一种基于混沌动力系统同步原理的非对称水印

刘　伟，宋文敏
（莱芜职业技术学院，山东　莱芜　271100）

摘　要：提出了一种基于混沌动力系统同步原理的非对称数字水印构造方法。将二值水印图像转化为二进制数字信号，控制混沌驱动系统两路交替输出信号，形成载有水印信息的混沌信号，并将其作为水印信号嵌入载体图像。水印提取过程中将提取出的水印信号送入混沌响应子系统，根据响应子系统的输出信号与水印信号的相关性来恢复水印图像。在水印嵌入及提取过程中使用不同的混沌系统模型、参数及状态变量初值，实现了非对称数字水印系统的构造。

关键词：混沌同步；非对称数字水印；混沌键控；小波变换
中图分类号：TP309　　**文献标识码**：A

Asymmetric digital watermarking based on chaotic synchronization theory

LIU Wei, SONG Wen Min
(Laiwu College of Technology, Laiwu 271100, China)

Abstract: A method of making an asymmetric digital watermarking based on chaotic synchronization theory is proposed in this paper. Firstly, we transform the double value watermark image into binary digital signals that control the alternative output of two-way chaos signals in chaotic driving system. Secondly, we embed the final chaotic signals which are loaded with watermark information into the carrier image. During the watermark extraction process, we input the watermark signals extracted from the carrier image with watermark information into the chaotic response system, and revert the watermark signals to the watermark image according to the relativity between the outputting signals of chaotic response system and the watermark signals. Different chaotic models, parameters and initial values of variable in watermark embedding process and extraction process are applied; therefore, the digital watermarking on the theory of chaotic synchronization is an asymmetric digital watermarking.

Key words: chaotic synchronization; asymmetric digital watermarking; chaotic shift keying; wavelet transform

数字水印作为新型数字版权保护技术其应用日趋广泛。目前大部分水印嵌入与检测技术都是对称体制的，即水印检测所需信息与水印嵌入时所知信息是一致的，而许多实际的应用都要求非对称的数字水印方案，如网上交易，公众通过检测水印信息来明确数字产品的版权归属，此时的水印应为非对称数字水印。

近年来，有不少学者在非对称水印算法方面作了大量研究工作，提出了一些可行的技术。如扩频非对称数字水印、legendre 水印、特征向量水印、基于单向信号处理的非对称水印、基于 MPEG 图像类型标记水印等[1]。

本文尝试将混沌动力系统的同步理论应用于非对称数字水印系统的构造，先把二值水印图像转化为二进制数字控制信号，控制混沌驱动系统生成混沌信号，然后将混沌信号作为水印信息嵌入载体图像。水印提取过程中将提取出的水印信息转化为水印信号，送入混沌响应系统，从而恢复原二值水印图像。

1　混沌动力系统同步理论

混沌动力系统同步是指两个动力学结构完全相同的混沌系统（一个被称为驱动子系统，另一个称作响应子系统），通过驱动信号对响应系统的作用，在演化开始时两个子系统的初值不同，随着时间的演化，两个子系统相对应的状态量的差值趋于零，称这两个子系统达到了同步。

目前，应用在保密通信中的同步方案主要有驱动响

应同步、耦合同步、反馈微扰同步、自适应同步、噪声同步等[2]。大部分混沌动力系统的同步化方法都属于驱动响应类型。

1.1 驱动-响应同步方案

驱动-响应混沌同步方法是由美国学者 Pecora 和 Carroll 在 1990 年提出来的。其基本原理为：将驱动系统分解成一个稳定的子系统和一个不稳定的子系统，复制一个与稳定的子系统完全相同的系统作为响应系统。设有如下 n 维混沌系统：

$$\dot{x}=f(x) \quad (1)$$

式中，$x\in R^n$。将式(1)的状态变量分解为 $u=(x_1,x_2,\cdots,x_m)$ 和 $v=(x_{m+1},x_{m+2},\cdots,x_n)$2 个部分，相应的 $f(x)$ 分解为 $f_u=(f_1,f_2,\cdots,f_m)$ 和 $f_v=(f_{m+1},f_{m+2},\cdots,f_n)$。将驱动系统分解为 2 个子系统：$\dot{u}=f_u(u,v)$，$\dot{v}=f_v(u,v)$；复制子系统 v，建立响应系统 w：$\dot{w}=f_w(u,w)$。当 $t\to\infty$ 时，若有 $w\to v$，则子系统 w 与 v 同步，其中 u 为驱动变量。如果响应系统的所有条件 Lyapunov 指数为负，则经过一段时间后，响应系统和驱动系统达到同步，且同步是渐近稳定的[3]。

参考文献[4]的研究结果表明：采用离散时间驱动方式，当驱动信号的采集周期(采集 2 个驱动信号的时间间隔)小于某一阈值时，用离散的混沌信号驱动响应系统可达到与连续混沌信号驱动响应系统同样的渐近稳定性。因此，只要适当选择驱动信号采样间隔，总可以使响应混沌系统与驱动混沌系统达到同步。该研究成果证明了将离散的混沌信号作为水印信息嵌入载体图像，然后在提取过程中将提取出的水印信号送入响应子系统进行离散时间驱动，从而恢复原水印图像的算法的可行性。

以 Lorenz 系统为例，驱动系统为：

$$\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=cx-xz-y\\ \dot{z}=xy-bz\end{cases} \quad (2)$$

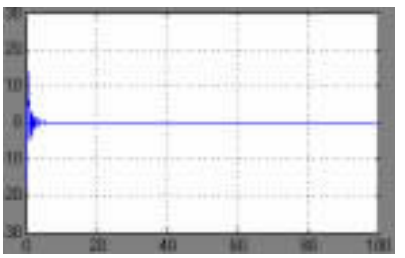
当 $a=10$、$b=\frac{8}{3}$、$c=28$ 时，系统进入混沌状态。响应系统可构造为：

$$\begin{cases}\dot{x}=a(y'-x)+k_x(x-x')\\ \dot{y}=cx-xz'-y'\\ \dot{z}=xy'-bz'\end{cases} \quad (3)$$

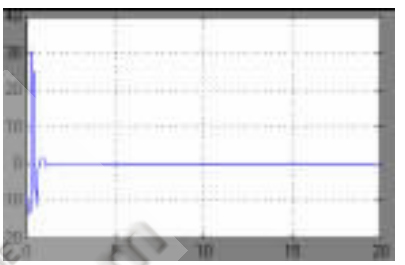
$$\begin{cases}\dot{x}=a(y-x')\\ \dot{y}=cx'-x'z'-y+k_y(y-y')\\ \dot{z}=x'y-bz'\end{cases} \quad (4)$$

(3)式响应系统的驱动信号 x 与(4)式响应子系统的驱动信号 y 均来源于驱动子系统(2)式的输入；k_x、k_y(k_x、k_y 均大于 7.7[5])是由同步稳定性条件决定的常数反馈增益。

图 1 给出了不同初始条件下，信号采样周期 $t=0.02$s 时，驱动系统和响应子系统的同步情况。可以看出，两个响应子系统都可以在短时间内迅速与驱动系统保持同步。



(a)$x-x'$驱动信号为 x



(b)$y-y'$驱动信号为 y

图 1 驱动系统与响应系统同步情况

1.2 混沌键控

混沌键控的基本思想是：首先将二进制(或多进制)数字信息信号分别映射为 2 种(或多种)混沌吸引子，被传输的混沌信号在不同的混沌吸引子之间切换，然后利用混沌同步来判断传输信号来自哪种混沌吸引子，从而解调出二进制(或多进制)数字信息信号的混沌通信机制[6]。

本文采用二进制混沌键控的保密通信方法，实现由二值水印图像生成的二进制数字信号控制驱动系统生成水印信号嵌入载体图像，提取水印时通过响应系统恢复水印图像。

驱动系统与响应系统结构图分别如图 2、图 3 所示。

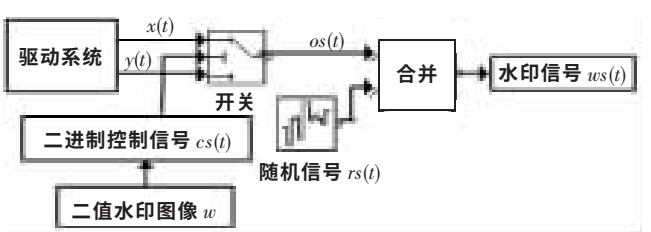


图 2 驱动系统结构图

在驱动系统结构图中，将二值水印图像转化为二进制数字信号，并作为控制信号控制驱动系统使其状态变量 $x(t)$、$y(t)$ 交替输出，输出信号可表示为 $os(t)=\begin{cases}x(t) & cs(t)=1\\ y(t) & cs(t)=0\end{cases}$。为了防止预测法的攻击，最终的水印信号 $ws(t)$ 由混沌信号 $os(t)$ 加强度小于某一阈值的随机噪

声 $rs(t)$ 生成，这样既不会改变混沌信号良好的特性与驱动能力，又使得攻击者无法由混沌信号重构原系统的相空间，进而无法恢复水印信息。

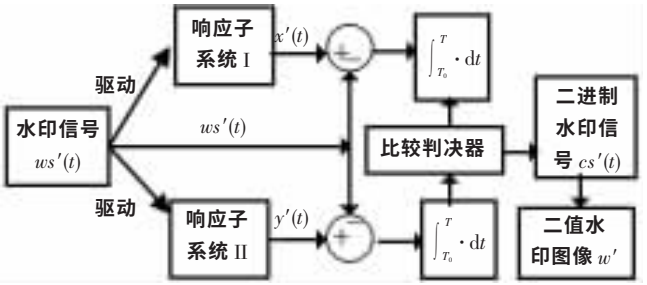


图 3　响应系统结构图

在响应系统中，将提取的水印信号同时送入响应系统 I 和响应系统 II 进行驱动。在每个时刻 t，只有一个响应子系统受到正确同步信号的驱动，因而其轨道误差收敛，2 个系统渐近同步，而另一个响应子系统必然受到非同步信号的驱动，故其轨道误差必然发散[7]。如在某时刻 t，有 $os(t)=x(t)$，则只有响应系统 I 受到正确信号驱动，$x(t)\to x'(t)\to 0$。

响应子系统的输出信号 $x'(t)$、$y'(t)$ 分别与信号 $ws'(t)$ 相减，形成误差信号 $|ws'(t)-x'(t)|$ 和 $|ws'(t)-y'(t)|$，将 2 个误差信号送入积分器积分得 $e_x(t)=\int_{T_s}^{T}|ws'(t)-x'(t)|\mathrm{d}t$，$e_y(t)=\int_{T_s}^{T}|ws'(t)-y'(t)|\mathrm{d}t$。其中，$T$ 是驱动系统中 1 bit 控制信号 $cs(t)$ 的码宽，T_s 是到达同步的时刻，$T-T_s$ 是观测时间。当 $cs(t)=1$ 时，驱动系统发送的信号为 $x(t)$，响应子系统 I 受到同步信号驱动，而响应系统 II 受到非同步信号驱动，因此，$e_x(t)$ 收敛而 $e_y(t)$ 发散，有 $e_x(t)<e_y(t)$；当 $cs(t)=0$ 时，驱动系统发送的信号为 $y(t)$，则有 $e_y(t)<e_x(t)$。比较判决器的输出可定义为：$cs(t)'=\begin{cases}1 & e_x(t)<e_y(t)\\ 0 & e_y(t)<e_x(t)\end{cases}$

图 4 给出了当数据采样时间 $t=0.02$、1 bit 控制信号码宽 $T=6$ 时，控制信号、误差信号 $|ws'(t)-x'(t)|$ 及误差信号 $|ws'(t)-y'(t)|$ 的波形图。

2　基于混沌同步的非对称数字水印算法

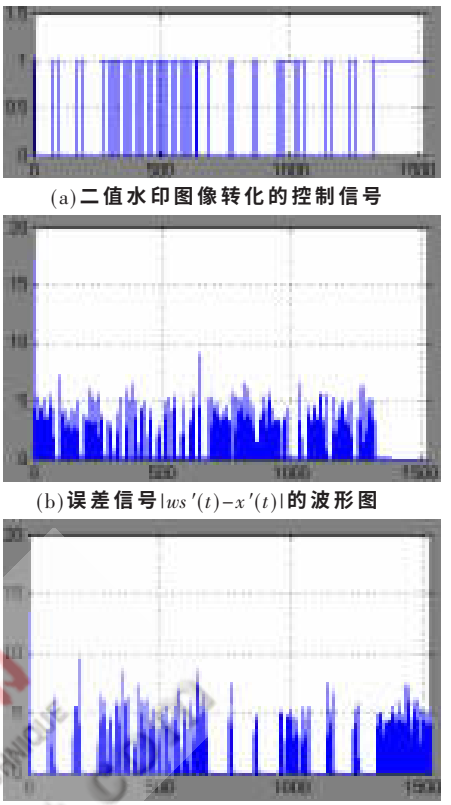
2.1　水印嵌入算法

混沌驱动系统通过生成混沌信号实现了将水印图像信息加载于混沌信号中，形成水印信息。本文采用小波变换的乘性嵌入算法将水印信息嵌入载体图像中，具体步骤如下：

(1)对原图像 I 进行三级小波分解，得到中、高频系数 LH_k、HL_k、$HH_k(k=1,2,3$，以下同)。

(2)将水印信息 ws 映射为范围在 $[-1,1]$ 间的实数序列 $wsrl$。

(3)按绝对值的大小对小波系数 LH_k、HL_k、HH_k 分别进行排序，并记下其位置。



(a)二值水印图像转化的控制信号

(b)误差信号 $|ws'(t)-x'(t)|$ 的波形图

(c)误差信号 $|ws'(t)-y'(t)|$ 的波形图

图 4　控制信号及误差信号波形图

(4)根据各级中、高频小波系数的个数，将 $wsrl$ 分为 9 部分：$wsrl=\{\underset{length=m_1}{wsrl_{LH_1}},\underset{length=m_2}{wsrl_{LH_2}},\cdots,\underset{length=m_9}{wsrl_{HH_3}}\}$，其中 $\sum_{i=1}^{9}m_i=\mathrm{length}(wsrl)$。采用乘性嵌入方法，将 $\{\underset{length=m_1}{wsrl_{LH_1}},\underset{length=m_2}{wsrl_{LH_2}},\cdots,\underset{length=m_9}{wsrl_{HH_3}}\}$ 分别嵌入对应的 LH_k、HL_k、HH_k 系数中绝对值最大的 $m_i(i=9)$ 个系数中。令小波系数统一表示为 x_{i_w}，加入水印信息后的小波系数为 $x_{i_w}^{w}$，则乘性嵌入方法的公式为：$x_{i_w}^{w}=x_{i_w}(1+\alpha\, wsrl_i)$，其中 α 为嵌入强度因子，为兼顾不可见性与健壮性，α 可取 0.1~0.3。

(5) 对嵌入水印信息的小波系数进行小波反变换，得到嵌有水印信息的图像 I′。

2.2　水印信息提取算法

水印信息提取是嵌入的逆过程，具体步骤如下：

(1)对嵌有水印信息的载体图像 I′和原载体图像 I 分别进行三级小波分解，得到中、高频系数 LH_k'、HL_k'、HH_k' 及 LH_k、HL_k、HH_k。

(2)按绝对值的大小对原载体图像的小波系数 LH_k、HL_k、HH_k 分别进行排序，并记下其位置。按照原载体图像小波系数的排列顺序对嵌有水印信息的载体图像的小波系数 LH_k'、HL_k'、HH_k' 分别进行排序。

(3)按乘性嵌入算法的逆过程分别从图像 I′的中、高频系数 LH_k'、HL_k'、HH_k' 中提取出水印信息。令图像 I 的

小波系数统一表示为 x_{i_u}，图像 I′的小波系数统一表示为 $x^{w}_{i_u}$，则水印信息 $wsrl_i=(x^{w}_{i_u}-x_{i_u})/\alpha\cdot x_{i_u}$。将各水印信息段 $\{wsrl'_{\underset{length=m_1}{LH_1}}, wsrl'_{\underset{length=m_9}{LH_2}}, \cdots, wsrl'_{\underset{length=m_9}{HH_3}}\}$ 组合，生成 $wsrl'\in[-1,1]$。

(4)按照嵌入算法中的映射函数将 $wsrl'$ 还原，生成最终从图像 I′中提取出的水印信息 ws'。

将提取出的水印信息转化为水印信号 $ws'(t)$ 送入响应子系统，按图 2 所示原理恢复水印图像 w'。

3 实验结果与分析

本文算法在 MATLAB 中进行仿真。原图像为 512×512 位的灰度图像 Barbara，水印图像为 16×16 位的灰度图像 yin。驱动系统为(2)式所表示的系统，以 x 作为驱动信号的响应子系统为(3)式所示系统，以 y 作为驱动信号的响应子系统为(4)式所示系统，混沌同步部分用四阶龙格-库塔法在 Simulink 中进行仿真。控制信号 $cs(t)$ 中 1 bit 码宽 T 的取值应该大于驱动系统与响应系统达到同步的时间。在混沌模型及参数确定的情况下，采用离散时间驱动的同步轨道误差与 $\frac{T}{t}$(t 为驱动信号的采样周期)成反比关系，但 $\frac{T}{t}$ 越大生成的水印信号量也越大，嵌入水印后载体图像的质量也越差。综合考虑同步误差及原图像承载水印信息的能力，实验中，选取 $T=6$，$t=0.02$ 可达到比较好的效果。水印嵌入算法中的强度因子 α，HL_1、LH_1、HH_1 部分取 $\alpha_1=0.1$；HL_2、LH_2、HH_2 部分取 $\alpha_2=0.2$；HL_3、LH_3、HH_3 部分取 $\alpha_3=0.3$。

3.1 不可见性

加入水印信息的载体图像要求具有一定的不可见性，一般常使用峰值信噪比来衡量原图像与嵌有水印图像之间的差别。本算法的峰值信噪比为 $PSNR=45.629\ 1$ dB，由此可见该算法具有良好的不可见性。原始图像与嵌有水印图像对比如图 5 所示。

(a)水印图像　(b)无失真提取的水印图像

(c)原图像　(d)嵌入水印图像

图 5　原图像与嵌入水印图像对比图

3.2 健壮性

(1)抗噪声干扰

加入噪声是对水印算法的一种常见攻击，本实验对嵌入水印的图像分别添加均值为 0、不同方差的高斯噪声。以 Matlab 提供的 corr2 函数作为判断函数，用数值的形式说明，加噪后提取出的水印信息与嵌入水印时信息的一致性，结果如表 1 所示。

表 1　添加高斯噪声后的水印提取

方差	0.005	0.01	0.02
提取出的水印			
cor	0.886 5	0.820 1	0.776 9

(2)抗图像几何处理

常用的图像几何处理攻击有剪切、JPEG 压缩、滤波等。图 6 给出含水印载体图像被剪掉部分信息后，水印图像的提取情况。

(*cor*=0.906 0)

(a)32×32 像素被剪切后提取出的水印图像

(*cor*=0.641 1)

(b)64×64 像素被剪切后提取出的水印图像

(*cor*=0.754 7)

(c)被任意剪切后提取出的水印图像

图 6　不同剪切尺寸下提取的水印图像

本算法对剪切、JPEG 压缩及滤波等几何处理有一定的抗攻击能力。

3.3 安全性

(1)结合混沌同步原理，将水印图像加载于混沌信号

中形成水印信号，混沌信号的非周期性连续宽带频谱，类似噪声的特性，使其具有天然的隐蔽性，增强了水印信号的安全性。

(2)最终的水印信号由混沌信号加随机噪声生成，随机噪声的加入使攻击者无法从信号 $ws(t)$ 中分离信号 $os(t)$，也就无法重构原系统的相空间，进而无法恢复水印图像。

(3)由于混沌信号的生成采用了离散时间驱动，保留了混沌载波的类噪声特性，因而仍可很好地掩盖信息信号的频谱，增强了水印信息的安全性；由于所包含的动力学特征因离散化而大大减少，从而有效地防止了基于预测法的攻击[7]。

本文提出了一种基于混沌同步原理的非对称数字水印构造方法，将二值水印图像转化为二进制数字信号，控制驱动系统在 $x(t)$、$y(t)$ 两路信号中作选择性输出，并将载有水印信息的混沌信号 $ws(t)$ 作为最终水印信息嵌入载体图像；水印图像恢复过程中，将提取出的水印信息转化为水印信号，送入两个响应子系统，根据响应子系统 I、II 的输出信号 $x'(t)$、$y'(t)$ 在某时刻 t 与水印信号 $ws'(t)$ 的相关性来恢复水印图像。其中，驱动系统的类型、各参数值及状态变量初值可作为水印嵌入过程所需要知道的信息或密钥；响应子系统的类型、各参数值及状态变量初值可作为水印提取过程所需要知道的信息或密钥。该算法可抵抗一定强度的噪声干扰和预测性攻击。在实际应用中，由于载体图像承载水印信息量有限，水印图像不宜过大。

参考文献

[1] 邹潇湘，李锦涛.非对称数字水印技术研究[J].计算机工程与应用，2002(16)：7-10.

[2] 关新平，范正平，陈彩莲，等.混沌控制及其在保密通信中的应用[M].北京：国防工业出版社，2002.

[3] PECORA L M，CARROLL T L.Synchronization in chaotic system[J].Phys Rev Lett，1990，64(8)：821-824.

[4] AMRITKAR R E，CUPTE N.Synchronization of chaotic orbits：effect of finite time step[J].Phys Rev E，1993，47(6)：3889-3895.

[5] 陈关荣，吕金虎.Lorenz 系统族的动力学分析、控制与同步[M].北京：科学出版社，2003：215-217.

[6] 强浩.混沌同步及其在保密通信中的应用[D].南京：南京理工大学，2004(6)：57-59.

[7] 罗晓曙，汪秉宏.一种基于混沌渐近同步的数字保密通信方法[J].通信学报，2003，24(1)：60-65.

(收稿日期：2009-02-11)