图像混沌加密技术分析

张连俊
(山东理工大学计算机学院，淄博 255012)

〔摘 要〕 本文介绍了混沌加密技术和利用混沌技术进行图像加密的方法，并阐述了图像混沌加密的特点和|些值得进| 步研究的问题。

〔关键词〕 混沌；图像加密；混沌加密技术

〔**Abstract**〕 The chaotic image encryption technique is Presented in this paper; some advantages with chaotic technique and some valuable Problems for further research were illustrated.

〔**Key words**〕 image encryption; chaos; chaotic encryption technique
〔中图分类号〕TP391.41 〔文献标识码〕B 〔文章编号〕1008-0821(2005)08-0118-02

1 引 言

多媒体通信技术是本世纪科学技术发展的热点。随着信息技术和计算机网络的快速发展，数字化的多媒体可以通过网络方便地复制、存储和通信。在很多情况下通信双方都不希望网络上所传输的图像数据被未授权者所浏览或处理，要求发送方和接收方要进行保密通信。这就涉及到图像加密技术，通过图像加密操作后，原来的数字图像变为类似于信道随机噪声的信息，这些信息对不知道密钥的网络窃听者是不可识别的，进而可以有效地保护传输中的图像数据。随着人们对知识产权的重视，图像加密技术有着广阔的应用前景。图像加密的措施很多，本文重点分析混沌加密技术。

2 混沌图像加密技术

混沌现象是指在非线性动态系统中出现的确定性和类似随机的过程。这种过程非周期、不收敛、但有界，并且对初始值和外部参数有极其敏感的依赖性，即初始条件的微小差异会随着时间的推移，以李雅普诺夫指数规律相互分离，最终变成运动轨迹或特性完全不同的两条轨迹。混沌是一种特殊的动力学系统，可以提供数量众多、非相关、类随机、易于产生和再生的信号，并且只要一个映射公式和初始值就可以产生混沌序列，不必存储各个序列点的值。混沌序列的实现方法大致可分为以下几种：(1) 经典的一维混沌映射，形式简单且易实现，便于理论设计和分析，其研究也最多和最深入；(2) 采用高阶非线性数字滤波器，能部分地克服有限精度效应，并可用DSP非常方便地实现；(3) 基于神经网络的方法，实质上是利用神经网络来学习和逼近一个混沌系统，具有系统结构灵活的特点；(4) 基于高维的时空混沌，较低维的混沌映射其产生的混沌序列数量更多，且易实现同步。

近年来，由于混沌动力学的发展，人们逐渐认识到混沌可以用来作为一种新的密码系统，可以用来加密文本、声音及图像数据等。混沌之所以被用来作为一种新的密码体制，这是和混沌系统自身的特性分不开的。具体来说，混沌系统具有以下几个适合作为密码系统的特性：(1) 遍历性。在有限区域内，混沌轨道上的点可以任意接近，这使得对初始条件(明文)的预测非常困难；(2) 混合性。混沌轨道的极不规则性以及系统局部扩展、压缩、折叠，使得混沌系统的输出类似于随机噪声；(3) 指数发散性。相平面上任意接近的两点随着迭代的进行都会指数性发散。混沌系统既具有混合特性，又具有扩散特性，完全符合密码学的要求，是一种天然的密码系统。而混沌在二维相平面上的不规则性，使得混沌系统更加适合于图像数据的加密。混沌密码是鉴于混沌系统对系统的参数变化及系统的初始条件非常敏感这一事实来设计的。其混沌系统应用于图像数据的加密的方法：

2.1 将加密系统的密钥设置为混沌系统的参数，而将明文设置为混沌系统的初始条件，或者不改变混沌系统的参数，而将加密系统的密钥设置为混沌系统的部分初始条件，将明文设置成混沌系统的另一部分初始条件，之后经过密码学中类似于Feistel网络的多次迭代来实现对明文和密钥的充分混合和扩散。现在已知的基于混沌动力学的图像加密算法的加密速度很快，并且只经过少数的几次迭代就能使得原始图像完全不可识别，但这种加密算法没有考虑图像数据压缩，加密后的数据量没有减少，这对网络中的图像通信会造成一定的压力。

2.2 基于混沌自同步的概念，这种设计思路特别适用于用混沌系统对模拟信号的加密传输，易于用电路硬件实现。其基本做法是在发送端应用混沌信号调制待加密的信号，并把经过调制的信号一起在通信信道上传输。这种信道上的信号类似于噪声信号，使得窃听者无法识别。而在接收端，应用混沌自同步技术，去除混沌信号，检出有用信号，即完成了收发双方的保密通信。这种技术主要用于模拟信号的加密。

2.3 利用混沌序列代替一般的伪随机序列实现保密通信。现在CDMA系统中，大都采用线性或非线性移位寄存器产生伪随机序列作为扩频序列，例如M序列、GOLD序列。

收稿日期：2005-03-04
作者简介：张连俊(1964—)，男，毕业于西安电子科技大学，硕士，山东理工大学计算机学院副教授，主要从信息处理、通信工程方面的研究。

这些序列码用于生成扩频地址码的个数都很有限，容易被破译，因此根据混沌的特点用混沌序列代替一般的伪随机序列，用混沌序列来充当扩频通信中的扩频序列，即混沌扩频序列。这不但对多用户通信提供了条件，而且可实现对信息的加密，在多址通信和安全通信中有广泛的应用前景。混沌序列产生的码源丰富，平衡性好，优于现行系统中的伪随机序列。作为 CDMA 系统用户地址码，能保证地址码的实用性和稳定性，可以为多用户通信及保密通信性能的改善起到重要的作用。

将混沌系统作为伪随机序列发生器，其中混沌系统由离散混沌系统或经过离散化的连续混沌系统构成。混沌系统产生的伪随机序列与明文进行异或操作，得到输出即为密文。这种加密算法最先由 Matthewst 提出，但在计算机上实现的混沌系统，由于计算机精度的限制，在本质上都是周期的，而且某些这样实现的混沌系统的周期还非常短。应用选择密文和选择明文攻击技术时，这种密码体制是容易破译的。寻找具有长周期的“准混沌序列”及对这样的系统测试方面的研究是非常重要的。如利用多个混沌系统的复合，可产生统计性能良好的伪随机序列。由于混沌系统的普遍性及混沌序列的计算机产生非常容易，若能产生随机性好的伪随机序列，再结合图像压缩编码技术，设计一种实用的图像加密算法是非常有前途的。

2.4　基于二维混沌的分组密码加密体制。这种体制的基本思路是：应用二维混沌系统，如 Baker 映射、标准映射等实现对明文的置换操作，再应用某种简单的替代操作，经过多轮（< 15 轮）迭代来实现对数据的有效加密。这种技术特别适合对图像数据进行加密，计算机仿真结果表明，这种图像加密技术可获得：可变的密钥长度（进而可获得不同级别的安全性）；相对大的分组尺寸（几 kB 或更大），这对大数据量的图像数据特别适合；相对高的加密速率（未优化的 C 代码在 600MHz 的奔腾机上可达到 10Mb 的加密速率）。因为加密过程不需要图像预处理，可节省预处理时间。但加密过程没有引进数据压缩技术，这对加密后图像密文的通信会造成一定的压力。近年来的研究表明，混沌动力学与密码学有着某些天然的联系。在混沌动力学中，Lyapunov 指数能有效地表示相空间内邻近轨道的平均指数发散率，而基于混沌动力学与密码学的类比研究，将 Lyapunov 指数的概念应用到加密系统中去，可能有效地测度密码的扩散程度。在混沌动力学中，Kolmogorov 熵可以有效表示信息在加密过程中信息量损失的速率，而对于迭代密码系统中迭代轮数的确定，可以应用混沌动力学中 Kolmogorov 熵的概念来有效标度。研究还表明，很多混沌系统与密码学中常用的 Feistel 网络结构是非常相似的，如标准映射、Henon 映射等。研究表明，混沌与密码学存在着天然的联系。但混沌毕竟不等于密码学，其最大的不同点在于密码学工作在有限集上，而混沌系统是定义在无限集上的。应用混沌来设计密码系统的最大困难在于如何把定义在无限集上的混沌变换到密码特性良好的有限集密码上，这方面的研究正在进行中。对于混沌应用于图像加密，以下几个方面值得注意的问题：混沌与密码学内在联系的研究；如何用混沌动力学的物理量，如 Lyapunov 指数、Kolmogorov 熵等来标度混沌密码系统定量的安全性；如何设计安全性高的混沌密码系统；如何实现混沌定义的无限集到密码系统有限集的映射；如何应用密码系统来研究混沌系统等。

3　结论及展望

本文对图像混沌加密技术做了阐述，指出了混沌应用于密码系统的主要形式，并说明了混沌系统适合于作为密码系统的原因及用于图像加密的特点。利用混沌动力学中的一些物理量，如 Lyapunov 指数、Kolinogorov 熵可能作为密码安全性的一种标度，一些具有良好密码特性的混沌变换可以用作为密码变换。通过研究混沌动力学和混沌加密技术来促进加密技术的发展。

参 考 文 献

[1] Cox I J, Kilian J, Leighton F T. Secure spreads spectrum watermarking for multimedia [J]. IEEE Trans. on Image Processing, 1997, 6, (12): 1673－1687.

[2] Chang C C, ed al. A new encryption algorithm for image cryptosystems [J]. The Journal of systems and Software, 2001, 58, (7): 83－91.

[3] 一玮，齐东旭. 数字图像变换及信息隐藏与伪装技术 [J]. 计算机学报，1998, 21, (9): 535－543.

[4] 冯登国，吴文玲. 分组密码的设计与分析 [M]. 北京：清华大学出版社，2000.

[5] Chang H K, Liu J L. An image encryption scheme based on quadtree compression scheme [A]. Proceeding of the International Computer Symposium [C]. teiwan: 2001: 230－237.

[6] Makoto I. Spread spectrum communication via chaos [J]. International Journal of Bifurcation andChaos, 1999, 9, (1): 155－213.

[7] 于银辉，刘卫东. 两种混沌扩频序列平衡性分析 [J]. 重庆邮电学院学报（自然科学版），2004, 16, (3): 61－64.

（上接第 117 页）

形码上印上该书的索取码。一张条形码贴在书的正面，供借换书使用；另一张贴在书的侧面，供整理书架时本系统识别。这样一本书还是贴两张条码，同原来没有使用本系统时贴纸的工作量一样多，而且数据库中两个登录号一致，也就可以直接使用原来的数据库了，这样就没有增加任何工作量。

5　结束语

条形码的印刷成本非常便宜，该机器又能够极大地提高图书管理人员的工作效率，降低工作人员的劳动强度。同时该机器稍作处理，还能够进行图书馆现存图书的盘点、查找图书等工作，因而该系统必将受到广大图书管理人员的欢迎！

参 考 文 献

[1] 沈嵘. 无线射频识别技术（RFID）及其在图书馆的应用 [J]. 现代图书情报技术，2004,（9）: 37－39.

[2] http: ∥ www. morerfid. com. cn/article/1104/cn①04110101. html（Accessed Dec. 23, 2004）[EB]

[3] 于从新. 光笔条形码记录器 [J]. 光电工程，1994,（5）: 36－38.