第34卷 第17期 计 算 机 工 程 2008年9月
Vol.34 No.17 Computer Engineering September 2008
·安全技术· 文章编号：1000—3428(2008)17—0158—04 文献标识码：A 中图分类号：TP301.6

基于超混沌迭代的双重零水印算法

李 帅，王卫星
（重庆邮电大学计算机科学与技术学院，重庆 400065）

摘 要：提出一种用超混沌迭代产生的序列进行加密的双重零水印算法，用图像离散余弦变换和小波变换后的重要系数分别构造零水印，以提高水印算法的抗攻击能力，采用超混沌序列进行加密，以提高系统的安全性。实验结果表明，该算法提高了水印系统的综合性能，具有较好的不可见性、鲁棒性和安全性。

关键词：超混沌迭代；双重零水印；不可见性；鲁棒性；安全性

Double Zero-watermarking Algorithm Based on Hyperchaotic Iteration

LI Shuai, WANG Wei-xing
(Collage of Computer Science & Technology, Chongqing University of Posts & Telecommunications, Chongqing 400065)

【Abstract】 This paper presents a double zero-watermarking algorithm based on transform domain and hyperchaotic iteration. It uses the important coefficients of Discrete Cosine Transform(DCT) domain and Discrete Wavelet Transform(DWT) domain to constructure zero watermarkings separately, uses a hyperchaotic sequence to encrypt, so that the robustness, invisibility and security are improved. Experimental results show that the algorithm improves the integrated performance of the watermarking system.

【Key words】 hyperchaotic iteration; double zero-watermarking; invisibility; robustness; security

1 概述

数字水印技术作为一种数字信息的版权保护技术被提出之后，很好地解决了数字化产品的产权保护等问题，并且得到更深入的研究和更广泛的应用[1]。目前数字水印技术的难点集中在：如何隐藏大量信息，保证水印本身的鲁棒性和安全性，又不破坏原文件。针对这一问题，文献[2]提出了零水印算法，其主要思想是利用宿主信息的重要特征构造可唯一识别的水印。由于零水印技术没有向宿主文件嵌入任何信息，因此很好地保证了不可见性。而零水印与常规水印算法一样，要对各种攻击保证良好的鲁棒性，目前主要的技术是基于时空域和变换域的算法。后者由于运算速度快且抗噪声、抗压缩等方面的性能较好，因此研究和应用得更为广泛。

由于离散余弦变换(Discrete Cosine Transform, DCT)和离散小波变换(Discrete Wavelet Transform, DWT)域的数字水印对于不同的攻击鲁棒性各有优势，因此应在实际应用中将两者更好地结合。有人曾提出双水印技术，即在宿主文件的变换域中选择不同频带嵌入水印信息。有理论研究表明，将水印信号直接嵌入到DCT域的DC分量或小波域的LL子带，可以更好地实现水印信号的稳健嵌入[3-5]。本文基于零水印技术提出了双重零水印的算法，并结合超混沌迭代系统对水印信号进行加密。通过仿真实验证明该技术可以大大提高系统的整体性能，有效保证数字产品的安全性。

2 超混沌迭代序列加密

1963 年，美国气象学家 Lorenz 提出混沌理论，认为气候本质上是不可预测的，最微小的条件改变都会导致巨大的天气变化，即著名的“蝴蝶效应”。此后混沌在各个领域得到了不同程度的应用。20 世纪 80 年代末，混沌序列开始应用于密码学方面，之后得到了一定的发展，并且由于具有伪随机性、数量多、容易生成等优良特性而越来越受重视。但由于采用一维混沌系统加密易被混沌同步分析法破译，因此本文采用二维超混沌系统对水印进行加密，极大地提高了系统的安全性。

2.1 混沌加密

混沌加密基于混沌系统所具有的特性：对初值的极端敏感性和高度的随机性。混沌加密的原理与序列密码的原理相似，不同点在于：一般的序列密码是以移位寄存器为基础电路来产生伪随机序列作为密钥序列的，而混沌加密是以混沌系统产生混沌序列作为密钥序列的，利用该序列对明文加密，密文经信道传输，接收方用混沌同步的方法提取明文信号，实现解密。

混沌序列加密的主要特点是加密方式简单，只要对 2 个序列进行叠加即可。混沌序列加密原理如图 1 所示。

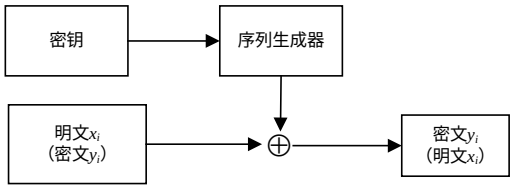


图 1 混沌序列加密原理

在实际应用中，可以根据需要采用低维混沌系统、高维混沌系统甚至时空混沌系统产生混沌信号流，以对信息进行加密。由于混沌信号具有类随机性，特别是高维超混沌信号和时空混沌信号，随机性更大，因此经过混沌加密的信号即

作者简介：李 帅(1983－)，女，硕士，主研方向：图像处理，信息安全；王卫星，教授、博士

收稿日期：2008-07-10 **E-mail：**baishui0317@163.com

使被盗版人员获取，也很难被破解。即使可以被破解，也需要很长时间。这样，利用保密信息的时效性也可以达到保密的目的。

2.2 超混沌序列

超混沌是一类特殊的混沌现象，它和混沌相比具有更多方向的不稳定性。一般，系统的状态变量愈多，可能出现不稳定的程度就愈高。所以，从实际应用的角度考虑，更希望用超混沌序列作为随机码来提高系统的安全性；但采用高维系统产生超混沌序列较之低维系统计算更复杂，实际应用中通常寻找系统状态变量参数尽可能少的超混沌系统。

二维超混沌离散系统一般有如下形式：

$$\begin{cases} x_{n+1} = m_1 + m_2 x_n + m_3 x_n^2 + m_4 y_n + m_5 y_n^2 + m_6 x_n y_n \\ y_{n+1} = m_7 + m_8 x_n + m_9 x_n^2 + m_{10} y_n + m_{11} y_n^2 + m_{12} x_n y_n \end{cases} \tag{1}$$

其中， m_i (i=1, 2,⋯, 12)为待定常系数。

用 λ_L 作为确定混沌和超混沌系统的判据，按照相应的参数选择准则，可以得到如下的简单二维超混沌系统：

$$\begin{cases} x_{n+1} = m_4 y_n + m_5 y_n^2 \\ y_{n+1} = m_8 x_n + m_{10} y_n \end{cases} \tag{2}$$

按照上述参数生成的超混沌方程可以产生二维伪随机混沌序列，由于用变换域特征参数构造的水印序列是一维的，因此还要对这个二维伪随机序列进行降维处理。假定输出的二维序列为

$$x(n) = [x(1), x(2), \cdots, x(N)]$$

$$y(n) = [y(1), y(2), \cdots, y(N)]$$

降维后输出的伪随机序列为

$$L(n) = [L(1), L(2), \cdots, L(N)]$$

仿真实验中发现，如果仅仅令

$$L(n) = x(n)$$

或者

$$L(n) = y(n)$$

得到的超混沌序列数值点的分布在边界处较为稠密，无法得到扩散度比较理想的随机分布序列点。由初值到经迭代得到的结果已经是伪随机序列，在不破坏它们整体分布的情况下，可采用如下降维模型：

$$L(n) = a_1 x(n) + b_1 + a_2 y(n) + b_2 \tag{3}$$

通过大量的仿真实验发现，采用如下参数的降维模型生成的序列扩散均匀度比较理想：

$$L(n) = \frac{x(n) - y(n) + 1.5}{2.5} \tag{4}$$

采用此降维模型生成 2 000 个点的一维随机序列码如图 2 所示。

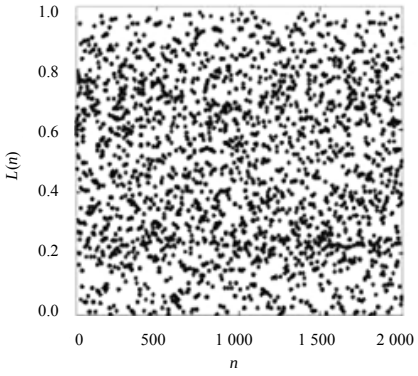


图 2 超混沌序列降维后的一维伪随机序列码

为了验证按照以上方案所产生的伪随机序列的扩散度是否理想，又对目前常用的一维 Logistic 混沌序列做了实验仿真，其动力学方程定义为

$$x_{n+1} = \mu x_n (1 - x_n)$$

其中， μ 称为分枝参数，当 $x_n \in (0,1)$ 且 3.569 945 $6 < \mu \le 4$ 时，Logistic 映射工作于混沌态。本文取 $\mu = 3.9$ 、初值密钥 $x_0 = 0.4$ 来产生 2 000 个点的 Logistic 混沌序列，如图 3 所示。

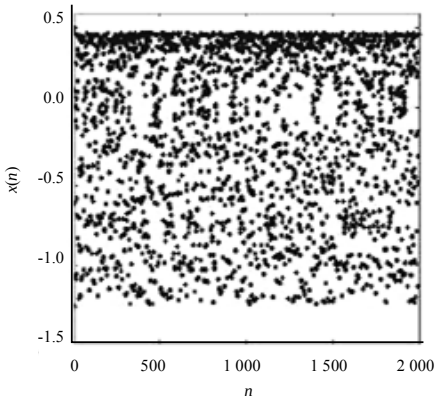


图 3 Logistic 混沌映射产生的伪随机序列码

可以明显看出，二维超混沌序列降维后生成的伪随机序列比直接用普通混沌模型生成的一维序列码的随机扩散度好，为以后对水印进行加密以提高系统的安全性提供了良好的基础。

3 基于变换域的双零水印算法

(1)生成超混沌伪随机序列

在仿真实验中，先固定m_5= −1.2, m_8= −1.1, m_{10} =0.1；经多次实验发现，当m_4 =1.52 时，系统已经进入超混沌状态，则式(1)可以写成

$$\begin{cases} x_{n+1} = 1.52 y_n - 1.2 y_n^2 \\ y_{n+1} = -1.1 x_n + 0.1 y_n \end{cases} \tag{5}$$

按照该二维超混沌方程产生的二维超混沌相空间如图 4 所示。

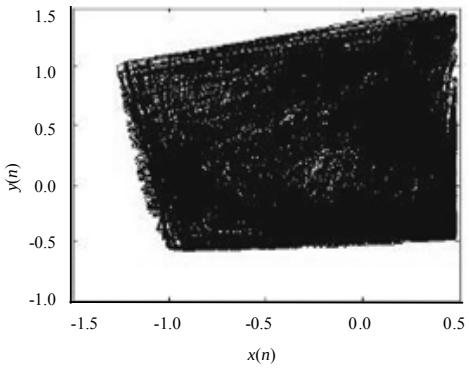


图 4 二维超混沌相空间

按照式(5)构造超混沌序列，并由式(4)的降维模型将二维超混沌序列转换为长度为 $N \times N$ 的一维超混沌伪随机序列，然后由实值序列转换为二值序列。转换方法主要有阈值门限法、多种量化法等，本文采用的是阈值门限法，且设定阈值为 0.5，经过下面的映射得到混沌二值序列。

$$L(i) = \begin{cases} 1 & \text{if} \quad 1 \ge f(i) \ge 0.5 \\ 0 & \text{if} \quad 0 \le f(i) < 0.5 \end{cases} \tag{6}$$

其中，$1 \le i \le N \times N$。

再根据本文设计的降维模型，将二维序列转换成 $N \times N$ 的一维随机序列。

(2)DCT 域构造零水印

经实验分析，DCT 变换后的能量分布图像的主要能量集中在左上角，即 DCT 变换后的低频部分。这表明人眼视觉系统对 DCT 系数低频部分的改变很敏感，如果对图像的篡改要达到视觉无法察觉的效果，必须避免对低频系数的改动。因此，本文选择这一部分重要系数进行特征水印的构造，以充分保证零水印的鲁棒性。

主要步骤如下：

1)对所选图像进行 DCT 变换，得到其 DCT 变换矩阵。并选择左上角的 $N \times N$ 个系数。

2)将所选取的 $N \times N$ 个 DCT 系数序列经过以下映射转换成 0,1 序列。

$$W_{\mathrm{DCT}}(i)=\begin{cases}1 & \text{if } C(i)>0\\ 0 & \text{if } C(i)\le 0\end{cases} \tag{7}$$

其中，$1 \le i \le N \times N$。

3)通过超混沌迭代系统降维得到的一维随机序列与上述 0, 1 序列进行按位异或，从而对水印信息进行加密，构造成零水印。

(3)DWT 域构造零水印

本算法对图像进行小波变换时采用 Haar 小波，因为 Haar 小波的支撑长度最短，它的分解和重构计算复杂度远低于其他小波，且 Haar 小波是对称的，可以减少量化误差，不会导致边缘错位，在边界点也不需要周期延拓，所以在用作数字水印方面，Haar 小波优于其他小波。

主要步骤如下：

1)对原图像进行 3 级小波变换。由于是零水印，没有对原图像嵌入任何信息，不会影响图像的视觉效果，因此选择携带了图像最重要信息的 3 阶子带的 LL 子带(即逼真子带)系数进行构造。

2)对所取的 $N \times N$ 个系数用下列映射转换为 0, 1 序列。

$$W_{\mathrm{DWT}}(i)=\begin{cases}1 & \text{if } C(i)\ge C_{\mathrm{mean}}\\ 0 & \text{if } C(i)< C_{\mathrm{mean}}\end{cases}$$

$$C_{\mathrm{mean}}=\frac{\sum_{i=1}^{N\times N}C(i)}{N\times N}$$

其中，$1 \le i \le N \times N$。

3)通过超混沌迭代系统降维得到的一维随机序列，与该 0, 1 序列进行按位异或得到零水印。

4 水印检测及实验结果分析

水印检测算法的基本步骤与构造算法完全相同，根据待检测图像所有者提供的密钥，由式(5)确定超混沌序列，由式(4)降维得到一维序列，由式(6)映射得到二值序列，再与待检测图像进行 DCT 及 DWT 变换得到的二值序列进行按位异或，得到特征水印 W_{DCT}' 和 W_{DWT}'，长度为 $N \times N$。按位比较原始水印 W_{DCT} 与 W_{DWT}'、W_{DWT} 与 W_{DWT}'，计算两者中元素相同的个数 C，则其相似度 SIM 可以定义为：$SIM=C/N$。给定一个阈值 T，如果 $SIM>T$，则认为检测图像中含有原始特征水印，图像的版权属于该图像提供者，否则认为图像不具有原始特征水印，图像的版权与其无关。经大量测试实验，将阈值 T 定为 0.5。

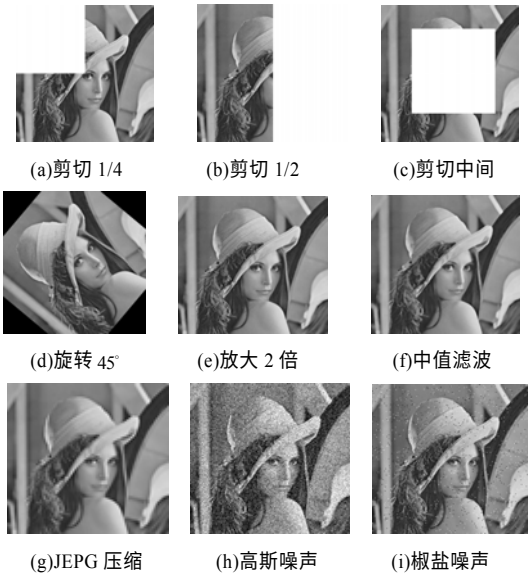
实验采用的是 256×256 的灰度图像 Lena，如图 5 所示，对其分别进行 DCT 变换和 3 级小波变换，然后进行水印嵌入，即提取重要参数构造零水印。图 6 为文献[3]的水印算法，对图像进行 DCT 分解，并加入高斯水印。可以看出，文献[3]的水印算法对原图信息破坏较大，甚至产生了严重的方块效应，而本文算法所构造的零水印由于没有向其嵌入任何数据，因此原始图像没有任何失真。

图 5　原始 Lena 图像

图 6　以文献[3]算法加入水印的 Lena 图像

(1)对水印图像的各种攻击

对原始 Lena 图像进行剪切、旋转、缩放、中值滤波、加高斯、椒盐噪声等攻击，如图 7 所示。



(a)剪切 1/4　(b)剪切 1/2　(c)剪切中间

(d)旋转 45°　(e)放大 2 倍　(f)中值滤波

(g)JEPG 压缩　(h)高斯噪声　(i)椒盐噪声

图 7　对原始图像进行攻击所得图像

由密钥提取特征水印 W' 并与原始水印 W 进行对比，得到各种攻击下的 DCT 及 DWT 的 2 个零水印的相似度 SIM 如表 1 所示。

表 1　各种攻击下所提取水印的相似度

	剪切 1/4	剪切 1/2	剪切中间	旋转 45°	放大 2 倍	中值滤波	JEPG 压缩	加入高斯噪声 (0.00, 0.02)	加入椒盐噪声 (0.00, 0.02)
SIM_{DCT}	0.869 1	0.691 4	0.671 9	0.521 5	0.987 3	0.992 2	0.991 2	0.931 6	0.948 2
SIM_{DWT}	0.671 9	0.658 2	0.552 7	0.573 2	-	0.993 2	0.994 1	0.970 7	0.979 5
系统 SIM 值	0.869 1	0.691 4	0.671 9	0.573 2	0.987 3	0.993 2	0.994 1	0.970 7	0.979 5

对上述数据进行综合分析得到各种攻击下水印的相似度曲线，如图 8 所示。由此可以更直观地看出：系统的 *SIM* 值由双水印中 *SIM* 较高的数值确定。系统综合了 DWT 和 DCT 域变换各自的优点，效果更好，尤其针对缩放这类攻击，仅凭DWT域的水印技术无法检测，此时系统可由DCT域的 *SIM* 值判断版权归属，体现了多重水印技术对多种攻击的适应性和先进性。

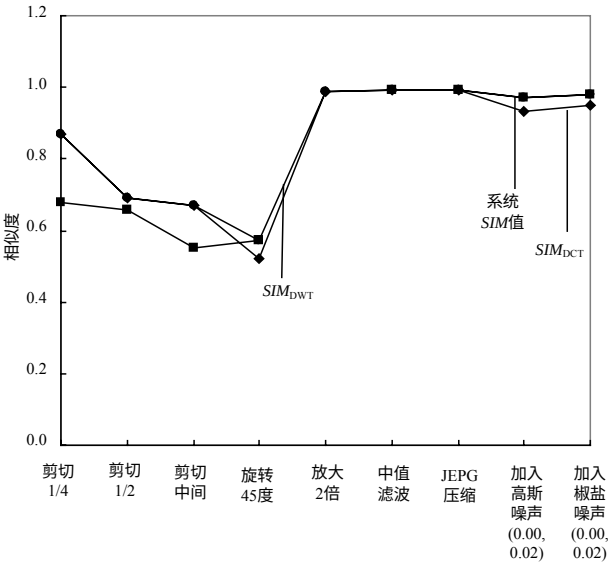


图 8　系统在各种攻击下的 *SIM* 曲线

(2)添加高斯噪声和椒盐噪声攻击

为进一步验证本算法的鲁棒性，以高斯噪声和椒盐噪声为例，图像添加的噪声密度设置在 0.02~0.30 间，向图像中添加密度占全部像素 30%的噪声对图像的视觉效果影响非常大。目前水印研究中对图像降质的度量均借鉴图像压缩的方法，即通过峰值信噪比

$$PSNR = 10\lg\frac{E_{\max}^2 \times W_X \times H_X}{\sum\left[X_{i,j} - X'_{i,j}\right]^2}$$

来衡量图像的质量。*PSNR* 值越大，图像的质量越好，通常 $PNSR > 30$ dB 时，不会使人感到图像质量的变化。当噪声参数达到 0.30 时，其图像质量下降非常大，*PSNR* 远小于 30 dB，如图 9、图 10 所示。图像重要信息大部分被破坏，但由表 2 可看出，本系统的 *SIM* 值仍能达到 0.898 4~0.923 8，且综合表 1 的数据分析，本算法构造的水印系统对于此类攻击鲁棒性很高，完全可以保证版权识别的可靠性。

图 9　加入参数为 0.30 高斯噪声的 Lena 图像

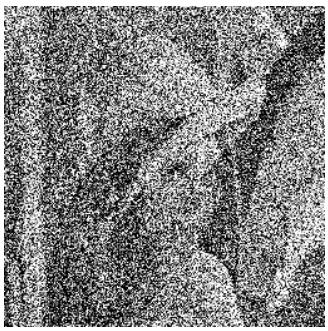


图 10　加入参数为 0.30 椒盐噪声的 Lena 图像

表 2　添加高斯噪声、椒盐噪声得到的系统 *SIM* 值

噪声类型	系统 *SIM* 值						
	0.02	0.04	0.06	0.08	0.10	0.12	0.14
高斯	0.968 8	0.956 1	0.945 3	0.943 4	0.937 5	0.937 5	0.925 8
椒盐	0.979 5	0.983 4	0.970 7	0.966 8	0.965 8	0.965 8	0.959 0
噪声类型	0.18	0.20	0.22	0.24	0.26	0.28	0.30
高斯	0.922 9	0.903 3	0.913 1	0.895 5	0.881 8	0.904 3	0.898 4
椒盐	0.938 5	0.947 3	0.945 3	0.929 7	0.938 5	0.926 8	0.923 8

由实验数据可以看出，对于缩放攻击，基于小波变换的零水印是无法检测的，必须将图像缩小到原来的大小，才可以进行特征水印的提取，而此时基于 DCT 变换的算法得到的相似度达 0.987 3，完全可以进行版权的归属判断。对于中值滤波、JEPG 压缩、添加噪声等攻击，DWT 域变换的 *SIM* 值更高，系统可以凭借这些数据进行版权的判定。而对于剪切 1/4 图像、1/2 图像、剪切中间部分以及旋转 45 ° 等较为严厉的几何攻击，可以利用 DCT 域变换的优势进行判断，从而大大提高了系统的整体鲁棒性。

5　结束语

本文基于超混沌迭代的双重零水印算法用图像的重要信息构造特征水印而不嵌入任何信息，使水印的不可见性达到最优，并充分利用这 2 种变换各自的优势提高了抗攻击能力，解决了单一水印对某种攻击无法检测的问题，保证了水印的鲁棒性。采用超混沌迭代序列进行加密，极大地提高了系统的安全性。从水印系统的综合参数考虑，该算法提高了水印系统的整体性能，为水印系统的研究提供了新思路。

参考文献

[1] 邵利平, 覃　征, 衡星辰. 一种基于图像置乱变换的空域图像水印算法[J]. 计算机工程, 2007, 33(2): 122-124.

[2] 杨树国, 李春霞, 孙　尧, 等. 基于小波变换的零水印方案[J]. 中国图像图形学报, 2003, 6(8): 664-669.

[3] 黄继武, 程卫东. DCT 域图像水印: 嵌入对策和算法[J]. 电子学报, 2000, 28(4): 57-60.

[4] Huang Jiwu, Shi Yunqing, Shi Yi. Embedding Image Watermarks in DC Components[J]. IEEE Trans. on Circuits and Systems for Video Technology, 2000, 10(6): 974-979.

[5] 黄达人, 刘九芬, 黄继武. 小波变换域图像水印嵌入对策和算法[J]. 软件学报, 2002, 13(7): 1290-1297.