基于线性同余的伪随机序列图像加密

陈 帅[1,2],钟先信[1],朱士永[2],石军锋[1]
(1.重庆大学 光电技术及系统教育部重点实验室,重庆 400030;
2.淮南师范学院 物理系,安徽 淮南 232001)

摘 要:为了进行保密通信,需要对图像进行加密,采用了一种基于线性同余的序列加密方法。提出了一种基于24比特的线性同余随机序列发生器 $y(n+1)=(32719*y(n)) \bmod (16777213)$,通过独立性和均匀性检验证明了发生器产生的序列的随机性。将初始值作为密钥,产生伪随机序列,与图像像素通过异或加解密。描述了基于该线性同余随机序列的图像加解密算法。图像加密解密实验表明,序列具有参数敏感性。所提出的线性同余随机序列发生器能够正确产生伪随机序列,可以用于最大像素为2896×2896的图像加解密通信。

关键词:图像;加密;线性同余;伪随机序列发生器
中图分类号:TP309.7;TN911.73 **文献标识码**:A **文章编号**:1005-3751(2006)04-0017-02

Image Encryption Through Pseudo-Random Sequence Based on Linear Congruence

CHEN Shuai[1,2], ZHONG Xian-xin[1], ZHU Shi-yong[2], SHI Jun-feng[1]
(1. Ministry of Edu. Key Lab. of Optoelectronic Techn. & System, Chongqing Univ., Chongqing 400030, China;
2. Physics Department of Huainan Normal University, Huainan 232001, China)

Abstract: In order to encrypt communication, sequence cipher in linear congruence was used to image security. The pseudo-random sequence generator in 24 bits based on linear congruence such as $y(n+1)=(32719*y(n)) \bmod (16777213)$ was studied. The randomicity of sequences from the generator was verified through independence and uniformity. The images were encrypted and decrypted through exclusive OR algorithm of images and pseudo-random sequence coming from initial security key. The algorithm for encrypting images through sequences from linear congruence generator was described. The images encrypting and images decrypting show that the sequences are sensitive to initial parameter. The generator can produce pseudo-random sequence, and can be used to encrypt images with maximum picture pixel.

Key words: image; encryption; linear congruence; pseudo-random sequence generator

0 引 言

在嵌入式uClinux构成的图像采集与传输系统中[1,2],还需要图像的加密通信。图像的加密研究较多的是图像的置乱变换,如Arnold变换、Conway游戏、FASS曲线、Gray码变换、广义Gray码变换、IFS模型、Hibert曲线、Tangram算法、幻方变换、混沌加密等[3,4]。

随机序列在网络安全算法中被大量使用,如网络中通信双方的相互认证需要随机数来防止重放攻击;用随机数作为会话密钥;公钥密码中用随机数作为种子密钥;序列密码中用随机序列加密数据等[5]。真正随机数的产生方法有物理方法(如物理噪声),但物理方法产生的随机数难以重现,难以与应用系统连接。网络安全中的随机数都是借助于安全算法来产生,使得产生的数不是真正的随机数。算法产生的随机数序列由于表现为一定的近似随机性,因而称为伪随机序列。只要产生的序列的周期性足够长,伪随机序列就可以用于信息安全。常用的伪随机序列产生方法有:线性同余算法、基于密码算法的随机数产生器(如循环加密、DES的输出反馈模式、ANSI X9.17)、MS(Micali-Schnorr)和BBS(Blum-Blum-Shub)产生器[6]。

应用随机序列的均匀分布特性,可以将信息隐藏。图像信息可以应用随机序列进行加密和解密。然而,图像数据量大,这就需要产生周期长的随机序列。文中研究了基于线性同余的一类24比特随机数产生算法,并分析检验

收稿日期:2005-08-01
基金项目:"九七三"计划(国家重点基础研究发展规划资助项目)(G1999033105);重庆市自然科学基金资助项目(2005BB2198);重庆市科技计划资助项目(8673);安徽省高等学校自然科学研究资助项目(2005KJ092);淮南师范学院青年教师自然科学研究资助项目(2004LKQ01)
作者简介:陈 帅(1969-),男,四川蓬溪人,讲师,博士研究生,研究方向为嵌入式智能化仪器及测控系统、EDA/SOC、信息处理与网络安全;钟先信,教授,博士生导师,主要研究方向为微/纳技术、智能化仪器及机械、检测与控制系统。

了其随机性,最后应用于图像加密解密实验。

1 线性同余序列产生

线性同余为:

$$y(n+1) = (a * y(n) + b)\bmod(m) \tag{1}$$

根据数论知识,如果 m 为素数且 $b = 0$,则当 a 满足

$$\begin{cases} a^n \bmod(m) \neq 1, & n = 1,2,\cdots,m-2 \\ a^{m-1} \bmod(m) = 1 \end{cases} \tag{2}$$

时,线性同余产生的数在重复之前就能产生出0到 m 之间的所有数,称产生的数列是整周期的。如基于线性同余的随机数发生器[5]

$$y(n+1) = (16807 * y(n))\bmod(2^{31}-1) \tag{3}$$

是整周期的,且方便 32 位处理,已被广泛应用,并经过了更多检验。

为了方便处理 24 位的图像,对式(1),取 $a = 32719$, $m = 16777213$, $b = 0$,得到 24 位运算处理的线性同余序列发生器:

$$y(n+1) = (32719 * y(n))\bmod(16777213) \tag{4}$$

统计表明根据该式产生的序列周期为 8388606,由于 $\sqrt{8388606} \approx 2896$,所以该线性同余发生器产生的序列可以用于加密图像的最大尺寸为 2896×2896。

2 随机性检验

随机性通过独立性和均匀分布性两个准则来检验。

2.1 独立性

图 1 为根据式(4)产生的序列的自相关性,具有良好的近似二值特性。可见序列的独立性很好。

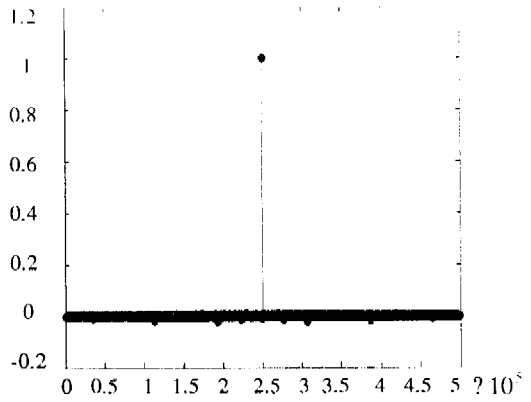


图 1 线性同余序列的自相关

2.2 均匀性

表 1 为计算长度为 10^6 的序列统计的各比特位出现 1 的总数值。可以根据皮尔逊提出的 χ^2 检验[7]来检验均匀分布性。χ^2 统计量为:

$$K_n^2 = \frac{1}{n}\sum_{j=1}^{k}\frac{(n_j - np_j)^2}{p_j} \tag{5}$$

其中 n_j 为样本 $X_i(i = 1,2,\cdots,n)$ 落在分布区间 S_j 中的个数,k 为分布区数,p_j 为分布区概率,n 为样本总数。

对于均匀分布,$p_j = \frac{1}{k}$,得:

$$K_n^2 = \frac{1}{n}\sum_{j=1}^{k}\frac{(n_j - np_j)^2}{p_j} = \frac{1}{n}\sum_{j=1}^{k}\frac{[n_j - (n/k)]^2}{1/k}$$
$$= \frac{k}{n}\sum_{j=1}^{k} n_j^2 - n \tag{6}$$

对于给定的水平 α,当 $K_n^2 > \chi^2_{k-1,\alpha}$ 时,则认为总体分布不是均匀分布在 $x_1,\cdots,x_k$ 上,否则认为是均匀分布在 $x_1,\cdots,x_k$ 上。

对于表 1,计算 $K_n^2 = 7.9928$,取 $\alpha = 0.05$,查表得 $\chi^2_{k-1,\alpha} = \chi^2_{23,0.05} = 35.172$。因为满足 $K_n^2 < \chi^2_{k-1,\alpha}$,故认为总体位是均匀分布的。

表 1 各比特位出现 1 的总数值(序列长度为 10^6)

位	1	2	3	4	5	6	7	8
出现 1 的总数值	499412	500204	499561	499736	500263	499569	499928	500644
位	9	10	11	12	13	14	15	16
出现 1 的总数值	499357	500298	500512	499554	500162	499837	499872	499951
位	17	18	19	20	21	22	23	24
出现 1 的总数值	499499	499914	500155	499536	500849	500097	499973	500646

3 图像加密算法及加解密实验

取常用的 BMP 格式图像。BMP 图像文件由表头、调色板和图像数据 3 部分组成,其中表头长度固定为 54 个字节。在图像数据区用连续的 3 个字节分别表示同一个像素点的红、绿、蓝三基色的值。

将产生的序列的每一个 24bits 的元素与图像的像素点的红、绿、蓝三基色的值进行异或运算,就得到图像加密算法:

1)给定初始密钥;

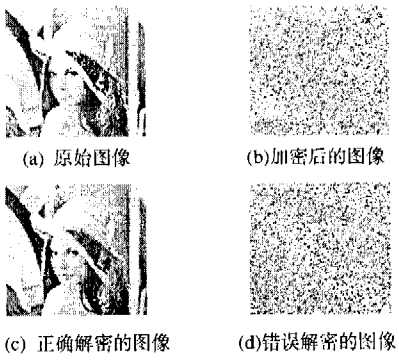
2)运用式(3)进行线性同余序列值计算;

3)取图像一个像素点,分别将红、绿、蓝三基色值与序列值进行异或运算;

4)如果取完了图像的所有像素点,结束;否则,转步骤 2)。

解密是加密的逆过程。

图 2 为图像加密解密对比图,其中(a)为原始图;(b)为初始值为 $y(1) = 128$ 产生的序列加密的图像;(c)为初始值为 $y(1) = 128$ 产生的序列对加密图像解密后的图像;(d)为用初始值为 $y(1) = 129$ 产生的序列对加密图像进行解密的图像。



(a) 原始图像 (b)加密后的图像

(c) 正确解密的图像 (d)错误解密的图像

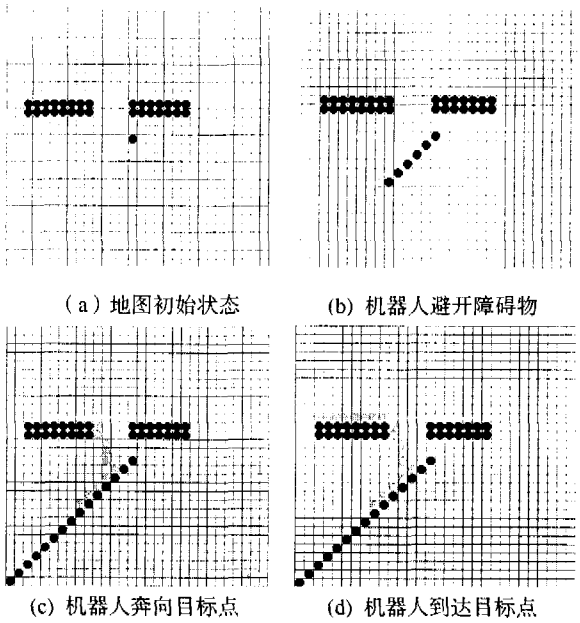
图 2 图像加密解密对比图

(下转第 21 页)

2.2 仿真分析

为了验证改进后方法的有效性和可行性,对改进后的方法进行了仿真实验,图 4 所示为改进后的仿真结果。结果显示运用改进后方法生成的路径仍可避障到达目标点,但生成路径大大缩短,是最短或是接近最短的。进一步根据改进后的算法对动态不确定环境下机器人的路径生成过程进行仿真。机器人、目标点和障碍物的初始位置如图 5(a)所示,长方形区域为静态障碍物,然后目标点以 60 个单元格/分钟的速度向左运动,动态障碍物以 60 个单元格/分钟的速度向左下方运动。如图 5(b)所示,机器人以 60 个单元格/每分钟的速度开始向右上方运动,在即将碰上迎面而来的障碍物时,机器人迅速地转向正上方避开了运动的障碍物。而后机器人如图 5(c)所示转向运动目标点,最终机器人如图 5(d)所示到达目标点。仿真结果表明该方法能对迅速变化的环境做出快速的反应,生成连续、平滑的避障路径。

由于只是在当前邻近位置中具有最大活性值的位置不惟一时,才需计算邻近位置具有最大活性值位置与目标点的距离,而不是每步都要计算,计算量虽有所增加,但复杂度仍是较低的,与其它目标制导方法相比,更加灵活,具有原神经网络模型的优点,通过引入目标制导,使生成避障路径大大缩短,所以改进方法是有效、可行的。



(a) 地图初始状态　(b) 机器人避开障碍物

(c) 机器人奔向目标点　(d) 机器人到达目标点

图 5　避开动态障碍物追踪动态目标点的路径生成

3 结　论

文中对原有基于生物激励神经网络方法进行了仿真验证的同时也发现了该方法的不足:在当前邻近位置具有最大活性值的位置不惟一时,产生路径可能不理想,到达目标点的避障路径是较长的,而不是最短或接近最短。文中对该不足进行了分析,并对改进方法进行了仿真,仿真结果说明了该方法生成避障路径最短或是接近最短,是有效的、可行的。

参考文献:

[1] 陈宗海,陈　锋.一种不确定环境下移动机器人的避障规划算法[J].机器人,2002,24(4):358－361.

[2] 童　亮,陆际联.仿真机器人足球学习方法研究综述[J].计算机仿真,2004,21(6):1－5.

[3] 郭　琦,洪炳熔.基于人工神经网络实现智能机器人的避障轨迹控制[J].机器人,2002,24(6):508－512.

[4] 马向玲,田宝国.Hopfield 网络应用实例分析[J].计算机仿真,2003,20(8):64－66.

[5] Meng M, Yang X. A neural network approach to real－time trajectory generation[A]. in IEEE Proc Int Conf Robot Automat[C]. Leuven,Belgium:[s.n.],1998.1725－1730.

(上接第 18 页)

对比图 2(c)、(d)可见,仅仅错误一个比特的错误密钥就不能解密图像,表明序列对密钥参数敏感,因此,所产生的序列对图像加密具有较强的安全性。

4 结　论

文中提出了一种 24 比特的线性同余伪随机序列发生器,并应用于图像加密。通过自相关特性的二值性说明了其独立性好,通过假设检验证明了分布均匀性。将其应用于图像加密解密,表明对初始密钥敏感,有利于增强图像加密的安全性。该序列密码可以用于最大像素为 2896×2896 的图像加解密。

参考文献:

[1] 陈　帅,钟先信,李晓毅,等.基于队列结构的嵌入式系统多进程应用[J].微机发展,2004,14(11):49－51.

[2] 陈　帅,钟先信,李晓毅,等.Linux 嵌入式网络仪器的远程图像通信系统实现[J].自动化与仪器仪表,2005(1):59－62.

[3] Qi Dongxu,Zou Jiancheng,Han Xiaoyu. A new class of scrambling transformation and its application in the image information covering[J]. Chinese in Science(Series E),2000,43(3):304－312.

[4] 鲍官军,计时鸣,张　利,等.一种基于位运算的图像加密算法[J].浙江工业大学学报,2003,31(3):315－318.

[5] 杨　波.网络安全理论与应用[M].北京:电子工业出版社,2002.

[6] 孙淑玲.应用密码学[M].北京:清华大学出版社,2004.

[7] 陆　璇.数理统计基础[M].北京:清华大学出版社,1998.