),重庆市教委资助项目(No. kj051501,No. kj061501)。**张 伟** 教授,博士后,主要研究方向为信息安全、计算智能与数据挖掘;**廖晓峰** 教授,博士生导师,主要研究方向为神经网络、混沌理论;**韦鹏程** 博士研究生,主要研究方向为信息安全、混沌理论;**杨华千** 博士研究生,主要研究方向为信息安全、混沌数字水印;**黄 松** 博士研究生,主要研究方向为图像处理、数字水印。

① 反身性：f 与 f 是拓扑共轭的，即 $f\sim f$；

② 对称性：若 $f\sim g$，则 $g\sim f$；

③ 传递性：若 $f\sim g$，$g\sim\varphi$，则 $f\sim\varphi$。

具有拓扑共轭关系的两个映射实际上是不同坐标表示下的同一种映射，因此拓扑共轭变换具有一些不变性质。

性质 1 如果映射 $f(x)$ 和 $g(\theta)$ 具有拓扑共轭关系，则

$$g^{(n)}=h^{-1}\circ f^{(n)}\circ h$$

即 f 的迭代与 g 的迭代仍然存在拓扑等价关系。

推论 1 设有一对满足拓扑共轭变换的映射 f 和 g，如果 f 有 n 周期轨道，则 g 也有 n 周期轨道，且两者具有相同的稳定性，即 Lyapunov 指数。

对于 Logistic 映射：

$$f(x)=4x(1-x),x\in[0,1] \tag{2}$$

与 Tent 映射：

$$g(x)=\begin{cases}2x, & x\in[0,1/2]\\ 2(1-x), & x\in(1/2,1]\end{cases} \tag{3}$$

是具有拓扑共轭关系。

证明：考虑如下映射：

$$h(x)=\sin^2\frac{\pi x}{2},x\in[0,1]$$

易见 $h(x)$ 是[0,1]到[0,1]上的单调可逆映射，且

$$f\circ h(x)=4\sin^2\frac{\pi x}{2}(1-\sin^2\frac{\pi x}{2})=\sin^2\pi x$$

$$h\circ g(x)=\begin{cases}\sin^2\dfrac{\pi x\cdot 2x}{2}=\sin^2\pi x,x\in[0,\dfrac{1}{2}]\\ \sin^2\dfrac{\pi x\cdot 2(1-x)}{2}=\sin^2\pi x,x\in[\dfrac{1}{2},1]\end{cases}$$

即 $f\circ h(x)=h\circ g(x)=\sin^2\pi x$，于是有 $g(x)=h^{-1}\circ f\circ h(x)$，根据定义 1 可知 $f(x)$ 与 $g(x)$ 是拓扑共轭的。

拓扑共轭映射的密度分布也有着密切的关系。由“点数守恒”条件

$$\rho_T(\theta)\mathrm{d}\theta=\rho_L(x)\mathrm{d}x$$

得到：

$$\rho_L(x)=p_T(h^{-1}(x))\left|\frac{\mathrm{d}h^{-1}(x)}{\mathrm{d}x}\right|$$

注意 Tent 映射具有唯一不变的密度分布函数 $\rho_T(x)=1$，因为分布函数与初值无关，所以该映射一定是遍历的。又

$$h^{-1}(x)=\frac{2}{\pi}\arcsin\sqrt{x},x\in[0,1]$$

于是得到 Logistic 映射的密度分布函数为

$$\rho_f(x)=\frac{1}{\pi\sqrt{x(1-x)}},x\in[0,1]$$

此外 Tent 映射的 Lyapunov 指数为 ln 2，由拓扑共轭的性质可知道 Logistic 映射的 Lyapunov 指数也为 ln 2。与下式(Lyapunov 指数定义)计算结果相同。

$$\lambda_L=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n}\ln|f'(x_i)|=\ln 2$$

利用概率密度函数，可以容易地计算出 Logistic 映射所产生的混沌序列一些统计特性：平均值：

$$\bar{x}=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N=1}x_i=\int_{-1}^{1}x\rho(x)=0 \tag{4}$$

对于自相关函数 $ac(m)$，当自相关间隔 $m=0$ 时，

$$ac(m)\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N=1}x_i^2-\bar{x}^2=\int_{-1}^{1}x^2\rho(x)-0=\int_{-1}^{1}\frac{x^2}{\pi\sqrt{1-x^2}}\mathrm{d}x=$$

$$\left.\frac{1}{\pi[\arcsin x-0.5(\pi\sqrt{1-x^2}+\arcsin x)]}\right|_{-1}^{1}$$

$$=0.5 \tag{5}$$

当自相关间隔时 $m\neq 0$，

$$ac(m)=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N=1}x_ix_{i+m}-\bar{x}^2=\int_{-1}^{1}xf^m(x)\rho(x)\mathrm{d}x-0=0 \tag{6}$$

式中 $f^m(x)=f(f\cdots f(x)\cdots)$。

独立选取 2 个不同的初始值 x_{01} 和 x_{02}，它们分别产生 2 个混沌序列的互相关函数为：

$$ac_{12}(m)=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N=i}x_{1i}x_{2i+m}-\bar{x}^2=\int_{-1}^{1}\int_{-1}^{1}x_1f^m(x_1)\rho(x_1)\rho(x_2)\mathrm{d}x_1\mathrm{d}x_2-0=0 \tag{7}$$

式中 $f^m(x)=f(f\cdots f(x)\cdots)$。

从以上的统计特性可以看出，Logistic 映射在参数 $\mu=4.000$ 时产生的混沌序列均值为 0，自相关是 δ 函数，互相关为 0，其概率统计特性与白噪声一致的。

3 水印图像置乱

设 W 为 $N_1\times N_2$ 大小的水印图像。为使水印信号具有宽频特性和提高水印系统的保密性与鲁棒性，在水印被嵌入前，我们先对水印信号进行混沌加密。

借鉴混沌系统中的标准映射[6,7]

$$\begin{pmatrix}x_{n+1}\\ y_{n+1}\end{pmatrix}=\begin{pmatrix}\mathrm{mod}(x_n+y_n,2\pi)-\pi\\ y_n+p\sin(x_n+y_n)\end{pmatrix} \tag{8}$$

为了设计图像的置换变换，将式(8)推广成如下形式

$$i'=\mathrm{mod}(i+\Phi(j),M)\quad j'=\mathrm{mod}(j+\Phi(i'),N) \tag{9}$$

其中 i,j,i',j',M,N 是整数，

$$\Phi(j)=\mathrm{mod}(i,\lfloor j.k1_n+0.5\rfloor,N)$$

$$\Phi(i')=\mathrm{mod}(i',\lfloor i.k2_n+0.5\rfloor,M) \tag{10}$$

其中，$\lfloor x\rfloor$ 表示取 x 的整数部分，$k1_n,k2_n$ 为第 n 置换操作的密钥，n 为进行置换操作的次数。式(10)的逆为：

$$j=\mathrm{mod}(j'-\Phi(i'),N)\quad i=\mathrm{mod}(i'-\Phi(j'),M) \tag{11}$$

$k1_n,k2_n$ 是由共扼映射(2)和(3)产生的。利用式 (8)可以对大小为 $M\times N$ 的图像进行置换加密操作，文[7]已经证明了式(9)的逆映射(11)的存在性，故可用(11)进行逆置换解密操作，所以算法是正确的。

4 载体图像加密

设载体图像的灰度等级为 L，$I(i,j)$ 表示 (i,j) 位置的灰度值，$I'(i,j)$ 表示进行灰度替代之后 (i,j) 位置的灰度值，$k1_n,k2_n$ 是由共扼映射(2)和(3)产生的伪随机序列，令 $S_n=k1_n+k2_n$ 设计如下的灰度替代：

$$I'(i,j)=k1_n\oplus((k2_n+I(i,j))\bmod L,\text{ 当 }S_n\text{ 为偶数}$$

$$I'(i,j)=k2_n\oplus((k1_n+I(i,j))\bmod L,\text{ 当 }S_n\text{ 为奇数} \tag{12}$$

式(12)的逆变换为：

$$I(i,j)=k1_n\oplus((I'(i,j)-k2_n)\bmod L)\text{ 当 }S_n\text{ 为偶数}$$

$$I(i,j)=k2_n((I'(i,j)-k1_n)\bmod L)\text{ 当 }S_n\text{ 为奇数} \tag{13}$$

式(12)可以对大小为 $M\times N$ 的图像进行灰度替代的加密操作，可用(13)进行逆变灰度替代的解密操作，所以算法是正确的。

5 水印嵌入与提取

5.1 水印嵌入

设载体图像的灰度等级为 L，$I(i,j)$ 表示 $M_1\times M_2$ 的载体图像 (i,j) 位置的像素值，n 表示混沌水印序列 w_n 的长度，$1\leqslant n\leqslant N_1\times N_2$，采用位平面算法，将水印信号嵌入到第 a，$a+1$ 和 $a+2$ 位，$(a\leqslant\min(M_1-N_1,M_2-N_2)$。嵌入过程为：

For $i=0$ to N_1-1

For $j=0$ to N_2-1

Let $I(i,j)=\sum_{t=0}^{a+2} d_t\times 2^t$

$no=a+b(2\times i\times N_2+2\times j)+b(2\times i\times N_2+2\times j+1)$

$d_{no}=w(i,j)$

$I^*(i,j)=\sum_{t=0}^{a+2} d_t\times 2^t$

End

End

5.2 水印提取

对载体图像 I^* 运用与嵌入过程相同的置乱变换后恢复水印信号 w'。其方法与嵌入过程相似，只需作以下改动：

Let $I^*(i,j)=\sum_{t=0}^{a+2} d_t\times 2^t$

$n0=a+b(2\times i\times N_2+2\times j)+b(2\times j\times N_2+2\times j+1)$

$w'=d_{no}$

将提取出的水印信号 w' 解密即可得到近似于原始水印的水印信号 w^*。

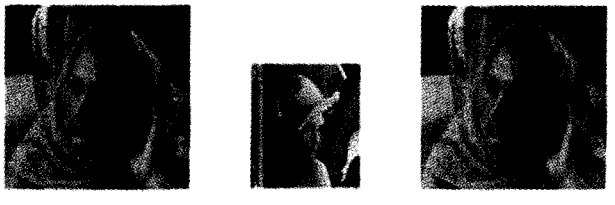
6 实验与分析

6.1 水印检测实验

水印检测中，我们运用相似度来评价提取水印与原始水印的相似性，相似度采用下式计算：

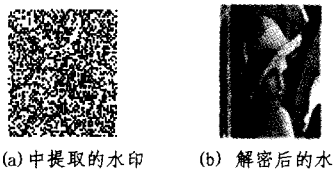
$$sim(W,W^*)=\frac{\sum_{i=1}^{N}W(i)W^*(i)}{\sqrt{\sum_{i=1}^{N}W(i)^2}\sqrt{\sum_{i=1}^{N}W^*(i)^2}} \tag{14}$$

式中 W 与 W^* 分别是原始和提取的水印序列，N 为嵌入水印的长度。当提取水印与原始水印相同时 $sim=1$，否则 $sim<1$。显然，sim 越接近 1 表明提取的水印越有效。图 1 和图 2 是水印检测的结果。按照嵌入算法将水印嵌入后，得到含水印的图像(如图 1(c))，与图 1(a)对比，说明算法具有很好的不可感知性；同时从含水印的图像中所提取的水印具有较好的安全性。



(a) 原始图像　(b) 原始水印　(c) 含水印图形

图 1



(a) 中提取的水印　(b) 解密后的水印

图 2

图 3　从图 1(c)中剪切 32、64、96 和 128 像素

6.2 抗剪切实验

将含水印图像两边分别剪去 32、64、96 和 128 像素，如图 3 所示。检测时先用原始图像填充被剪切的部分，然后进行检测，从被剪切图像中提取的水印和原始水印的相似度值如表 1 所示。

表 1　从剪切的图像中提取水印和原始水印的相似度值

剪切长度	32	64	128
Sim 值	0.887	0.736	0.602

将含水印图像(图 1(c)分别加噪声，高斯噪声值分别是 2,4 和 8，然后从含噪声的水印图像提取水印，结果如图 4 所示，表 2 是从噪声图像中提取的水印和原始水印的相似度值。

图 4　从含噪声的图像提取水印

表 2　从噪声图像中提取的水印和原始水印的相似度值

高斯噪声强度	2	4	8
Sim 值	0.842	0.696	0.621

6.3 抗 JPEG 压缩变换

将含水印图像图 1(c)分别进行 JPEG 压缩变换，压缩比分别为 80,70 和 60。然后从经过 JPEG 压缩变换的水印图像提取水印，结果如图 5 所示，表 3 是从经过 JPEG 压缩变换图像中提取的水印和原始水印的相似度值。

图 5　经过 JPEG 的水印图像提取水印

表 3　从经过 JPEG 压缩变换图像中提取的水印和原始水印的相似度值

压缩比	80	70	60
Sim 值	0.897	0.675	0.598

结束语　本文提出了一种空域内基于共轭的抗剪切鲁棒水印算法。运用混沌动力学系统所产生的伪随机序列对水印信号进行混沌加密、对载体图像进行混沌密码变换，然后对水印进行嵌入，经过水印检测、剪切、压缩和添加噪声等实验，可以看出，该算法具有较强的保密性和抗几何攻击的能力。

参 考 文 献

1 Yen J C. Watermarks Embedded in the Permuted Image. Electronics Letters, 2001, 37: 80～81

2 Feng G R, Jiang L G, He C, Wang D J. A Novel Algorithm for Embedding and Detecting Digital Watermarks. Acoustics, speech and signal processing 2003 proceedings, ICASSP'03, 2003, 3: Ⅲ 549～552

3 Lin C Y, Wu M, Bloom J I. Rotation, Scale, and Translation Resilient Watermarking for Images. IEEE Trans. Image Processing, 2001, 10: 767～782

4 Wang Y, Doherty J, Dyck R V. A Wavelet-based Watermarking Algorithm for Ownership Verification of Digital Images. IEEE Trans. Image Processing, 2002, 11: 77～88

5 彭军. 混沌在网络信息安全中的应用研究:[博士论文]. 2003, 6: 27～40

6 李昌刚，韩正之，张浩然. 一种随机密钥及"类标准映射"的图像加密. 计算机学报，2003, 26 (4): 465～470

7 樊春霞. 混沌保密通信系统的研究:[博士论文]. 2004, 10: 97～99