

基于新的变参数混沌系统的图像加密

周志刚¹, 李苏贵², 刘 嫒¹

(1. 郑州大学 信息工程学院, 郑州 450001; 2. 郑州大学 物理工程学院, 郑州 450001)

(tianhuook@foxmail.com)

摘 要:针对一维离散单混沌系统在计算机有限精度下存在的退化问题,提出了一种在生成混沌信号的过程中参数随机变化的混沌伪随机序列产生方法,基于该方法构建的混沌系统较单混沌系统具有伪随机序列周期大、密钥数量多、密钥空间大等优势,所产生的密码具有更高的安全性能。基于该方法,还提出了一种新的图像加密算法。仿真分析证明,该图像加密算法原理简单,安全性高,便于软硬件实现。

关键词:混沌系统;参数随机变化;伪随机序列;图像加密

中图分类号: TP309 **文献标志码:** A

Image encryption based on chaotic system with variable parameters

ZHOU Zhi-gang¹, LI Su-gui², LIU Yi¹

(1. School of Information Engineering, Zhengzhou University, Zhengzhou Henan 450001, China;

2. School of Physical Engineering, Zhengzhou University, Zhengzhou Henan 450001, China)

Abstract: Concerning the degeneracy of the computer limited precision effect in a single one-dimensional discrete chaotic system, this article proposed a method of pseudo-random sequence generation with variable parameters in the process of the generation of the chaotic signal. The constructed chaos system based on this method had some advantages, such as the long cycle of pseudo-random sequence, the large quantity of key and the big superiority of key space, and the produced password has a higher safety performance. Besides, based on the method, a new image encryption algorithm was put forward. The simulation results show that this algorithm is simple, safe and easy to meet the software and hardware requirements.

Key words: chaotic system; parameters random change; pseudo-random series; image encryption

0 引言

在当今信息社会,随着计算机网络技术的飞速发展和微型计算机的普及,越来越多的多媒体数字信息通过网络进行传输,据统计,其中图像信息约占信息总量的70%。这些信息在传输过程中的安全与保密不仅关系到个人隐私、企业的商业机密等问题甚至关系到国家安全,因此在网络中图像信息的安全与保密技术已变得越来越受到全社会的重视。

混沌是确定性系统中出现的伪随机现象,混沌系统产生的混沌序列是一种具有良好随机性、相关性和复杂性的伪随机序列,其结构复杂,难以分析和预测。混沌信号还具有对初始条件的极端敏感性、拟噪声等天然的优良密码学特性,因此基于混沌的图像加密方法具有很好的安全特性。但是,目前广泛应用于图像加密的混沌系统大部分都是基于单个一维离散混沌系统,不但密钥空间小,而且在计算机的有限数字精度下,其混沌特性存在明显的退化,从而使得生成的混沌序列退化为周期序列,而且实际生成的序列的周期和密码学特征难以度量,导致实际结果与理论结果大相径庭。

针对基于一维离散单混沌系统的缺陷,本文基于一维分段线性混沌映射 PLCM 和 Logistic 混沌映射,提出了一种参数随机变换的混沌伪随机序列产生的新方法,及基于该方法的图像加密方案。研究表明,在有限精度条件下,该方法大大增大了产生的混沌序列的周期,易于实现,加密/解密速度快;同时,由于引入了另一个参数 μ 随着迭代次数的变化在两个值

μ_1 、 μ_2 之间来回切换的混沌映射来产生混沌序列生成过程中的控制参数,增大了系统的密钥空间,极大地提高了该方案下加密系统的抗破译能力。

1 参数随机变化的一维混沌映射

通过随机改变混沌映射的参数,可以提高混沌序列的复杂性,并且在有限精度实现时,使得混沌序列的周期可用不同参数的混沌映射的数目来度量,即混沌序列的周期等于状态 $x(i)$ 的周期与参数的周期的乘积。

1.1 一个良好随机统计特性的分段线性混沌映射 PLCM

文献[1-2]提出了一个良好随机统计特性的一维分段线性迭代混沌映射,其定义如下。

$$x_{n+1} = F(x_n, p) = \begin{cases} x_n/p, & x_n \in [0, p) \\ (x_n - p)/(0.5 - p), & x_n \in [p, 0.5) \\ F(1 - x_n, p), & x_n \in [0.5, 1) \end{cases} \quad (1)$$

其中, $x \in [0, 1)$, $p \in (0, 0.5)$ 。

该迭代系统是混沌的,其输出信号 $\{x(t)\}$ 在 $[0, 1)$ 上遍历,且具有良好的自相关性和均匀分布特性。

1.2 Logistic 混沌映射

$$x_{n+1} = F(x_n, \mu) = \mu x_n (1 - x_n) \quad (2)$$

其中, $0 \leq x_n \leq 1$, $n \in \mathbb{Z}$, 当 $\mu \in [3.57, 4)$ 时,系统是混沌的。

若直接利用式(1)的迭代来产生密钥序列存在混沌参数 p 易被破解的缺陷。

收稿日期:2009-01-14;修回日期:2009-03-06。 基金项目:国家973计划项目(2007CB307102)。

作者简介:周志刚(1978-),男,河南洛阳人,硕士,主要研究方向:信息安全、混沌加密; 李苏贵(1970-),男,河南郑州人,副教授,主要研究方向:智能测控、网络安全; 刘嫒(1982-),女,四川自贡人,硕士,主要研究方向:网络多媒体、网络安全。

对于由式(1)生成的混沌序列,只要得到位于同一个分段上的任意两个(或多个)的点对 $(x(t), x(t+1))$ 、 $(x(t'), x(t'+1))$,就能确定出参数:

$$p = (x(t' + 1) - x(t + 1)) / (x(t') - x(t)) \quad (3)$$

1.3 参数随机变化的多级一维分段线性混沌系统

基于 PLCM 和 Logistic 混沌映射,本文设计了一个基于参数随机变化的多级混沌系统。如图 1 所示。

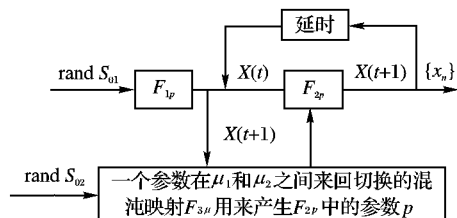


图 1 参数随机变化的混沌模型

其中, s_{01}, s_{02} 是用户随机输入的初始条件, F_{1p} 是一个按式(1)定义的一维分段线性混沌映射 PLCM 迭代 k 次后的混沌映射, 其表达式为: $x(i+1) = F^k(x(i), p)$, 其中 $k > n^{[2]}$, k 为迭代级数, F_{1p} 的初始值是用户随机输入的 S_{01} , 利用 S_{01} 作为 F_{1p} 的初始条件来生成 $x(1)$ 。 F_{1p} 用来控制 F_{2p} 的初始化和迭代过程, 其中 F_{2p} 是按式(1)定义的一个一维分段线性混沌映射 PLCM。由于是在有限精度下实现, 所以设其精度为 n , 则序列 $\{x(i)\}_{i=1}^{\infty}$ 的取值空间为 2^n 。

F_{2p} 也是一个一维线性混沌映射 PLCM, 在 $n = 16$ 精度下, 由于参数 p 的取值空间为 2^{16} 所以对不同的参数 p , F_{2p} 可以看成是不同的混沌模型。也即相当于存在 2^{16} 个一维线性混沌映射 $F(x, p)$ 。在每次迭代的过程中, F_{2p} 中的控制参数 p 是这样产生的。

1) 初始时, 随机输入一个数据 $0 < S_{02} < 1$, 计算 $F_{3\mu}(S_{02}, \mu)$, $p = F_{3\mu}(S_{02}, \mu)/3$, 其中 $\mu = \mu_1$ 或 μ_2 , $F_{3\mu}$ 是按式(2)定义的一个 Logistic 混沌映射。

2) 当 $t > 1$ 时, $p = F_{3\mu}(x(t-1), \mu)/3$, 其中 $\mu = \mu_1$ 或 μ_2 。

3) $F_{3\mu}$ 中的参数 μ 是这样控制在 μ_1 和 μ_2 之间来回切换的:把迭代次数 t 余运算正整数 m , 当运算结果为奇数时, $F_{3\mu}$ 中使用参数 μ_1 , 当运算结果为偶数时, $F_{3\mu}$ 中使用参数 μ_2 。

这就保证了在生成 $\{x(t)\}_{t=1}^{\infty}$ 的过程中,当某次迭代产生的 $x(t')$ 与之前的某次 $x(t)$ 相等时其中 $t' > t$, 与 $x(t')$ 对应的参数 p' 也以极大的概率与 $x(t)$ 对应的参数 p 不相等。只有当某次的迭代状态与之前的相同而且要使其对应的参数也与之前的相同时,混沌序列才会出现循环。在该伪随机序列发生器中,只有当 $x(t-1)$ 与 $x(t'-1)$ 相等, $x(t)$ 与 $x(t')$ 相等,而且还必须当 $t \% m$ 与 $t' \% m$ 运算得到的这两个数的奇偶性相同时,该伪随机序列才可能会进入周期循环之中。这样,混沌序列的周期即 $T = h \times 2^{2n}$, 其中 n 为精度, $h = 1, 2, 3, 4, \dots, h$ 的初始值和 m 有关。从而在有限精度实现时,输出混沌序列的周期变大,并可以度量。

2 $\{x(t)\}_{t=1}^{\infty}$ 序列转换为 0-1 序列 $\{K(i)\}_{i=N_1}^{N_2}$

把根据图 1 生成的模拟序列 $\{x(t)\}_{t=1}^{\infty}$ 用量化函数进行量化, 得到 0-1 二进制序列 $\{s(t)\}_{t=1}^{\infty}$:

$$s(t) = Q(x(t)); t = 1, 2, 3, \dots, n$$

$$Q(x(t)) = \begin{cases} 1, & x \in \bigcup_{d=0}^{2^{n'-1}-1} I_{2d+1}^{n'} \\ 0, & x \notin \bigcup_{d=0}^{2^{n'-1}-1} I_{2d+1}^{n'} \end{cases} \quad (4)$$

其中, n' 为任意正整数, $I_0^{n'}, I_1^{n'}, I_2^{n'}, I_3^{n'}, \dots$ 是区间 $[0, 1]$ 的 $2^{n'}$ 个连续的等分区间。

由于混沌序列 $\{x(t)\}_{t=1}^{\infty}$ 具有良好的随机统计特性, 这样生成的 $\{s(t)\}_{t=1}^{\infty}$ 在理论上具有均衡的 0-1 比和 δ -like 的自相关等优良的统计特性。

最后,为了进一步增加算法的随机性,提高序列的抗破解能力,使得对初始条件的攻击无效,加密时截掉序列的初始端部分和结尾部分,假设序列 $\{s(t)\}_{t=1}^L$ 的长度为 L ,任取截点 N_1, N_2 ,满足 $1 < N_1 < N_2 < L$,经过这样的处理后,得到所需要的二进制伪随机序列 $\{K(i)\}_{i=N_1}^{N_2}$,该序列的长度为 $(N_2 - N_1 + 1)$ 。

这样,本算法的保密性不但依赖于混沌系统的参数和初始条件,而且还依赖于保密系统的初始值 N_1, N_2 和随机选取的某个正整数 $m, m = 1, 2, 3, 4, 5, \dots$ 。这样,加密系统的密钥就包括 $N_1, N_2, m, n', s_{01}, s_{02}, p, p(1) \sim p(2^n), \mu_1, \mu_2$, 这就使得密码分析变得极其困难。

3 混沌系统性能分析

本文设计的混沌系统有以下优点。

1) 保证了产生的 0-1 序列满足二值分布。在迭代过程中,每次换一个混沌参数 $p(t)$, 相当于更换了一个混沌方程。由此来提高产生的混沌序列的复杂性,而且对于相同的状态 $x(t)$, 由于它所对应的参数 $p(t)$ 不同,使得它的下一个状态 $x(t+1)$ 不同。

2) 使得破解参数 p 变得异常复杂。破解一个一维分段线性混沌的参数 p 需要该混沌 2 个点对。本系统有 2^n 个不同的混沌方程。所以一个点对落入一个指定的混沌的概率为 2^{-n} , 2 个点对同时落入一个指定的混沌方程的概率为 $2^{-n} \times 2^{-n} = 2^{-2n}$, 因此, 破解本系统的一个混沌参数的复杂度是破解一维分段线性混沌映射的 2^{2n} 倍。全部破解 $p_1, p_2, p_3, \dots, p_{2^n}$ 这 2^n 个参数, 其复杂度是破解一维分段线性混沌系统的 $2^n \times 2^{2n} = 2^{3n}$ 倍。同时由于 N_1, N_2, m 的引入, 破解该混沌系统的复杂度在此基础上又得到了极大的提高, 使得到的混沌序列的随机性更强, 周期更长, 极大地增强了抗密码分析的能力。

3) 进一步增大了序列的周期。作为密码序列,其周期应该越长越好。而定参数的方法产生的序列的周期完全取决于序列 $\{x(i)\}$ 的精度。而本文采用的方法其周期由混沌参数的改变周期与 $\{x(i)\}$ 的周期的乘积来决定,即, $h \times 2^n \times 2^n = h \times 2^{2n}$ (n 为数字化精度, h 为正整数),这样产生的序列周期大大增加。而且可以度量。

4 变参数混沌系统的仿真验证

从图 2(a) 可以看出,该混沌系统在初始值 S_{01} 改变 10^{-16} 时,该混沌系统大约经历 15 次迭代之后,这两个序列就变得完全不同了,其中,实线为初值 $S_{01} = 9.501\,292\,851\,471\,754\text{e}-001$,虚线为初值 $S_{01} = 9.501\,292\,851\,471\,753\text{e}-001$,这说明该伪随机序列发生器对初始值具有极高的敏感性。由 Berlekamp-Messy 算法对该序列的线性复杂度进行分析,可从图 2(b) 看出,该序列的线性复杂度曲线趋向于独立二项同分布随机序列的复杂度曲线,约等于序列长度的一半,表现出良好的随机性,满足保密通信的要求。从图 2(c)、(d) 可以看出,该伪随机数发生器生成的二进制混沌序列 $\{k(t)\}_{t=1}^{\infty}$ 具

有类似 δ -like 的性质,有尖锐的自相关和良好的互相关性。

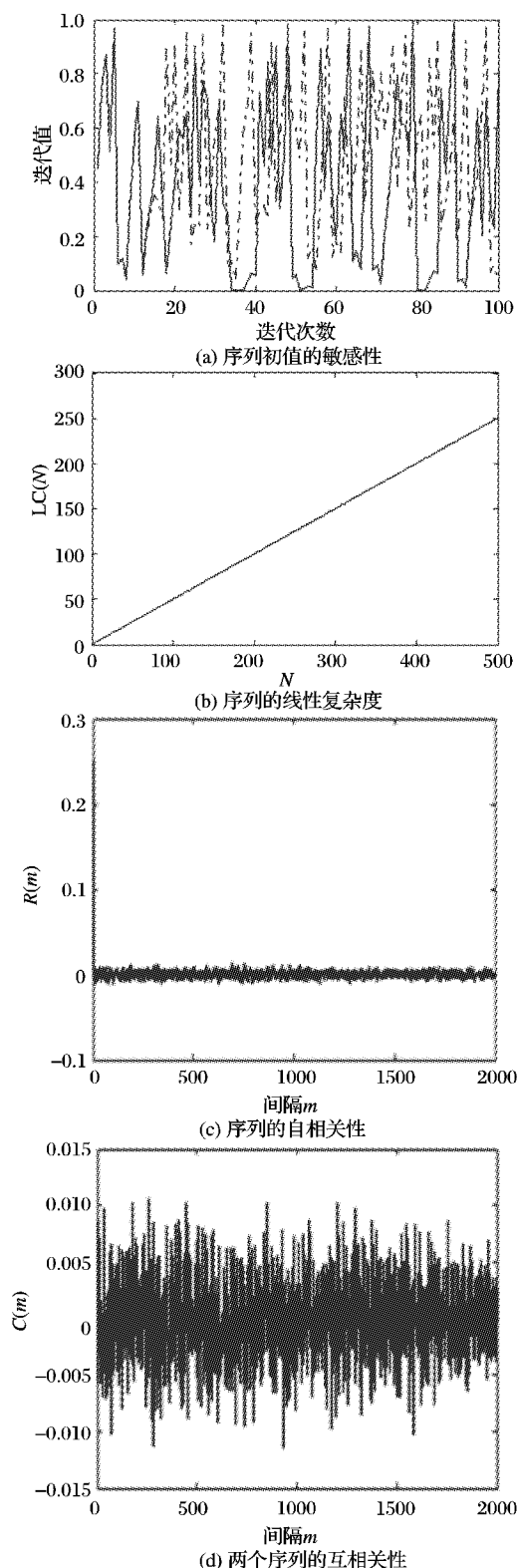


图2 对图1所示混沌系统进行仿真实验结果

5 基于该混沌系统的图像加密算法

5.1 图像加密/解密算法原理

加密算法

1) 发送方利用该混沌模型在本地生成加密序列 f 。(假定图像大小为 $M \times M$, 灰度等级为 256, 则序列 f 的长度为 $M \times M \times 8$; 如果数字图像不是方阵, 可以通过填充为背景色的方法扩充为方阵^[12]。注意: 为了提高加密/解密效率, 序列 f 可以

多次使用, 发送方和接收方经过协商可以在约定时刻更换加密序列 f , 以提高加密算法的安全性。

2) 发送方通过初始值 S_{01}, S_{02} 和混沌参数利用该混沌模型生成一个序列, 将该序列量化为 0-1 序列后, 转换为一个十进制数组 $X(L)$, 且 $L \leq M$ 。用 $X(L)$ 对图像的灰度矩阵 m 进行行置乱, 即根据 $X(L)$ 中的元素值对 m 的相应于该值的行进行倒置, 得到 m_2 。

3) 同 2), 发送方利用该混沌模型最终生成一个十进制数组 $Y(L_2)$, 且 $L_2 \leq M$ 。用 $Y(L_2)$ 对经过第 2) 步后图像的灰度矩阵 m_2 进行列置乱, 即根据 $Y(L_2)$ 中的元素值对 m_2 的相应于该值的列进行倒置, 得到 m_3 。

4) 发送方利用该混沌模型最终生成一个十进制数组 $Z(L_3)$, 且 $L_3 \leq M$ 。通过 $Z(L_3)$, 对 m_3 以主对角线为对称轴, 把按 $Z(L_3)$ 指定的那些平行于主对角线的行进行翻转, 得到 m_4 。

5) 同 4), 发送方生成十进制数组 $W(L_4)$, 且 $L_4 \leq M$ 。通过 $W(L_4)$, 对 m_4 以副对角线为对称轴, 把按 $W(L_4)$ 指定的那些平行于副对角线的行进行翻转, 得到最终置乱后的矩阵 m_5 。

6) 用第 1) 步生成的加密序列 f 对 m_5 转换成的二进制位进行逐位异或运算, 得到加密后的图像。

7) 发送方把生成该混沌模型加密序列 f 的各个初始值和参数以及生成 $X(L)$ 、 $Y(L_2)$ 、 $Z(L_3)$ 、 $W(L_4)$ 的各个初始值和参数在一个安全信道上传给接收方。

8) 发送方把加密后的图像通过公共信道传给接收方。

解密算法

1) 接收方从公共信道上收到加密图像后首先用从安全信道上得到的初始值和参数后恢复出加密序列 f , 对图像的灰度矩阵转换成的二进制位进行逐位异或运算, 恢复出 m_5 ;

2) 接收方利用各个初始值和参数恢复出数组 $X(L)$ 、 $Y(L_2)$ 、 $Z(L_3)$ 和 $W(L_4)$;

3) 接收方先对 m_5 按 $W(L_4)$ 以副对角线为对称轴进行翻转恢复出 m_4 ;

4) 接收方再对 m_4 按 $Z(L_3)$ 以主对角线为对称轴进行翻转恢复出 m_3 ;

5) 接收方再对 m_3 按 $Y(L_2)$ 进行列倒置, 恢复出 m_2 ;

6) 接收方再对 m_2 按 $X(L)$ 进行行倒置, 恢复出 m , 最终得到了解密后的图像。

5.2 算法安全性分析

1) 从算法的原理看, 整个算法由两部分组成: 置乱和替代。这与很多图像加密算法原理相似, 不同的是, 一般的图像加密算法中置乱矩阵时不受密钥的控制, 导致无法完全公开加密算法, 不能抵御选择明文攻击, 而本算法在对灰度矩阵置乱时要 4 次用到混沌系统产生的混沌序列, 即要受到密钥的控制, 而且本系统密钥数量众多; 此外, 以本文中大小为 256×256 的灰度矩阵为例, 矩阵的置乱方案共有 $(C_{256}^1 + C_{256}^2 + C_{256}^3 + \dots + C_{256}^{255} + C_{256}^{256})^4$ 种, 完全能够抵御穷举攻击, 这就极大地增加了加密图像的抗破解性。

2) 该加密方案利用本文中提出的混沌系统产生的混沌序列作为加密序列, 利用了该混沌系统对初始条件的极端敏感性, 对于初始值仅有非常微小的偏差, 该混沌系统在迭代了一定的次数后便会产生完全不同的混沌序列, 本文中混沌系统由于使用的是迭代 2000 次之后的混沌序列, 使得加密效果更佳, 安全性更高。

3) 由于本文采用的混沌系统是有多个混沌映射级联而成,这就大大增大了密钥的个数和密钥空间;从一次一密的角度分析,加密者可以随意地选择密钥,这极大地增强加密后图像抵抗强行攻击的能力;同时,该混沌系统设计原理简单,便于用硬件实现。

6 加密仿真及安全性分析

6.1 可视效果及对密钥的敏感性

采用该加密方案对多幅图像进行了实验,图3为用该方案对大小为 256×256 ,灰度等级为 256 的 BMP 图像 Yanhn 加密/解密的结果。其中,图3(a)为 Yanhn 原始图像,生成加密序列 f 的密钥参数为 $(0.45, 3.57, 3.92, 12, 5, 5000 + 65536 \times 8, S_{01}, S_{02})$, 其中, $S_{01} = 9.501292851471754e - 001$, $S_{02} = 2.311385135742878e - 001$;生成置乱矩阵时所用的密钥参数为: $(0.45, 3.57, 3.67, 11, 5, 200, 4.450964322879468e - 001, 9.318145784616647e - 001, 0.38, 3.65, 3.97, 9, 5, 210, 4.659943416754240e - 001, 4.186494677275062e - 001, 0.49, 3.82, 3.71, 12, 7, 240, 8.462214178243245e - 001, 5.251524963051724e - 001, 0.48, 3.73, 3.62, 10, 5, 180, 2.026473576503873e - 001, 6.721374684742885e - 001)$;图3(b)为置乱操作后异或加密前图像,图3(c)为加密后图像。图4(a)为使用正确密钥解密后得到的图像。把生成加密序列 f 的初始密钥 S_{01} 改为: $9.501292851471753e - 001$, 即 S_{01} 减小了 10^{-16} , 其他一切参数都不变,解密后得到的图像为图4(b);把生成加密序列 f 的初始密钥 S_{02} 改为: $2.311385135742879e - 001$, 即 S_{02} 增加了 10^{-16} , 其他一切密钥参数都同正确的密钥参数相等,解密后得到的图像为图4(c)。从仿真结果可以看出,该混沌系统对密钥参数极其敏感,即使密钥参数发生极其微小的偏差都会造成无法正确解密。

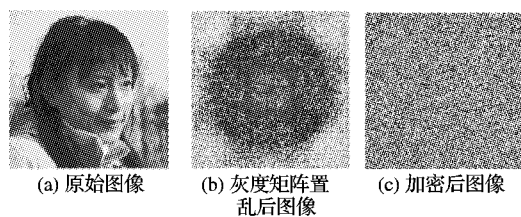


图3 BMP图像的加密

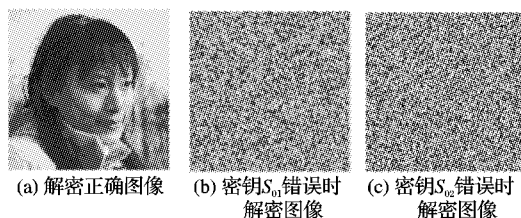


图4 BMP图像的解密

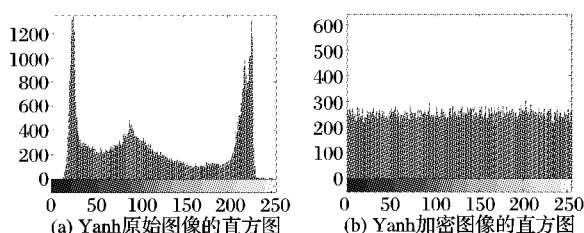


图5 图像的直方图

从图5(a) Yanhn 原始图像的直方图可以看出,不同像素

值的像素数目分布是不均等的;而加密后的直方图图5(b)表明,密文像素值在整个取值空间的取值概率趋于均等,呈现出良好的均匀分布特性,完全掩盖了 Yanhn 原图的特性。

6.2 相邻像素的相关性分析

为了检验明文图像和密文图像相邻像素的相关性,从图像中随机选取部分水平方向相邻像素对,部分垂直方向相邻像素对和部分对角线方向相邻像素对,用下列公式定量计算相邻像素的相关系数^[13]:

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad (5)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N [x_i - E(x)]^2 \quad (6)$$

$$Conv(x, y) = \frac{1}{N} \sum_{i=1}^N [x_i - E(x)][y_i - E(y)] \quad (7)$$

$$g_{xy} = \frac{Conv(x, y)}{\sqrt{D(x)} \sqrt{D(y)}} \quad (8)$$

其中, x 和 y 分别表示灰度图像中相邻 2 个像素的像素值, g_{xy} 即为灰度图像中相邻 2 个像素的相关系数。

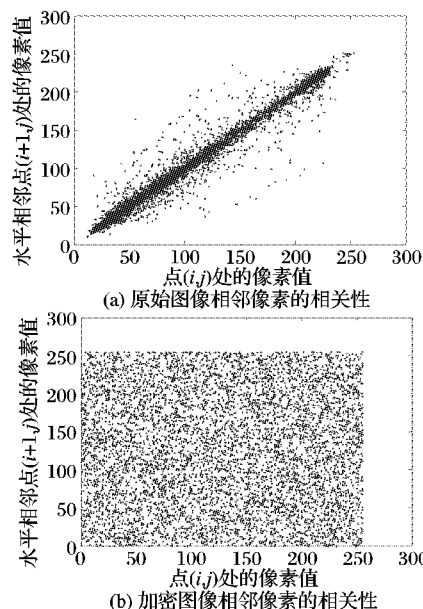


图6 图像水平方向相邻像素间的相关性

图6所示为原始 Yanhn 灰度图像相邻像素和加密后 Yanhn 灰度图像相邻像素的相关性,表1列出了按水平、垂直及对角线 3 种方向计算所得的图像相邻像素间的相关系数值。可以看出,原始明文 Yanhn 图像的相邻像素高度相关,相关系数值接近于 1;加密后 Yanhn 图像的相邻像素相关系数接近于 0,表明相邻像素已基本不相关,证明图像的统计特征已被扩散到了随机的密文中,能够有效抵御像素相关统计分析攻击。

表1 明文和密文相邻像素的相关系数

方向	明文/密文	相关系数
水平	明文	$9.896034034313970e - 001$
	密文	$4.598517694808644e - 004$
垂直	明文	$9.847465786361783e - 001$
	密文	$2.126598583929400e - 003$
对角	明文	$9.795658673812677e - 001$
	密文	$-4.737300090449297e - 003$

(下转第 1857 页)

份。从交互过程来看,两方的连接一直保持着。

4 性能分析

在普适计算环境下基于移动 Agent 的分布式交互中,用户通过由移动 Agent 实现的交互 Agent 在网络中进行交流,这种方式不同于客户机/服务器实现的交互方式,表1给出了这两种交互方式的性能比较。

表1 移动 Agent 与客户机/服务器方式的比较

比较项	交互方式	
	移动 Agent	客户机/服务器
异构平台的迁移	支持	不支持
交互的透明性	支持	不支持
集中化管理	部分支持	支持
交互的健壮性	强	弱
交互平台的扩展性	强	弱
交互的智能性	强	弱
交互的多样性	强	弱

移动 Agent 交互方式建立在 Agent 执行环境上,不依赖于特定的平台,因而支持异构平台的迁移。当网络交互方所在的主机非常繁忙或者遇到不可用于网络交互的原因时,交互 Agent 可移动到比较空闲的主机或者其他可用于网络交互的主机继续与交互对方进行交互,而不需要断开连接,同时正在交互的对方并不需要了解这一行为,因而实现交互的透明性。

同时,客户机/服务器交互方式能够集中化管理,但交互的健壮性、扩展性和智能性不好。在移动 Agent 交互方式中,用户可以通过交互 Agent 之间的交互实时地与多个对等实体之间进行交互。交互 Agent 之间的交互实现了共享信息的功能,而这些 Agent 的移动性和智能性更增强了信息共享的灵活性。交互 Agent 移动到交互对方所需信息的地方,而不影响与对方实际的交互,而且在这一交互过程中无需庞大的服务器和超量的带宽,因而提高了交互的健壮性。

另外,移动通信技术的发展和手持终端设备软硬件的发展为移动 Agent 交互方式提供了更广阔更强大的执行环境,交互 Agent 在 PC 之间、PC 和手持终端设备之间以及手持终

端设备之间的移动更加提升了随时沟通、及时互动的质量和交互理念,实现了交互的多样性。与客户机/服务器方式相比,移动 Agent 交互方式通过扩充交互 Agent 的智能^[8],能够实现自动化交互,这些代表用户的交互 Agent 能够感知其运行环境,并根据环境的变化做出适当的反应,使交互过程能够健壮持续地进行。

5 结语

本文给出普适计算环境下一种基于移动 Agent 的分布式交互方法,交互 Agent 代表用户作为交互的对等实体封装一个完整交互过程,自主移动到用户需要的网络节点持续在个体之间、群体之间以及个体和群体之间进行交互。这种交互方式实现了移动对等体之间透明的交互,通过定制 Agent 各种行为和协同运作方式提升了普适计算环境下人机交互的多样性和持久性,提高了交互服务的及时性和信息共享的灵活性。

参考文献:

- [1] 徐光祐, 史元春, 谢伟凯. 普适计算[J]. 计算机学报, 2003, 26(9): 1042-1050.
- [2] ANDREW O, ANDY O. Peer-to-peer: Harnessing the power of disruptive technologies[M]. Sebastopol, CA: O'Reilly and Associates, 2001.
- [3] GHOSH H. Personal Agents for impersonal interaction[J]. IEEE Technology and Society Magazine, 2008, 27(1): 4-4.
- [4] 王汝传, 徐小龙, 黄海平. 智能 Agent 技术及其在现代信息网络技术中的应用[M]. 北京: 北京邮电大学出版社, 2006.
- [5] 张云勇, 刘锦德. 移动 Agent 技术[M]. 北京: 清华大学出版社, 2003.
- [6] XIAO L, ROBERTSON D, CROITOROU M, et al. Adaptive Agent model: An Agent interaction and computation model[C]// Proceedings of 31st Annual IEEE International Computer Software and Applications Conference. Washington, DC: IEEE Computer Society, 2007: 153-158.
- [7] CIOBANU G. Collaborative agents interaction using message passing interface[C]// Proceedings of Eighth International Symposium on Symbolic and Numeric Algorithms for Scientific Computing. Washington: IEEE Computer Society, 2006: 244-250.
- [8] MORATIS P, SPANOUDAKIS N. Argumentation-based Agent interaction in an ambient-intelligence context[J]. IEEE Intelligent Systems, 2007, 22(6): 84-93.

(上接第 1835 页)

7 结语

针对一维离散混沌系统在计算机有限精度下存在退化的问题,本文提出了一种新的一维离散混沌系统,该混沌系统继承了一维离散混沌系统结构简单、运算速度快、随机性好等优点,还增大了密钥数量和密钥空间;同时,增大了混沌序列的周期。基于该混沌系统,本文又提出了一种新的图像加密方案,实验分析表明,该方案安全性高,原理简单,加密/解密效率高,易于硬件实现快速加密、解密,有很高的实用价值。

参考文献:

- [1] 王相生, 甘骏人. 一种基于混沌的序列密码生成方法[J]. 计算机工程, 2001, 27(9): 103-104.
- [2] 李树均, 牟轩沁, 纪震, 等. 一类混沌流密码的分析[J]. 电子与信息学报, 2003, 25(4): 473-478.
- [3] 周红, 俞军, 凌雯亭. 混沌前馈型流密码的设计[J]. 电子学报, 1998, 26(1): 98-101.
- [4] 周红, 罗杰, 凌雯亭. 混沌非线性反馈密码序列的理论设计和有限精度实现[J]. 电子学报, 1997, 25(10): 57-60.
- [5] 罗启彬, 张健. 一种新的混沌伪随机序列生成方式[J]. 电子与信息学报, 2006, 28(7): 1262-1265.

- [6] 谢邦勇, 王德石, 蒋兴周. 基于双混沌系统的伪随机比特发生器的研究[J]. 海军工程大学学报, 2007, 19(5): 18-20.
- [7] 张巍, 胡汉平, 李德华. 一种新的混沌序列生成方式[J]. 华中科技大学学报, 2001, 29(11): 64-66.
- [8] 韦鹏程, 张伟, 杨华千. 一种多级混沌图像加密算法研究[J]. 计算机科学, 2005, 32(7): 172-175.
- [9] 王兴元, 刘威, 李瑞娟. 基于 SCS-PRBG 的数字流密码[J]. 计算物理, 2007, 24(4): 494-498.
- [10] 乌旭, 陈尔东, 胡家升. 一种基于混沌的图像加密改进方法[J]. 大连理工大学学报, 2004, 44(5): 754-757.
- [11] 樊春霞, 姜长生. 一种基于混沌映射的图像加密算法[J]. 光学精密工程, 2004, 12(2): 179-184.
- [12] 张永红, 康宝生, 张学锋. 基于混沌序列的迭代混合数字图像隐藏技术[J]. 计算机工程与设计, 2007, 28(4): 879-881.
- [13] 韩凤英, 朱从旭, 胡玉平. 一种基于高维混沌系统的彩色图像加密新算法[J]. 计算机应用, 2007, 27(8): 1888-1894.
- [14] CHEN G R, MAO Y B, CHARLES K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons and Fractals, 2004, 21(3): 749-761.
- [15] SCHIER B. Applied Cryptography: Protocols, algorithms and source code in C[M]. New York: John Wiley and Sons, 1996.