·信号与信息处理·

基于LDPC码的Logistic混沌序列加密算法

孟祥彩,王中训

(烟台大学 光电信息科学技术学院,山东 烟台 264005)

摘 要:Logistic混沌序列是一种加密序列,增强了信息序列的安全性,将LDPC信道编码方案应用于Logistic混沌序列中。首先随机产生混沌序列,用混沌序列置乱水印,然后对水印信息进行LDPC编码调制,嵌入宿主图像DCT域中,最后实现了双重加密,从而提高了信息传输过程中的抗干扰能力,降低了误码率,增加了传输系统的稳定性。

关键词:LDPC码;Logistic混沌序列;加密

中图分类号:TN912.3 **文献标识码**:A **文章编号**:1673-1255(2017)-05-0062-03

Logistic Chaotic Sequence Encryption Algorithm Based on LDPC Coding

MENG Xiang-cai, WANG Zhong-xun

(School of Opto-Electronic Information, Yantai University, Yantai 264005*, China)*

Abstract: Logistic chaotic sequence is an encryption sequence, which enhances the security of the information sequence. At first, low density parity check (LDPC) channel coding is applied to logistic chaotic sequence. The chaos sequence is generated randomly, and the watermark is scrambled with the sequence. And then, LDPC coding modulation is applied to the watermark message which is embedded to discrete cosine transform (DCT) domain of the host image. At end, double encryption is realized. Thus, the capacity of resisting disturbance during information transmitting process is advanced, the error rate is reduced and the stability of the transmitting system is increased.

Key words: low density parity check (LDPC) coding; logistic chaotic sequence; encryption

数字通信时代的到来,让人们更加关注信息通信过程中的保密性。传统加密方式是对原始信息直接进行加密再进行传输,保密性并不理想。混沌加密算法是通过产生混沌序列,是一种伪随机序列,通过在Logistic混沌系统中进行传输,然后设置密钥进行加密,提高了系统的抗干扰能力[1]。

同时图像保密传输的需求诞生了数字水印技术,通过将水印信息嵌入到原始图像中,其不可见性实现了传输的保密性,但由于其鲁棒性较差,导致接收到的信息效果并不理想。鉴于数字水印系统和通信系统具有相似性[2-3],将信道纠错码中低密度奇偶校验(low density parity check,LDPC)码引入到数字水印中,在数字水印嵌入到原始图像之前对其进行LDPC编码并调制,然后进行传输,提高了系统的抗攻击能力。

通过以上两种保密通信各自的优越性,文中提出将LDPC码应用到Logistic混沌序列中,用产生的混沌序列置乱水印,在一级保密性的基础上再对置乱后的水印进行LDPC编码调制,然后嵌入到宿主图像的DCT域中,实现二级保密。提取水印通过LDPC码迭代译码算法得到,从而提高了系统的稳定性。

1 Logistic混沌系统特性

Logistic混沌映射系统方程式为

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

收稿日期:2017-08-02

作者简介:孟祥彩(1992-),女,山东潍坊人,硕士研究生,主要研究方向为信号与信息处理.

其中，$\mu\in(0,4]$；$x_n\in(0,1)$。Logistic混沌映射系统Lyapunov指数随参数μ的变化如图1所示。从中可以看出，$\mu\in(3.571\,4,4]$时，这个映射处于混沌状态。

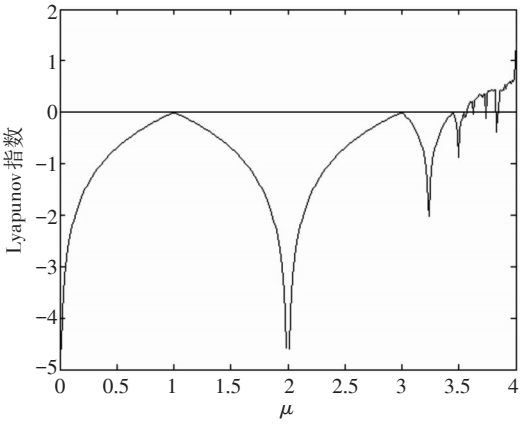

图1　Logistic映射随参数变化图

Logistic映射在参数$\mu=4$时所产生的混沌序列的统计特性跟白噪声统计特性相似[4]，其不仅有对初始值的敏感性，而且非周期性也很好，因此提高了信息序列的可靠性和安全性。因此利用Logistic映射产生混沌序列，会具有更好的保密性。

2　LDPC码概述

低密度奇偶校验(low density parity check, LDPC)码在1962年由美国Gallager教授提出，由于其性能最接近香农极限，仅差0.004 5 dB，它成为纠错码中最受热议的一种码，也被列为下一代移动通信的主流纠错码。LDPC码的关键是构造H校验矩阵，H矩阵是一种稀疏矩阵，内部元素几乎是由全零元素构成，即“1”的个数要远远小于“0”的个数，H矩阵中每一行“1”的个数称为行重，每一列“1”的个数称为列重，H矩阵的稀疏性使得行重和列重都是很小的数，且任意两行重叠数目小于1。

LDPC码可以用参数(n, r, g)定义，其中n表示码长，r表示行重(即H矩阵中每行中“1”的个数)，而g代表列重(即H矩阵中每列中“1”的个数)，如果行重与列重相等，那么称之为规则码，如果两者不相等，称之为非规则码[5]。

LDPC码的关键是构造H校验矩阵，为了达到稀疏性和译码性能的要求，需要满足以下公式

$$\begin{aligned}&r\geqslant 3,g>r,(N-K)g=Nr\\&r\ll N-K,g\ll N\end{aligned}\tag{2}$$

式中，K表示信息位；N代表常数，校验矩阵的构造需要符合以上前提条件。构造$M\times M$的稀疏矩阵H，首先通过高斯消元法，将H矩阵化为梯形矩阵，即$H=[I,P^T]$，其中P矩阵是$M\times(N-M)$，然后产生生成矩阵$G=[P^T,I]$，LDPC编码过程为$C=M\times G$。如果满足$\bar{C}H^T=0$，则译码过程正确，如果不满足，则会继续迭代译码。

3　基于LDPC码的改进加密算法

Logistic混沌映射系统不是鲁棒混沌的，在$\mu=4$左右数值时，系统的结构很不稳定，因此加密系统容易被攻击，导致加密信息出现丢失。文中提出在产生混沌序列之后，置乱数字水印信息，然后对水印进行LDPC编码及BPSK调制，再将其嵌入到原始图像的DCT域中，实现了双重加密，提高了信息传输的鲁棒性和稳定性。

图像的置乱包括位置的置乱和灰度的置乱[6]，其目的都是为了改变像素值或者灰度值，使图像在视觉上具有不可见性，进而实现图像的隐藏加密目的。利用混沌二值序列的伪随机性，使得加密的效果更好，更具有隐蔽性。

对置乱后的水印信息进行LDPC编码预处理，经BPSK调制之后，再经过扩频[7]，成为待嵌入水印，对原宿主图像进行8×8分块处理，并对每一块进行离散余弦变换DCT变换[8]，然后将扩频后的水印嵌入到原始图像中，基于HVS和DCT域的原理知识，由于人眼对低频区域感知明显，且打破了不可感知性的特征，而对高频区域不敏感，但是高频部分图像分量破坏大，因此，选择将水印信息嵌入到中频区域[9]。

在DCT域中的嵌入公式如下

$$\begin{cases}X=DCT(\tilde{X})\\X_i^{mz}=X_i^m(1+aW)\qquad(0\leqslant i<K)\\X=IDCT(\tilde{X})\end{cases}\tag{3}$$

式中，$\tilde{X}$代表分解层面系数；X代表DCT域系数；X_i^{mz}代表嵌入水印之后DCT域的最大嵌入幅度；W代表水印序列预处理；a代表嵌入强度。

改进后算法的具体流程框图如图2所示。

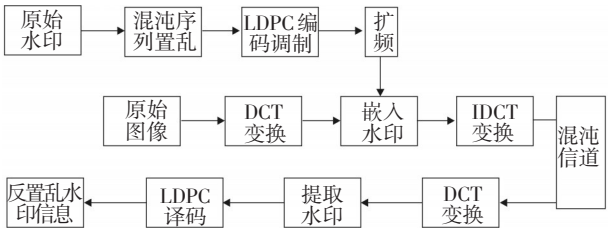

图2 水印系统框图

从图2可以看出,算法的具体流程为:首先产生随机的混沌序列,然后用混沌序列置乱原始的水印,增加了水印的不可见性,实现了一级加密。之后对置乱后的水印进行LDPC编码调制。鉴于抗干扰和安全性能的考虑,对预处理的水印信息进行扩频处理。至此,实现了对水印信息的双重加密。对原始图像进行分块DCT变换后,将处理后的水印信息嵌入中频域系数中,之后进行DCT反变换后得到嵌入水印后的图像。水印的提取过程与嵌入过程相反,同样是对传输图像做分块DCT变换,从中频域系数中提取水印,提取出水印之后再进行LDPC迭代译码处理和反置乱处理,得到估计的水印信息。

4 仿真结果分析

选取256×256的lena黑白图像为原始图像,其中LDPC码的码长为1 024,码率为1/2,编码方法采用的是Mackay构造法,最大迭代译码次数为1 000次,经过matlab仿真后,得到如图3所示的仿真图。

图3 matlab仿真图

从图3中可以看出,嵌入水印后的载体图像具有很好的隐匿性,实现了水印的隐藏,提取后的水印与原水印信息进行比较,基本上无损失。

之后对嵌入后的图像进行了攻击实验分析,包括直方图均衡攻击和添加高斯白噪声的攻击,仿真实验结果如图4、图5所示。

图4 直方图均衡化攻击图像及解密水印图像

图5 添加高斯噪声攻击图像及解密水印图像

从图4和图5中可以看出,经过两种攻击方式之后,嵌入水印后的载体图像并没有很大的破坏,图像还是清晰可见,解密之后的水印信息也几乎没有受到破坏。直方图均衡攻击后原始水印与提取水印之间的相关系数为0.957 4,而添加高斯白噪声攻击为0.947 7。这些数值和仿真效果图都体现了系统很好的鲁棒性,说明文中提出的新算法提高了系统的稳定性。

5 结 论

Logistic混沌序列是一种伪随机序列,具有很好的鲁棒性。在这个基础上,将LDPC编码调制引入,首先通过序列置乱水印,然后再对水印进行LDPC编码调制,实现了对水印信息的双重加密。通过matlab仿真实验中可以看出,此算法具有很好的鲁棒性,提高了水印在传输过程中抗干扰能力,增强了系统的稳定性,也弥补了单层加密算法的不足,具有很好的实现性。

(下转第69页)

扭矩误差等。

（2）在步进电机运行速度不同的情况下，系统误差的绝对值及变化趋势基本相同。

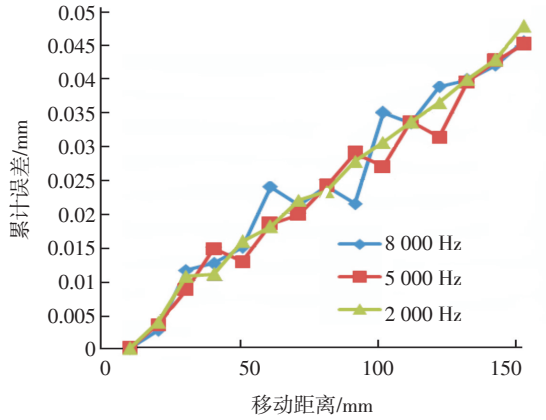

图8　系统误差图像

4　结　论

针对光学位移台的控制要求，设计了一套基于单片机ATMEG16A的步进电机驱动控制系统，采用单片机控制具有成本低、体积小、工作可靠的特点，步进电机驱动器采用专用集成芯片L293D，保证了系统的可靠性。单片机通过上电即寻零的方式，实现了位移台绝对位置寻址的功能，充分满足了光学位移台定位精度高、系统误差小的控制要求。另外，RS422模块的增加，可以实现位移台的上位机控制，以及位移台实时位置的查询的功能。

参考文献

[1] 马国利，尹学爱，郭洪岩，等. 一种基于光斑操控的光束轴向扫描新方法[J]. 光电技术应用，2015(2):8-9.

[2] 李玉虎，梁小雯，戴逸民. 利用步进电机控制偏光镜的精确定位[J]. 电子测量技术，2009，32(5)：176-178.

[3] 张晓娟，陈殿生. 假肢接受腔阳模数控加工机床的控制系统研制[J]. 机床与液压，2010，38(4)：71-72.

[4] BEVERIDE J，WIENE R. Multithreading Applications in Win32[M]. Addison-Wesley Developers Press，1997：251-252.

[5] 赵笑笑. 基于模糊理论与常规PID控制的模糊PID控制方法研究[J]. 山东电力技术，2009(6):54-56+63.

[6] 王储. 一种反射单元不对称规则采样法步进电机控制技术[J]. 光电技术应用，2016(6)：54-55.

[7] 李文仲，段朝玉. 短距离无线数据通信入门与实战[M]. 北京：北京航空航天大学出版社，2006.

[8] 华中理工大学电子学教研室. 电子技术模拟部分[M]. 4版. 北京：高等教育出版社，2004.

[9] WANG Yong, LIU Zhi-gang, BO Feng, et al. Design and control of an ultra-precision stage used in grating tiling[J]. Chinese Journal of Mechanical Engineering, 2007, 20(1): 1-4.

[10] 钱钟泰. 系统误差、偶然误差、随机误差和疏忽误差的分类方法[J]. 仪器仪表学报，1986(4)：346-351.

（上接第64页）

参考文献

[1] 王宏霞，何晨，丁科. 基于混沌映射的鲁棒性公开水印[J]. 软件学报，2004，15(8).

[2] SUI Ai-fei, LI Zhi, YAO Hui-min. The communication mode of digital watermarking system[J]. Military Communication Technology, 2004, 3(6): 1-4.

[3] ZHU Bing-lian, WANG Yan-an. Algorithm of blind checking for image watermarks based on LDPC code[J]. Journal of Chongqing University of Technology, 2010, 24(4): 7.

[4] 孙克辉. 混沌保密通信原理与技术[M]. 北京：清华大学出版社，2015.

[5] 唐田田，王中训，王岩. LDPC-CM-UEP在数字图像水印技术的应用[J]. 通信技术，2014，4(446).

[6] 邓晓衡，廖春龙，朱从旭，等. 像素位置与比特双重置乱的图像混沌加密算法[J]. 通信学报，2014(3)：216-223.

[7] INGEMAR J Cox y, JOE Kilian y, TOM Leighton z, et al. Secure spectrum watermarking for multimedia[J]. IEEE Transactions on Image Processing, 1997, 6 (12): 1673-1687.

[8] 霍智勇，朱秀昌. 基于LDPC码的数字水印技术研究与应用[J]. 中国图像图形学报，2007，12(11)：2018-2026.

[9] 王昕，袁东风. 借助LDPC码提高数字水印鲁棒性[J]. 计算机工程与科学，2006，28(8).

[10] 邵丹. 彩色图像数字水印技术[D]. 浙江：浙江大学，2004.