基于混沌加密的数字水印新方法研究

李莉[1]，刘远富[1]，薛春艳[2]，翟宏宇[1]

（1.长春理工大学 计算机科学技术学院，长春 130022；2.厦门大学 软件学院，厦门 361005）

摘 要：本文提出一种基于混沌加密的频率域数字图像水印新算法。将含有版权信息的二值图像作为水印，利用混沌密码对其进行加密。利用人类视觉系统(HVS)的特性，实现了水印在原始宿主图像小波域中的自适应嵌入。实验结果证明了对常见噪音和图像处理算法，该水印具有良好的不可见性和鲁棒性。

关键词：混沌；DWT；HVS；二值图像数字水印；信息隐藏

中图分类号：TN919.81 **文献标识码**：A **文章编号**：1672－9870（2008）03－0155－03

A New Methodological Research on Chaotic Encryption Based Watermarking

LI Li[1], LIU Yuanfu[1], XUE Chunyan[2], ZHAI Hongyu[1]

(1.School of Computer Science and Technology, Changchun University of Science and Technology, Changchun 130022;
2.Software Institute of Xiamen University, Xiamen 361005)

Abstract: In this paper, we propose an image digital watermarking algorithm based on chaotic encryption in frequency domain. A binary image carrying copyright information is used as watermarking and is encrypted by a chaotic sequence cipher before it is embedded. Using characteristics of human visual system (HVS), watermark is embedded into the original image in DWT domain. The experimental results show that the watermarks are invisible and robust against noises and common image processing methods.

Key words: chaotic; DWT; HVS; binary image digital watermark; information hiding

随着多媒体存储技术、传输技术的进步和网络技术的日益完善，数字媒体应用的迅速增长，数字媒体的版权保护问题成为研究的热点。目前，现有的解决办法就是加密算法和水印技术。本文将研究定位在有意义水印上，并主要考虑图标形式的水印。并选择了频域技术中的小波变换（DWT）技术。同时，考虑到传统方式的水印嵌入后容易遭到攻击，并被攻击方获取水印，所以，本文采用混沌方法对水印先加密之后再嵌入的方案。

1 理论分析

混沌理论及混沌现象是非线性科学研究中最重要的组成部分之一。混沌现象是在非线性动力学系统中出现的确定性的、类随机的过程。这种过程非周期、不收敛但有界，并且对初始状态具有极其敏感的依赖性，即初始状态只有微小差别的两个同构混沌系统在较短的时间后就会产生两组完全不同的、互不相关的混沌序列值。混沌信号具有天然的随机性，特别是经过一定处理后的混沌信号具有非常大的周期和优良的随机性，完全可以用来产生符合安全性要求的序列密码。更重要的是，通过混沌系统对初始状态和参数的敏感依赖性，可以提供数量众多的密钥。根据混沌系统的上述特点，可以用其产生序列密码。

嵌入水印的图像可能遭遇一些信号处理或噪声干扰而导致失真。不论何种情况，均可视为在嵌入

收稿日期：2008－06－22
作者简介：李莉（1963－）女，教授，主要从事计算机软件及应用的研究，E-mail：LL@cust.edu.cn。

水印的图像上叠加噪声。为了使嵌入的信号能被正确检测，噪声越强，允许嵌入的信号的量越小。非平稳信号的频率是随着时间变化的，分为慢变和快变两部分。慢变部分对应着信号的低频部分，代表信号的主题轮廓，而快变的部分对应信号的高频部分，表示信号的细节，与此相似，图像也分解为两个部分：低频部分和高频部分，他们分别相对于图像的轮廓边缘和细部纹理。在这一基础上发展出了图像分解与重构的一个著名的塔式算法，其基本思想是：将原整幅图像$f(x，y)$视为一个分辨率为$2^0=1$的离散逼近A_0f，它可以分解为一个较低分辨率2^{-J}的逼近A_jf与若干个高分辨率$2^{-J}(0<j<J)$的逐次细节逼近D_jf之和。在塔式算法的启发下，结合多分辨率分析，Mallat 提出了信号的塔式多分辨率分解与重构算法，即 Mallat 算法。

2 基于DWT的混沌加密图像水印算法

算法主要包括三部分：图像水印的混沌加密、水印的嵌入和提取。

2.1 图像水印的混沌加密

本文研究选取 Lorenz 系统，其动力学方程为

$$\begin{aligned}\frac{dx}{dt}&=a(y-x)\\ \frac{dy}{dt}&=-xz+yx-y\\ \frac{dz}{dt}&=xy-bz\end{aligned}\qquad(1)$$

混沌二进制序列密码的产生分两步：首先，用四阶龙格库塔法对 Lorenz 方程进行数值积分，得到随机性好的连续数值序列$x(nT)$，其中T为数值积分算法的步长；然后，用一个量化函数对上述连续数值序列$x(nT)$进行量化处理，产生二进制 0−1 序列。其计算机仿真结果表明，在其值域$x(nT)$区间是均匀分布的，因此可将该值域区间 16 等分，若$x(nT)\in I^i16$，则取$x_e(nT)=i-1$，($i=1$，2，3…16)。将$x_e(nT)$化成二进制数$x_{be}(nT)$，每一步将产生 4 位二进制数。以上从连续数值序列通过量化处理产生二进制序列$x(nT)$的过程，是一个不可逆变换过程，即可以用上述量化方法从$x(nT)$求得$x_{eb}(nT)$，但却不能从$x_{eb}(nT)$精确地推算出$x(nT)$，对于系统 Lorenz，由于的x值域是［−20，20］，推算的最大误差可达 40/16，这对安全性是十分有利的。

2.2 水印的嵌入与提取

设原始宿主图像为$I(i，j)(1\le i，j\le N)$，首先利用二维离散小波变换将I进行小波分解，得到不同空间、不同频率的子带图像。本文对I进行 3 级小波分解，$I_{m,d}(i，j)$表示位于分辨率为m，方向为d的子带中$(i，j)$处的小波系数，m=1，2，3，d=LL，HL，LH，HH，分别表示低频子带和水平、垂直、对角方向的高频子带图像，小波分解树如图1所示。

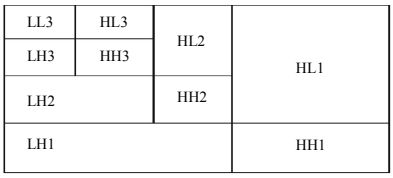

图 1 小波分解示意图

Fig.1 Demonstration of wavelet decomposition

人类视觉系统（HSV）的照度隐蔽特性和纹理隐蔽特性表明，背景的亮度越亮，纹理越复杂，人类视觉系统对轻微变化就越不敏感。因此，应该尽可能将水印嵌入到图像中满足上述条件的部位。相应于图像的小波变换域图像的纹理、边缘信息主要表现在HH，HL 和 LH细节子图中一些有较大值的小波系数上。因此可以考虑将水印嵌入到上述区域。从鲁棒性要求出发，隐藏于高频部分的信息在有损压缩等量化操作后容易丢失，所以本文选择将水印嵌入到中频子带图像HH_2，HL_2，LH_2，HH_3，HL_3和 LH_3中。为了保证水印的不可见性，水印的提取采取有源提取。其过程与水印嵌入过程相反。

3 实验结果

原始宿主图像是 512x512x256 的 Lena 标准灰度测试图像，如图 2 所示。图 3 为实验采用的 128x128x256 的图像水印 1，图 4 为实验采用的 128x128x256 的图像水印 2。图 5 为图像水印 1 混沌加密后的图像，图 6 为图像水印 2 混沌加密后的图像。试验中，从视觉不可见性、抗噪声的鲁棒性和抗一般图像处理的鲁棒性这三个方面对算法进行了检测。抗一般图像处理的鲁棒性主要从中值滤波、亚抽样、JPEG 压缩、抗锐化、抗亮度方面考查。

3.1 不可见性

如图 7 所示为嵌入混沌加密后数字水印 1 的图像，图 8 为嵌入混沌加密后数字水印 2 的图像。从视觉效果看，人眼很难分辨出嵌入水印后的图像与原图像的差别。

图 9 为从图 7 提出的数字水印图像经混沌解密之后的图像，图 10 为从图 8 提出数字水印图像经

图2　原始Lena图像
Fig.2　Original image

图 3　水印 1
Fig.3　Watermark−1

图 4　水印 2
Fig.4　Watermark−2

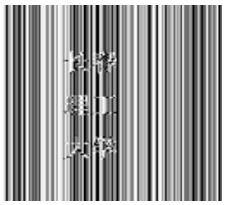

图 5　混沌加密后水印 1 图像
Fig.5　Image of watermark −1with chaotic encryption

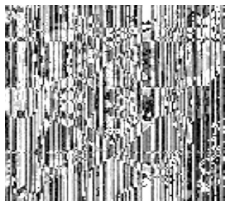

图 6　混沌加密后水印 2 图像
Fig.6　Image of watermark −2 with chaotic encryption

图 7　嵌入水印 1 的图像
Fig.7　Image encrypted with Watermark−1

图 8　嵌入水印 2 的图像
Fig.8　Image encrypted with watermark−2

图 9　提取水印 1 后的图像
Fig.9　Image of removing Watermark−1

图 10　提取水印 2 后的图像
Fig.10　Image of removing watermark−2.

图 11　加入噪声后图像
Fig.11 Image added with Noises

图 12　提出数字水印的图像
Fig.12　Image of removing Watermark.

图 13　中值滤波之后的图像
Fig. 13 Image after Median filtering

图 14　提出水印 2 后的图像
Fig.14　Image of removing watermark−2

混沌解密之后的图像。

3.2　抗噪声的强度

如图 11 所示为对图 8 加入 0.02 椒盐噪声之后的图像，图 12 为从图 11 提出数字水印图像经混沌解密之后的图像。

从图 12 和图 10 的图像对比来看，加入噪声之后的图像提取出的数字水印图像没有图 10 的效果好，不过，还是可以清晰的得到原有的数字水印。

3.3　抗中值滤波的强度

如图 13 所示对图 9 进行中值滤波之后的图像，图 14 为从图 13 提出数字水印图像经混沌解密之后的图像。

从图 14 和图 10 的图像对比来看，进行中值滤波之后的图像提取出的数字水印没有图 10 的效果好，不过，还是可以清晰的得到原有的数字水印。

实验结果表明，该算法可以有效地从嵌入水印后的载体中提取出可识别的水印图像。按照上述算法嵌入的水印信号，具有良好的不可见性，对常见的图像处理如滤波、锐化和常见的噪声干扰等具有足够好的鲁棒性。

4　结论

本文提出的一种基于 DWT 域的混沌加密图像水印算法，设计了一种包含版权信息和密钥的二值图像作为数字水印，利用混沌系列将其加密后嵌入到原始图像的 DWT 域。该水印不仅包含的版权信息量大，而且具有双重的安全性：（1）盗版者很难或者根本提取不出水印信号；（2）即使提取出水印信号，在不知道密钥的情况下，也很难恢复出原始水印图像。算法基于人类视觉系统（HVS）的亮度掩蔽特性和纹理掩蔽特性，折衷水印的不可知觉性和鲁棒性之间的矛盾。实验表明，该算法嵌入的图像水印具有视觉不可见性，并且对常见的信号处理和噪声干扰具有很好的鲁棒性。

（下转第 55 页）

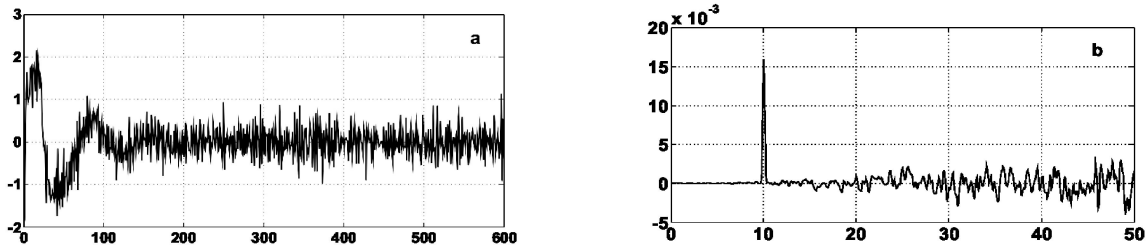

图 2　(a) 为驱动信号和响应信号的同步误差，(b) 为同步误差的互谱。

Fig.2　(a) chaotic synchronization error，(b) the cross- spectral of synchronization error

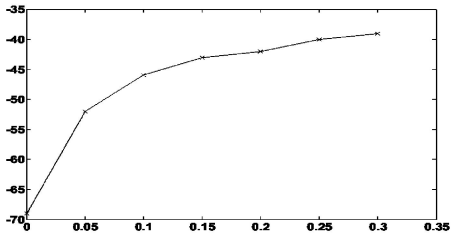

图 3 附加噪声方差与估计性能的关系

Fig.3 the variance of noise versus the estimation effect of the method

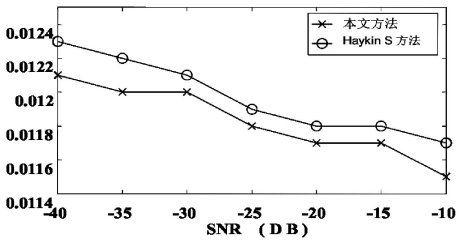

图 4　不同信噪比下本文方法与 Haykin S 法频率估计度对比

Fig.4　the estimation effect of the method versus the Haykin S method under different SNR.

立的实验。实验结果如图 4 所示，该方法频率估计精度好于神经网络相空间重构法。

4　结论

本文提出基于混沌同步的谐波频率估计方法，并给予相关理论证明。该法实现简单，计算量小。在仅有混沌噪声的背景下该方法可在 SNR=-68.2DB 时很好的估计频率，在有白噪声的情况下该法估计仍然能取得较好的估计效果。

参考文献

[1] Leung H,Huang X P.Parameter estimation in chaotic noise [J].IEEE Trans Sig Proc,1996,44:2456−2461.

[2] Haykin S,Li X B.Detection of signals in chaos [J].Proc IEEE, 1995, 83:94−98.

[3] Short K M. Steps toward unmasking secure communications [J].Int J Bif Chaos,1994,14:957−961.

[4] Broomhead D S,Huke J P,Potts A S.Cancelling deterministic noise by constructing nonlinear inverses to linear filters [J].Physical D, 1996,89:439−458,.

[5] 陈争,曾以成,付志坚.混沌背景中信号参数估计的新方法 [J].物理学报, 2008,57(1):46−50.

[6] 汪芙平,郭静波.强混沌干扰中的谐波信号提取 [J].物理学报,2001, 50(6):1019−1024,

[7] Pecora L M ,Carroll T L.Synchronization in chaotic systems [J].Phys Rev Lett ,1990,64:821−825.

[8] Hassan K,Khalil.非线性系统 [M].朱义胜,董辉,李作洲,译.电子工业出版社,2005.

(上接第 157 页)

参考文献

[1] 张彤,王育民.信息隐藏技术及其在信息安全中的应用 [J].中兴通信技术, 2002(2):42−45.

[2] 刘振华,尹萍.信息隐藏技术及其应用 [M].北京:科学出版社, 2002.

[3] 杨波.信息隐藏与数字水印 [J].信息技术, 2003,27(5):30−33.

[4] Pereira S,O'Ruanaidh J J,Pu T.Secure robust digital image watermarking using the lapped orghogonal transform [J].Proceeding of SPIE,3657.