摘 要

在信息时代的今天，随着通信技术和网络技术的高速发展和广泛应用，越来越多的信息在网络上传输，信息的安全与保护问题显得愈发重要，使得密码学理论与技术成为信息科学与技术中的一个重要研究领域。一些新兴的密码学理论，如混沌密码学、量子密码学等，也引起了愈来愈多的学者的青睐。本文主要研究混沌序列密码的设计与实现的有关问题。

本文系统介绍了混沌密码学的一些预备知识、现代密码学基本原理和混沌理论；详细讨论了 Logistic-map 混沌序列及其存在的不足，在此基础上，提出将 Logistic 混沌序列与 m-序列以异或方式结合形成一类混合混沌序列的方法。从理论上分析了混合混沌序列的密码学属性（包括混沌序列的周期性、随机性、平衡性、游程特性、相关性、线性复杂度等多项指标），并作了大量的对比分析实验。结果表明：在有限精度实现下，该方法可以有效提高混沌系统的复杂性和周期性。结合收缩式密钥流发生器，设计和实现混合混沌系统，并进行相应的仿真实验，同时对该系统的安全性能进行了深入分析，如扩散扰乱特性、密钥空间、弱密钥问题和抗密码学分析等；研究了如何利用混合混沌序列进行图像加密，提出了一种基于混合混沌序列的多级图像加密算法，并作了详细地描述。模拟实验证明本算法具有加密速度快，安全性高，无额外畸形产生等特点。

最后论文对研究工作进行了全面的总结，并对今后的研究方向进行了展望。

关 键 词： 序列密码，线性反馈移位寄存器，m-序列，混沌，混合混沌序列.

ABSTRACT

With the rapid development and wide application of communication technology and network technology, more and more information has been transmitted through the network. Therefore, the security of information is getting more and more important. The cryptography, which aims at the security of information, has become of the important research fields in information science and technology. Several new branches in this field such as chaotic cryptography and quanta cryptography have also attracted many research's interests. The main purpose of this dissertation is to investigate the theory and application of chaotic cryptography, especially the design and implementation of chaotic stream ciphers.

The preliminaries including the theory of modern cryptography and chaos dynamics are presented at first. Then the author has discussed the chaotic sequences generated via logistic map with chaos and has claimed that this type chaotic sequences are not suitable for key stream. Based on the discussion above, a class of mixed chaotic sequences, which are produced by combining logistic chaotic sequences and m-sequences in form of exclusive-OR, has been proposed in this paper. The cryptographic properties, such as long period, randomicity, balance, run length, correlation function and linear complexity, of mixed chaotic sequences have been analyzed in detail. The results show that the new approach allows us to improve the complexity and the period of the chaotic system under the finite-precision circumstances. By using the Shrinking Generator, the author has designed and implemented the mixed chaotic system, and made in-depth analysis of the security performances of the system, such as properties of confusion and diffusion, key space, weak key and capability against cryptanalysis, and so on.

This type mixed chaotic sequences has been also employed to image encryption, futhermore a multistage image encryption algorithm has been presented in this paper. The computer simulation demonstrates that this image encryption scheme have low computational complexity, high security and no distortion.

Finally, the summarization has been obtained and the future research directions have been also given.

Ked words: Stream cipher, LFSR, m-sequences, Chaos, Mixed chaotic sequences.

1 引 言

1.1 密码技术的进展

密码学是一门既古老又年轻的学科。早在四千年前，古埃及人就开始使用密码来保密传递消息。作为保密信息的手段，密码技术本身也处于密码状态，基本局限于军事目的，所以它的发展受到了限制。

在第一世界大战之前，密码技术的进展很少见诸于世，直到 1918 年，William F.Friedman 的论文“重合指数及其密码学的应用”[1]发表时，情况才有所好转。

1949 年, Claude Shannon 的奠基性论文“保密系统的通信理论”[2]的发表，奠定了密码学的理论基础。密码学从此成为一门学科。

20 世纪 70 年代，是密码学发展的重要时期，有两件重大的事件发生。其一，美国国家标准局颁布了联邦信息处理标准的 DES[3]（Data Encryption Standard）作为工业数据加密的工业标准。其二，Diffie 与 Helman 的革命性论文“密码学新方向”[4]发表，开辟了公开密钥密码学的新领域，成为现代密码学的一个里程碑。1978 年，R.L.Rivest，A.Shamir 和 L.Adleman 实现了 RSA[18]公密钥体制，它成为公钥密码的杰出代表和事实标准。数据加密标准 DES 的颁布和公钥密码概念的提出标志着现代密码学的诞生。

1984 年，Bennett.Charles H, Brassard.Gille 在 Wiesner 的“共扼编码”思想的启发下，首次提出了基于量子理论的 BB84 协议[5]，从此量子密码理论宣告诞生。量子密码不同于以前的密码技术，它是一种可以发现窃听行为、安全性基于量子定律的密码技术，可以抗击具有无限计算能力的攻击。

1985 年，N.Koblitz 和 V.Miller 把椭圆曲线理论[5]应用到公钥密码技术中，在公钥密码技术中取得重大进展，成为公钥密码技术研究的新方向。

密码技术的另一个重要方向 — 序列密码(也叫流密码)理论也取得了重要的进展。特别是把混沌理论引入流密码及保密通信理论中，为序列密码理论开辟了一条新的途径。

在传统流密码体制中，流密码强度完全依赖于密钥流生成器所生成序列的随机性和不可预测性，也就是说流密码体制安全的核心问题是密钥流生成器的设计。由于混沌序列是一种非线性的序列，其结构复杂，分布上不符合概率统计学原理，难以分析、重构和预测。目前只能在特殊的条件下对一些混沌系统进行重构，理论上还没有较好的一般性方法。因此混沌系统被广泛地用于信息加密。

混沌系统在密码学中的应用同时在国际密码学界和电子工程界受到重视。在密码学界里，英国数学家 Mathhews[6]首先提出了混沌加密方法，随后在 1991 年欧

洲密码学年会上，出现了多种混沌密码体制。同时，Carroll[7]构造出第一个同步混沌电路，从此，研究人员开始对混沌密码做大量的研究。在 Cryptologia、Eurocrypt、IEEE Trans on CAS、International Journal of Bifurcation&Chaos 等杂志和有关会议上发表了不少有关混沌密码的研究成果。混沌序列密码最早是由英国数学家 Matthews 提出的，他分析了 Logistic 混沌映射作为序列密钥流生成器的问题，并对其作了改进，以加大密钥空间和防止混沌信号中稳定周期窗的出现,其后得到了一定的发展。Habutsu 等[8]则提出了一种混沌加密系统，即加密时对一个用于替换明文的初值作用 N 次 Tent 逆映射，而解密时则使用 N 次 Tent 映射。随后 Biham[9]指出，使用选择密文攻击可容易地对该系统解密，并且已知明文攻击的复杂度为 2^{38}。以后 Carrol 等提出了以 Lorenz 系统和 Bernstein 等人提出了以一阶非均匀采样数字锁相环系统作为序列密码生成器。最近 L.Kocarev 等[10]提出了一种基于 Logistic 混沌映射的分组加密算法，讨论了混沌具有的密码学所要求的如扩散、混乱等特性。J.Fridrich[11]提出了一种基于二维 Baker 混沌映射的对称加密算法，并用于图像加密。此外，K.W.Wong[12]还提出了一种快速混沌加密方案，通过动态更新查询表来实现加解密，简化了加解密过程，适合于传输多媒体等大数据量文件。易开祥等[13]讨论了一种基于混沌序列的图像置乱算法，首先根据密钥生成实数值混沌序列，通过离散映射生成相应的符号矩阵和置乱矩阵，在 DCT 变换域对图像进行置乱加密。南京大学声学研究所倪皖荪等[14]也应用混沌序列实现了汉语拼音信号的加密解密和传输。尽管已有许多混沌加密方案的提出，但混沌密码学方法还未完全成熟，目前大部分混沌加密系统都采用自然的混沌系统，它们不一定能够是严格密码学意义的保密性，实际上，许多混沌密码学方法中已经发现了缺陷，例如：MIT 的 Short 利用非线性动力学预测方法（NLD forecasting）破译了美国海军研究所提供的混沌掩盖加密方案[15]；另外，Wheeler 也指出 Matthews 的混沌序列密码，由于具有严重的有限精度效应而不适于实际应用。混沌密码学的研究仍然是一个新的具有挑战性的前沿课题，探讨混沌加密机制、如何充分利用传统密码学思想和大量的已有研究成果、混沌密码安全性如何评价、克服有限精度的效应等问题还需要深入细致的研究。

1.2 密码学的基本概念

密码学是对信息进行编码实现隐蔽信息的一门科学。通过采用密码技术对信息进行编码可以隐蔽和保护需要保密的信息，将数据变成不可读的格式，防止数据在存储或传输过程中被篡改、删除、替换等，从而实现消息的保密性、完整性和可认证性。消息称为明文(Plaintext)，用某种方法伪装消息以隐蔽它的内容的过程称为加密(Encryption)，被加密的消息称为密文(Ciphertext)，把密文转换为明文

的过程称为解密(Decryption)。对明文进行加密时所采用一组法则称作加密算法，同样，对密文进行解密所采用的一组法则称为解密算法。加密算法和解密算法通常在一组密钥(Key)控制下进行的，分别称为加密密钥和解密密钥。如果一个密码体制的加密密钥与解密密钥相同，则称为单密钥体制或对称密码体制；否则，称其为双密钥密码体制或非对称密码体制或公开密钥密码体制。

一个完整的密码体制可由一个五元组(M,C,K,E_{ke},D_{kd})来描述。M是所有可能的明文组成的有限集，称为明文空间；C是所有可能的密文组成的有限集，称为密文空间；K代表密钥空间，是由所有可能的密钥组成的有限集；对任意的加密密钥$ke \in K$和相应的解密密钥$kd \in K$,都存在一个加密法则E_{ke}和相应的解密法则D_{kd}，并且有$D_{kd}(E_{ke}(m)) = m$ 。密码系统的数学模型[5]如图 1.1 所示。

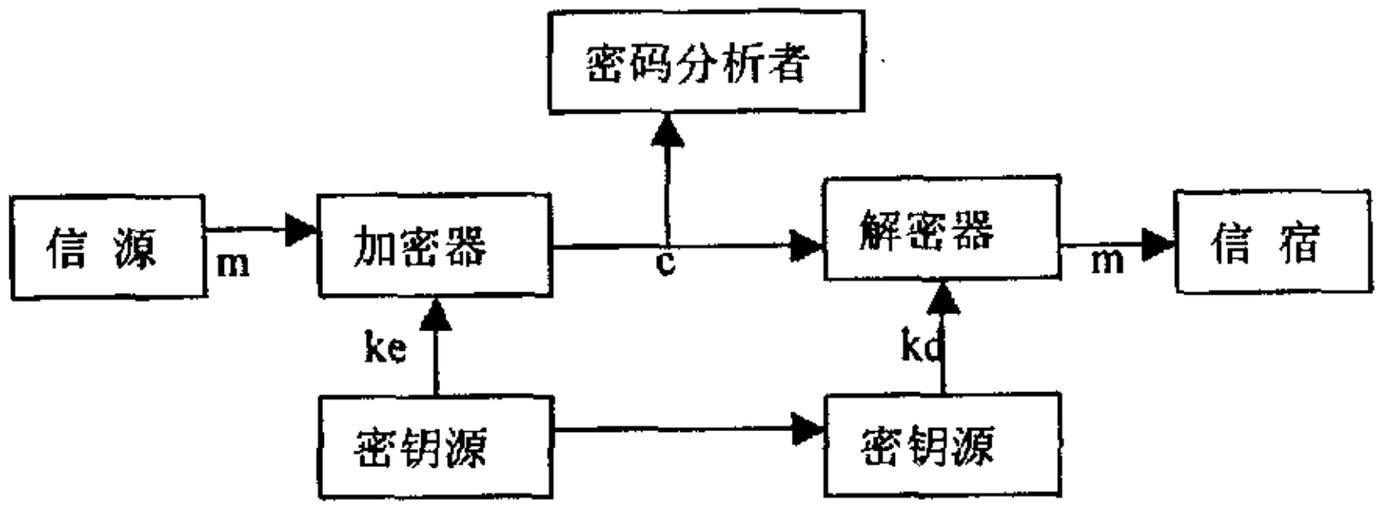


图 1.1 密码系统的数学模型

Fig.1.1 The mathematical model cryptosystem

一个好的密码体制至少应该满足下述两个条件：

① 在已知明文 m和加密密钥ke时，计算$c = E_{ke}(m)$容易，在已知密文c和解密密钥kd时，计算$m = D_{kd}(c)$容易。

② 在不知解密密钥kd是，不可能由密文c推知明文m。

对于一个密码体制，如果能够根据密文确定明文或密钥，或者能根据明文和相应的密文确定密钥，则这个密码体制是可破译的；否则，称其为不可破译。

根据密码分析者对明、密文掌握的程度，攻击可分为下述四种：

① 唯密文攻击：密码分析者仅知道一些密文。

② 已知明文攻击：密码分析者知道一些明文和相应的密文。

③ 选择明文攻击：密码分析者可以选择一些明文，并得到相应的密文。

④ 选择密文攻击：密码分析者可以选择一些密文，并得到相应的明文。

上述四种攻击的目的是获得密码系统所使用的密钥，这四种攻击类型的攻击强度按上述依次递增。

1.3 密码系统的安全理论

密码系统的安全性是密码学研究中的主要问题。一个密码系统安全性是基于密钥的安全性，而不是依赖于密码系统的加密体制或算法的保密。密码系统的安全性有两种标准：一种是理论安全性，另一种是实际安全性，这两种安全性只针对唯密文攻击。以下将分别阐述。

1.3.1 完全保密系统

完善保密性又称为无条件安全性，是指具有无限计算资源（如时间、空间、设备和资金等）的密码分析者也是无法破译该系统。研究密码系统的无条件安全性不能用计算复杂性的观点来研究，而一般采用概率的观点来研究密码系统的无条件安全性。

假设一个密码系统(M,C,K,E_{ke},D_{kd})具有有限的明文空间$M=\{m_1,m_2\cdots m_n\}$和有限的密文空间$C=\{c_1,c_2,\cdots c_n\}$。明文m_i和密文c_i分别以$p(m_i)$、$p(c_j)$的概率出现。在收到密文c_j的条件下发送明文为m_i的条件概率为$p(m_i\mid c_j)$。

定义 1.3.1[16] 密码系统(M,C,K,E_{ke},D_{kd})称为完全保密或无条件保密，如果有等式成立：

$$p(m_i\mid c_j)=p(m_i) \tag{1.1}$$

定义 1.1 表明，对于完全保密的密码系统，密码分析者截获的密文并不能帮助他得到比信源先验概率更多的信息，这是一种非常理想的密码系统。

引理 1.3.1[16]一个密码系统完全保密的充要条件为对所有$m_i\in M$，$c_j\in C$，有

$$p(c_j\mid m_i)=p(c_j) \tag{1.2}$$

定理 1.3.1[17]若一个密码系统的明文数、密文数和密钥数目都相等，则该密码系统完全保密的充要条件是：

（1） 每个明文恰好有一个密钥将其加密为一个密文。

（2） 所有密钥的选取是等概率的。

定理 1.3.1 表明完全保密的密码系统是存在的。一次一密钥系统就是完全保密的，但是这种密码系统并不实用，由于所需的密钥量等于所有明文的数量，对于这样巨大的密钥量的分配和管理是不现实的。在密码学中，绝大多数密码系统是不完全保密的。对于这些系统，可由信息论中的熵来度量。

1.3.2 密码系统的理论安全性

定义 1.3.2[16]对于一个密码系统(M,C,K,E_{ke},D_{kd})，明文熵定义为：

$$H(M)=-\sum_{m\in M}p(m)\log p(m) \tag{1.3}$$

密钥熵定义为：

$$H(K)=-\sum_{k\in K}p(k)\log p(k) \tag{1.4}$$

明文熵是从明文空间 M 中取一明文发送给接受者的不确定测度。密钥熵是对密钥空间 K 中密钥选取不确定性的测度。但是在实际情况中，密码分析者还拥有他的一定数量的密文信息，因此还要考虑在已获得某些密文的条件下，对发送某些明文或使用某一密钥的不确定测度。X^t 和 Y^n 分别表示明文空间所有长度为为 t 的明文和密文空间中所有长度为 n 的密文构成的集合，定义明文的疑义度和密钥的疑义度分别为：

$$H(X^t\mid Y^n)=-\sum_{\substack{m\in x^t\\ c\in Y^n}}p(c,m)\log p(m\mid c) \tag{1.5}$$

$$H(K\mid Y^n)=-\sum_{\substack{k\in K\\ c\in Y^n}}p(c,k)\log p(k\mid c) \tag{1.6}$$

其中 $p(c,m)$ 是发送明文为 m，收到密文为 c 的概率，$p(m\mid c)$ 是已知密文 c 后明文被发送的后验概率；$p(c,k)$ 是密文为 c 且加密密钥为 k 的概率，$p(k\mid c)$ 是已知密文 c 的条件下密钥为 k 的概率。明文疑义度 $H(X^t\mid Y^n)$ 和密钥疑义度 $H(K\mid Y^n)$ 分别表示在截获 n 长度密文后关于明文和密钥的不确定性。$H(X^t\mid Y^n)$ 和 $H(K\mid Y^n)$ 均是 n 的非增函数，因此随着截获密文的增多，获得关于明文和密钥的信息量就会增多，关于明文空间和密钥空间的不确定性就会减少。若 $H(X^t\mid Y^n)=0$，则表示从密文已经可以完全确定明文。同样，若 $H(K\mid Y^n)=0$，则由 c 可以完全确定获得密文 c 的密钥。

定义 1.3.3 一个密码系统的唯一解距离 N_0 定义为使 $H(K\mid Y^n)=0$ 的最小正整数 N_0。

唯一解距离是度量系统安全性的一个指标，它表示唯一确定破译加密所用密钥至少所需要截获密文的长度。

1.3.3 密码系统的实际安全性

由以上介绍可以知道，对于给定的密码，唯一解距离 N_0 表明，当截获的密文数量大于 N_0 时，原则上可唯一确定系统所使用的密钥，但是这种是假设密码分析者能拥有无限的资源。但是实际上，密码分析者可利用的资源总是有限的。一旦破译一种密码所需要的代价超出了破译该密码所得信息的价值，或者密码分析者破译成功的时间超出了所得信息的有效期，这种破译是徒劳的。在资源有限的条

件下，研究一个密码系统的安全性，被称为密码系统的实际安全性。

在实际条件下，一个理论上不安全的密码系统可能提供实际所需的安全性。另一方面，一个理论上安全的密码系统，实际上也可能不安全，因为理论上安全是在唯密文攻击下并且忽略了许多很重要的因素得出的结论，实际上由于密钥管理的复杂性、自然语言的冗余度和密码分析者可能得到明文一密文对等因素使得密码分析者可以破译理论上安全的系统。

现代密码系统的设计是建立在某个或某类数学难题的基础上，一个密码系统的实际安全性大小就取决于求解这些数学问题的难易程度。

1.4 密码体制的分类

1.4.1 单密钥体制和双密钥体制

一个密码系统按照加密密钥与解密密钥是否相同可分为单密钥体制和双密钥体制。单密钥体制又称对称或私密钥密码体制，双密钥体制又称非对称或公钥密码体制。

单密钥体制的加密密钥和解密密钥相同，最具有代表性的是 DES[3](Data Encryption Standard)算法。系统的安全性主要取决于密钥的安全性。单密钥体制存在的最主要问题是密钥的管理与分发，由于加/解密双方要使用相同的密钥，因此在发送、接受数据之前，必须完成密钥的分发，如何保证可靠、安全地进行大范围、随机变化环境下的密钥分发便成了对称密钥体制中最薄弱，也是风险最大的环节。然而，由于单密钥系统具有加密速度快和安全强度高的优点，在军事、外交、金融以及商业应用等领域中仍被广泛的使用。

1976 年，Diffe 和 Hellman 提出了双钥体制，最具有代表性的是 RSA 算法[18]、DSA 算法[19]等。它主要的特点是加密密钥和解密密钥分开。加密密钥公开，有加密密钥和密文不能容易地求得解密密钥和明文，另外，加密变换和解密变换可以交换。这样，双密钥体制完全克服了单密钥体制的上述缺点，极大的简化了密钥的管理和分发，特别适用于多用户通信网。但是双密钥算法较单钥密钥算法处理速度慢得多，因此，常把双密钥密码技术与单密钥密码技术结合起来实现最佳性能，即用双密钥密码体制在通信双方传送加密密钥，而用单加密密码技术对实际传输的数据进行加解密。

1.4.2 分组密码和序列密码

根据明文消息的加密形式的不同，密码体制可分为分组密码和序列密码。

分组密码就是将明文分成固定长度的组，比如 64 比特为一组，用同一密钥和算法对每一组加密，输出也是固定长度的密文。数据加密标准 DES 算法[3]以及公开密钥 RSA 算法[18]是分组密码系统的典型。

序列密码是将消息分成连续的符号或比特： $m=m_0,m_1,\cdots$ 用密钥流 $k=k_0,k_1,\cdots$ 的第 i 个元素 k_i 对 m_i 加密，即存在 $E_k(m)=E_{k0}(m_0),E_{k1}(m_1)\cdots$。如果密钥流经过 N 个符号之后重复，则称该序列密码是周期的，否则称为非周期的。一次一密密码是非周期的。

分组密码与序列密码的主要区别在于记忆性。(见图 1.2)。分组密码中，固定的加密密钥决定了相同的明文组对应相同的密文组。在序列密码中，由于密钥流元素 k_j 产生有第 j 时刻序列密码的内部状态和密钥 k 所决定，可表达为 $k_j=f(k,\sigma_j)$。因此在序列密码中，明文的重复部分是用密钥流不同部分加密的。

与分组密码相比，序列密码有以下优点：

① 加解密速度快，易于硬件实现，实现成本低；

② 错误扩散低，更适合于高准确传输环境中。

因而，在实际应用中序列密码占主导地位。虽然现在公开发表的文献中大多数是分组密码的研究，这主要是因为序列密码在军事、外交等领域中得到了广泛的应用而不便于公开。由于上述的优点，序列密码在实际应用中将得到广泛的应用。

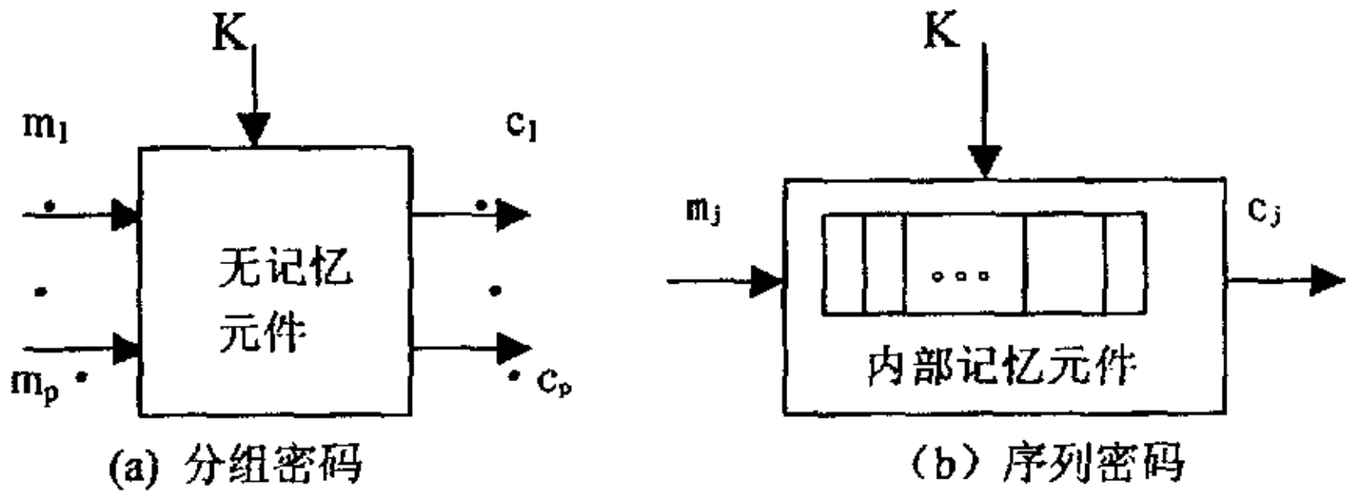


图 1.2 分组密码和序列密码的比较

Fig.1.2 The comparison between block cipher and stream cipher

1.5 本论文研究的主要内容和结构

本论文着重于研究如何将混沌技术应用于传统序列密码。主要包括以下几个方面：

第一章主要介绍密码技术的进展，包括混沌密码的进展，讨论了密码系统的数学模型和安全性理论和密码体制的分类；

第二章讨论序列密码的基本概念、原理和设计的方法，主要研究了线性移位寄存器序列和 m-序列的性质和在序列密码中的应用；

第三章介绍了混沌的起源应用前景、特征和混沌模型，主要研究刻划混沌的特征量，包括 Poincare 截面法、功率谱法、Lyapunov 指数、分维数分析法、

Kolmogorov 熵；

第四章首先介绍混沌加密原理和方法，并和传统加密原理作比较，讨论 Logistic-map 混沌序列的性能，指出 m-序列和混沌序列存在的问题。在此基础上把混沌序列和 m-序列结合起来提出混合混沌序列密码的设计和实现并对混合混沌序列做了比较分析与实验，它包括混合混沌序列的随机性、平衡性、游程特性、自相关和互相关函数及线性复杂度等多项指标。并对该系统的安全性能进行了深入分析，如扩散扰乱特性、密钥空间、弱密钥问题和抗密码学分析等；

第五章研究了如何利用混合混沌序列进行图像加密，提出了一种基于混合混沌序列的多级图像加密算法，并对该算法进行详细的设计和分析；

第六章对论文作了总结，并对今后的研究工作进行了展望。

2 序列密码理论

序列密码是单钥体制的一类，也是密码技术的一个重要分支。序列密码就是将密钥、明文表示成连续的符号或比特流，对应地进行加密。和分组密码相比，序列密码加/解密速度快，且容易硬件实现，因而是一种广泛应用的密码系统。本章将介绍序列密码的一些基本概念、以及密钥序列流必须满足的一些基本性质。

2.1 序列密码的基本概念

2.1.1 序列密码原理

由于各种消息(报文、语音、图象和数据等)都可以经过量化编码等技术转化为二进制数字序列，因此我们假设序列中的明文空间 M 、密文空间 C 和序列空间 K 都是由二进制数字序列组成的集合。那么一个序列密码系统可用 (M,C,K,E_k,D_k,Z) 的六元组来描述。对于每一个 $k\in K$ ，由算法 Z 确定一个二进制密钥序列 $z(k)=z_0,z_1,z_2\cdots$ ，当明文 $m=m_0,m_1,\cdots m_{n-1}$ 时，在密钥 k 下的加密过程为：对 $i=0,1,2\cdots n-1$ ，计算 $c_i=m_i\oplus z_i$ ，密文为 $c=E_k(m)=c_0,c_1,c_2\cdots c_{n-1}$ ，其中 $\oplus$ 表示模 2 加；解密过程为： $i=0,1,2\cdots n-1$ ，计算 $m_i=c_i\oplus z_i$ ，由此恢复明文 $m=D_k(c)=m_0,m_1,m_2\cdots m_{n-1}$ 。图 2.1 给出了序列密码保密通信模型。

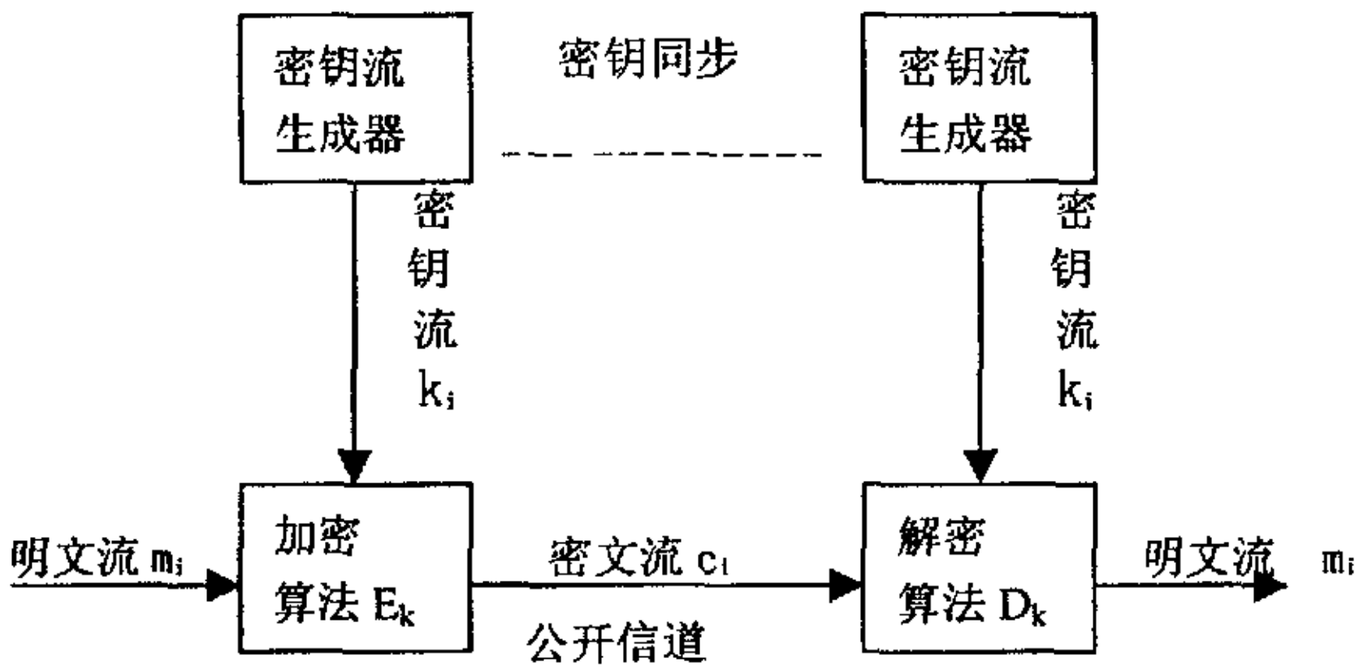


图 2.1 序列密码保密通信模型

Fig.2.1 The stream cipher of secure communication model

由上述可知，序列密码的安全性主要依赖于密钥序列 $z(k)=z_0,z_1,z_2\cdots$ ，因此序列密码系统设计的关键是如何设计出离散无记忆的二进制均匀分布的随机序列。但是，密码应用中不但不可能产生真正的随机序列，也不可能产生无限长序列，也就是说，实际使用中的序列都是周期的，但是只要序列的周期足够大，比

特随机足够好，就已满足密钥技术应用的要求了。所以我们讨论一种所谓的伪随机序列。

2.1.2 序列随机性概念

设有二进制序列$\{k_i\}$，其中$k_i \in \{0,1\}$，如果存在正整数 T，使得对于$\forall i$，$k_{i+T} = k_i$，则称$\{k_i\}$为周期序列，满足上述关系的最小 T 称为序列的周期。

若序列$\{k_i\}$，除开始若干项后的其余部分是周期序列，则此序列成为准周期序列。

定义 2.1.1 在序列$\{k_i\}$的一个周期中，若

$$k_{t-1} \neq k_t = k_{t+1} = \cdots = k_{t+l-1} \neq k_{t+l} \tag{2.1}$$

则称（$k_t, k_{t+1}, \cdots k_{t+l-1}$）为序列的一个长为$l$的游程。

定义 2.1.2 周期为T的序列$\{b_i\}$的周期自相关函数定义为

$$R(j) = \frac{A - D}{T} \tag{2.2}$$

式中，$A = |\{0 \le i < T : b_i = b_{i+j}\}|$，$D = |\{0 \le i < T : b_i \neq b_{i+j}\}|$，$A$表示序列$\{b_i\}$和$\{b_{i+j}\}$中相同的位的数目，$D$表示序列$\{b_i\}$和$\{b_{i+j}\}$中不同的位的数目。当$j$为$T$的倍数时，$R(j)$为自相关函数，$R(j) = 1$；当$j$不是$T$的倍数时，$R(j)$为异相自相关函数。

周期为T的伪随机二进制序列应满足 Golomb 提出的三条随机性公设[20]：

① 若T为奇数，则序列$\{k_i\}$一个周期内 0 的个数和 1 个数相差 1；若T为偶数，则 0 个数和 1 的个数相等。

② 长度为T的周期内，1 游程的个数占游程总数的1/2，2 游程的个数占游程总数的$1/2^2$，…，d游程的个数占游程总数的$1/2^d$，而任意长度的 0 的游程个数与 1 的游程个数相同。

③ 序列的异相自相关函数$R(j)$是一个常数。

公设①和②的意义很明确，主要用于衡量序列的平衡性和随机性，而公设③意味着对序列与其平移后的序列作比较，不能获取其它任何信息。满足以上三个条件的序列成为伪随机序列（Pseudo Random Sequence），也称为伪噪声序列(Pseudo Noise Sequence，PN 序列)。

密钥序列往往是个准周期的伪随机序列，但为了满足密码体制的要求，密钥序列除了满足上面的三个条件外，还要符合以下三个要求[21]。

① 周期 T 要足够大，如大于10^{50}；

② 序列的产生易于高速生成；

③ 当序列的任何部分暴露时，要分析整个序列，提取产生它的电路结构信息在计算上是不可行的，即序列的线性不可预测充分大。

其中的第三点要求确定了密码的强度，是序列密码的核心，它包含了序列密码

要研究的许多主要问题，如线性复杂性、相关免疫性、不可预测性等。

寻找生成一个具有良好随机特性密码序列的方法是序列密码技术和理论研究的重要工作。常见的方法有：线性移位寄存器、非线性移位寄存器、有限自动机、线性同余等方法和最近提出的混沌序列密码技术。其中线性移位寄存器是现代序列密码体制的基础，因此在下面我们将扼要进行介绍。

2.2 线性反馈移位寄存器序列

2.2.1 线性反馈移位寄存器的概念

定义 2.2.1 设 $f(x_1,x_2,\cdots,x_n)=c_1x_n\oplus c_2x_{n-1}\oplus\cdots\oplus c_nx_1$ 是一个线性函数，$c_i,x_i\in\{0,1\}$，$i=0,1,2\cdots$，其中的加号表示异或。对于给定的初始状 $s_0=(a_1,a_2,\ldots,a_n)$ $a_{i+n+1}=f(a_{i+1},a_{i+2},\cdots,a_{i+n})=c_1a_{i+n}+c_2a_{i+n-1}+\cdots+c_na_{i+1},i=0,1\cdots$ 称为一个 n 级线性反馈移位寄存器 n-LFSR(Linear Feedback Shift Register)，f 成为反馈函数，$c_1,c_2\cdots,c_n$ 成为反馈系数。如果 $f(x_1,x_2,\cdots,x_n)=c_1x_n\oplus c_2x_{n-1}\oplus\cdots\oplus c_nx_1$ 不是线性函数，则称该反馈移位寄存器是一个非线性反馈移位寄存器 NLFSR(Nonlinear Linear Feedback Shift Register)。

由此得到一个输出序列 $a_1,a_2,\cdots,a_{n-1},a_n,\cdots,a_i,\cdots$，和 $s_1,s_2,\cdots,s_{n-1},s_n,\cdots,s_i,\cdots$，$s_i=(a_i,a_{i+1},\cdots,a_{i+n-1})$，$i=0,1,2\cdots$。

图 2.2 是 n-LFSR 的示意图，可以看出，一个 n-LFSR 的输出序列的性质完全由其反馈函数决定的，一个 n-LFSR 最多可以输出 2^n 个不同状态。而若初始状态全为 0，状态下不会转入其它状态，所以输出序列最长的周期 2^n-1，这个最大周期的序列称为 m-序列。m-序列具有很好的随机统计特性，它满足 Golomb 的三个伪随机公设[20]。

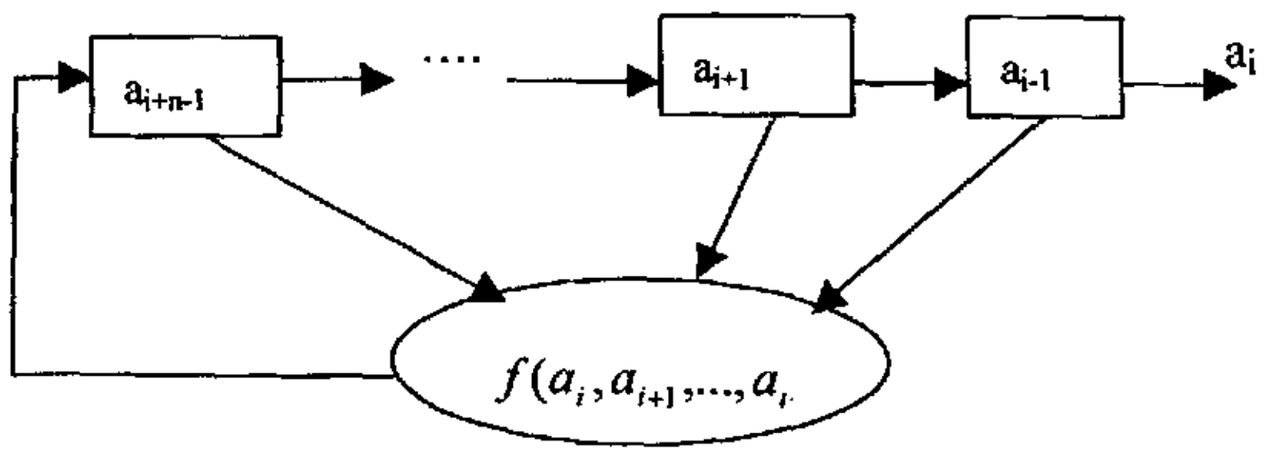


图 2.2 线性反馈移位寄存器

Fig.2.2 Linear Feedback Shift Register

2.2.2 LFSR 的特征多项式

定义 2.2.2 设 LFSR 的反馈系数为 $c_1,c_2,\cdots,c_n$，即

$a_{i+n+1}=c_1a_{i+n}+c_2a_{i+n-1}+\cdots+c_na_{i+1},i=0,1,2,\cdots$ 则 $p_n(n)=1+c_1x+c_2x^2+\cdots+c_nx^n$

称为 $LFRS\{a_i \mid i=0,1,2\}$ 的特征多项式。

LFSR 的特征多项式是描述该线性移位寄存器结构特征的数学模型，n-LFSR 由特征多项式决定，同时也决定着 n-LFSR 输出序列的特性。关于 n-LFSR 的输出序列和它的特征多项式之间有如下几个重要定理[22]：

定理 2.2.1 若 $p_n(x)$ 是 GF(2)上的 n 次多项式，也是序列 $\{a_i\}$ 的特征多项式，且存在关系 $p_n(x)|(x^m+1)$，则 $\{a_i\}$ 的周期 r 满足 $r|m$。符号“|”表示整除。

定理 2.2.2 n 级线性移位寄存器产生的状态序列有最大周期 2^n-1 的必要条件是其特征多项式是不可约的。

定理 2.2.3 若 $p_n(x)$ 是不可约多项式，且存在 $p_n(x)|(x^m+1)$,但对于任意正整数 k<m，$p_n(x)$ 不整除 x^k+1，则由 $p_n(x)$ 产生的序列 $\{a_i\}$ 的周期为 m。

从定理 2.2.3 中知道，如果一个 n-LFSR 产生一个周期为 2^n-1 的 m-序列，那么它的特征多项式是不可约的。但并非所有的不可约多项式都能够生成 m-序列，即定理 2.2.3 的逆命题不真。由于 m-序列的长周期和良好的随机统计特性，因此在序列密码中具有重要意义。那些能够生成 m-序列的不可约多项式称为本原多项式。

2.2.3 本原多项式

定义 2.2.3 设 $p_n(x)$ 为 n 次多项式，则 $l=\min\{k: p_n(x)|(x^k+1)\}$ 称为多项式 $p_n(x)$ 的阶。阶为 2^n-1 的不可约多项式称为本原多项式。

定理 2.2.4 设 $\{a_i\}\in a(p_n(x))$，则 $\{a_i\}$ 为 m-序列的充要条件是 $p_n(x)$ 为本原多项式。

证明：

充分性：

若 $p_n(x)$ 是本原多项式，其阶为 2^n-1，由定理 2.2.3 可知，$\{a_i\}$ 的周期等于 $p_n(x)$ 的阶，即 2^n-1，根据 m-序列的定义，$\{a_i\}$ 是 m-序列。

必要性：

若 $\{a_i\}\in a(p_n(x))$ 的周期为 2^n-1，由定理 2.2.2 可知，2^n-1 整除 $p_n(x)$ 的阶，而 $p_n(x)$ 的阶不超过 2^n-1，故 $p_n(x)$ 的阶必是 2^n-1。

若 $p_n(x)$ 可约，设 $p_n=q_1*q_2$，$q_1(x)$ 不可约，其次数 k<n。显然 $a(q_1(x))\subset a(q_2(x))$，这样，$\{a_i\}\in a(q_1(x))$，一方面周期应为 2^n-1，另一方面又不应超过 2^k-1，矛盾。故 $p_n(x)$ 是不可约的。

命题证得。

2.2.4 线性复杂度

定义 2.2.4 $GF(2)$ 上的有限长序列 $a=a_0a_1\cdots a_{n-1}$ 的线性复杂度 $L(a)$ 定义为：

$$L(a)=\min\{n \mid \text{存在}GF(2)\text{上的}n\text{级}LFSR\text{序列}a\}$$

可见，有限长序列 $\{a_i\}$ 的线性复杂度 $L(s)$ 是产生该序列的 $GF(2)$ 上级数最少

的线性移位寄存器的级数，对于全零序列a，约定 L(a)=0。对m－序列而言其线性复杂度就是构成该序列的移位寄存器阶数n。线性复杂度与序列的特征多项式关系有如下定理：

定理 2.2.5 设$a=\{a_i\}$是 GF(2)上的周期序列，且序列$\{a_i\}$的线性复杂度$L(a)$=n，则只要知道$\{a_i\}$中任意相继的 2n 位就可以确定整个序列$\{a_i\}$及产生$\{a_i\}$的多项式$p_n(x)$。

证明：设已知 2n 位为$a_0,a_1,a_2,...a_{2n-1}$，设 n—LFSR 的递归关系为：

$$a_i=\sum_{j=i}^{n}c_j a_{i-j} \qquad i=n,n+1,\cdots$$

，

则可得到关于$c_1,c_2,\cdots c_n$的线性方程组：

$$\begin{cases} a_n=c_1a_{n-1}+c_2a_{n-2}+...+c_na_0 \\ a_{n+1}=c_1a_n+c_2a_{n-1}+\cdots+c_na_1 \\ ..... \\ a_{2n-1}=c_1a_{2n-2}+c_2a_{2n-3}+...+c_na_{n-1} \end{cases}$$

容易看出，$\Delta=\begin{vmatrix} a_{n-1} & a_{n-2} & \cdots & a_0 \\ a_n & a_{n-1} & \cdots & a_1 \\ \cdots & \cdots & \cdots & \cdots \\ a_{2n-2} & a_{2n-3} & \cdots & a_{n-1} \end{vmatrix}\neq 0$，否则$a_n,a_{n+1},\cdots a_{2n-1}$将线性相关，

于是$\{a_i\}$可以用少于 n 级的线性移位寄存器产生，即$L(a)$<n，和假设矛盾。因此$\Delta\neq 0$成立，上述方程有解。

解此方程组，即可得$c_1,c_2,\cdots,c_n$和特征多项式$p_n(x)$。

从以上分析可以看出：对于一个线性复杂度为n的序列，只要知道$2n$密文的情况下，密码分析者就可以通过解线性方程组或借助 B-M 算法找到该 m-序列的特征多项式，从而可以确定整个序列，实现对系统的破译。

定理 2.2.6 序列的线性复杂度存在如下基本性质[23]：

设n长序列$\{s\}$和l长序列$\{t\}$分别是$GF(2)$上的两个有限长序列，则

① 对任何$n\geq 1$，n长序列$\{s\}$的线性复杂度$L(s)$满足$0\leq L(s)\leq n$；

② 序列$\{s\}$的线性复杂度$L(s)=0$当且仅当序列$\{s\}$为零序列；

③ 序列$\{s\}$的线性复杂度$L(s)=n$当且仅当序列$\{s\}$=$\{0,0,\cdots 0,1\}$；

④ 如果序列$\{s\}$是周期为N的序列，则$L(s)\leq N$；

⑤ $L(s \oplus t) \le L(s) + L(t)$， $s \oplus t$ 表示序列 s 和 t 按位异或。

定理 2.2.7 n 长独立等概同分布的二进制随机序列 $\{s\}$ 的线性复杂度 $L(s)$ 有以下特性[23,24]：

$$E(L(s)) = \frac{n}{2} + \frac{1}{4} + \frac{(-1)^n}{36} + O(n2^{-n}) \tag{2.3}$$

$$\lim_{n\to\infty} E(L(s)) = \frac{n}{2} \tag{2.4}$$

$$Var(L(s)) = \frac{86}{81} + O(n2^{-n}) \tag{2.5}$$

$$\lim_{n\to\infty} Var(L(s)) = \frac{86}{81} \tag{2.6}$$

其中 $E(L(s))$ 表示序列 $\{s\}$ 的线性复杂度的期望值，$Var(L(s))$ 表示序列 $\{s\}$ 的线性复杂度的方差。

定理 2.2.7 说明，对于长度为 n 的序列，其线性复杂度逼近于 $n/2$，并且不论序列有多长，其线性复杂度的方差都逼近于一个常数。

2.2.5 计算序列线性复杂度的 B-M 算法

Berlekamp-Massey 算法由 J.L.Massey 在 1969 年提出，其核心思想是用数学归纳法求得的一系列线性移位寄存器。算法描述[25]如下：

任意给定一个长为 N 的二元序列 $a_0, a_1, \cdots, a_{N-1}$，用 $\langle F_n(x), r_n \rangle$ 表示特征多项式为 $F_n(x)$ 并且复杂度为 r_n 的伪随机移位寄存器序列，$n = 1,2,\cdots,N$。

① 设 n_0 是个非负整数，使

$$a_0 = a_1 = \cdots = a_{n_0-1} = 0, \quad a_{n_0} \neq 0$$

则令

$$d_0 = d_1 = \cdots = d_{n_0-1} = 0, \quad d_{n_0} = a_{n_0}$$

并令

$$F_1(x) = F_2(x) = \cdots F_{n_0}(x) = 1$$

$$r_1 = r_2 = \cdots = r_{n_0} = 0$$

同时可以取任意一个 n_0+1 级线性移位寄存器作为 $\langle F_{n_0+1}(x), r_{n_0+1} \rangle$，可令

$$F_{n_0+1}(x) = 1 + x^{n_0+1}, \quad r_{n_0+1} = n_0 + 1$$

② 不妨设 $\langle F_i(x), r_i \rangle$， $i = 1,2,\cdots,n(n_0 < n < N)$ 都已求得，

而

$$r_1 = r_2 = \cdots = r_{n_0} < r_{n_0+1} \le r_{n_0+2} \le \cdots \le r_n$$

令

$$F_n(x) = 1 + c_{n_1}x + c_{n_2}x^2 + \cdots + c_{n_{r_n}}x^{r_n}$$

计算

$$d_n = a_n + c_{n_1}a_{n-1} + c_{n_2}a_{n-2} + \cdots + c_{n_{r_n}}a_{n-r_n}$$

d_n 称为第 n 步的差值。有以下两种情况：

1) $d_n = 0$，则 $F_{n+1}(x) = F_n(x)$，$r_{n+1} = r_n$

2) $d_n \neq 0$，这时取 $m(n_0 \leq m < n)$，使

$$r_m < r_{m+1} = r_{m+2} = \cdots = r_n,$$

并令

$$F_{n+1}(x) = F_n(x) + x^{n-m}F_m(x),$$

$$r_{n+1} = \max\{r_n, n+1-r_n\}。$$

最后得到产生序列 $a_0, a_1, \cdots, a_{N-1}$ 的一个最短线性移位寄存器 $\langle F_N(x), r_N \rangle$。

③ 序列的复杂度即为 r_N。

例 2.2.5 求序列 011001010 的最短线性移位寄存器和线性复杂度。

解： 设 $a_0 = 0, a_1 = 1, a_2 = 1, a_3 = 0, a_4 = 0, a_5 = 1, a_6 = 0, a_7 = 1, a_8 = 0$，由 B-M 算法求这个序列的线性复杂度（采用基于模 2 加法）：

① $d_0 = a_0 = 0$，$F_1(x) = 1$，$r_1 = 0$.

② $d_1 = a_1 = 1$，$F_2(x) = 1 + x^2$，$r_2 = 2$.

③ $d_2 = a_2 + 0 \cdot a_1 + 1 \cdot a_0 = 1$，因为 $r_1 = 0 < r_2 = 2$，所以

$F_3(x) = F_2(x) + x^{2-1}F_1(x) = 1 + x + x^2$，$r_3 = \max\{r_2, 2+1-r_2\} = 2$.

④ $d_3 = a_3 + 1 \cdot a_2 + 1 \cdot a_1 = 0$，$F_4(x) = F_3(x) = 1 + x + x^2$，$r_4 = r_3 = 2$.

⑤ $d_4 = a_4 + 1 \cdot a_3 + 1 \cdot a_2 = 1$，因为 $r_1 = 0 < r_2 = r_3 = r_4 = 2$，所以

$F_5(x) = F_4(x) + x^{4-1}F_1(x) = 1 + x + x^2 + x^3$，$r_5 = \max\{r_4, 4+1-r_4\} = 3$.

⑥ $d_5 = a_5 + 1 \cdot a_4 + 1 \cdot a_3 + 1 \cdot a_2 = 0$，$F_6(x) = F_5(x) = 1 + x + x^2 + x^3$，

$r_6 = r_5 = 3$.

⑦ $d_6 = a_6 + 1 \cdot a_5 + 1 \cdot a_4 + 1 \cdot a_3 = 1$，因为 $r_4 = 2 < r_5 = r_6 = 3$，所以

$F_7(x) = F_6(x) + x^{6-4}F_4(x) = 1 + x + x^4$，$r_7 = \max\{r_6, 6+1-r_6\} = 4$.

⑧ $d_7 = a_7 + 1 \cdot a_6 + 0 \cdot a_5 + 0 \cdot a_4 + 1 \cdot a_3 = 1$，因为 $r_6 = 3 < r_7 = 4$，所以

$F_8(x) = F_7(x) + x^{7-6}F_6(x) = 1 + x^2 + x^3$，$r_8 = \max\{r_7, 7+1-r_7\} = 4$.

⑨ $d_8 = a_8 + 0 \cdot a_7 + 1 \cdot a_6 + 1 \cdot a_5 = 1$，因为 $r_6 = 3 < r_7 = r_8 = 4$，所以

$F_9(x) = F_8(x) + x^{8-6}F_6(x) = 1 + x^4 + x^5$，$r_9 = \max\{r_8, 8+1-r_8\} = 5$.

因此 $\langle 1 + x^4 + x^5, 5 \rangle$ 就是产生所给序列的一个最短线性移位寄存器，序列的线性复杂度为 5。

下面的定理给出了由 B-M 算法产生给定序列的最短线性移位寄存器是否唯一的充要条件。

定理 2.2.8 对于给定 N 长二元序列 $a_0, a_1, \cdots, a_{N-1}$，假定产生该序列的最短线性移位寄存器的级数是 r_n，于是产生该序列的最短线性移位寄存器唯一的充分必要

条件是：$r_n \le N/2$.

推论 2.2.8 设r_n是产生序列$a_0, a_1, \cdots, a_{N-1}$的最短线性移位寄存器的级数，且$r_n \le N/2$，于是按 B-M 算法所求的$\langle F_{2r_n}(x), r_{2r_n} \rangle$即为产生$a_0, a_1, \cdots, a_{N-1}$的唯一最短线性移位寄存器。

在随后的内容中我们将利用 B-M 算法计算混合混沌序列的线性复杂度。

2.3 基于 n-LFSR 的密钥流生成器的一般结构

由前面分析可知，线性反馈移位寄存器生成的 m-序列的线性复杂度非常有限，用其直接构造密码系统容易被破解，因此单独的线性反馈移位寄存器不是适宜于作为安全的密钥流生成器，必须在生成器中使用非线性变换。Rueppel[26]给出了如图 2.3 的基于线性移位寄存器的密钥生成器的框图。

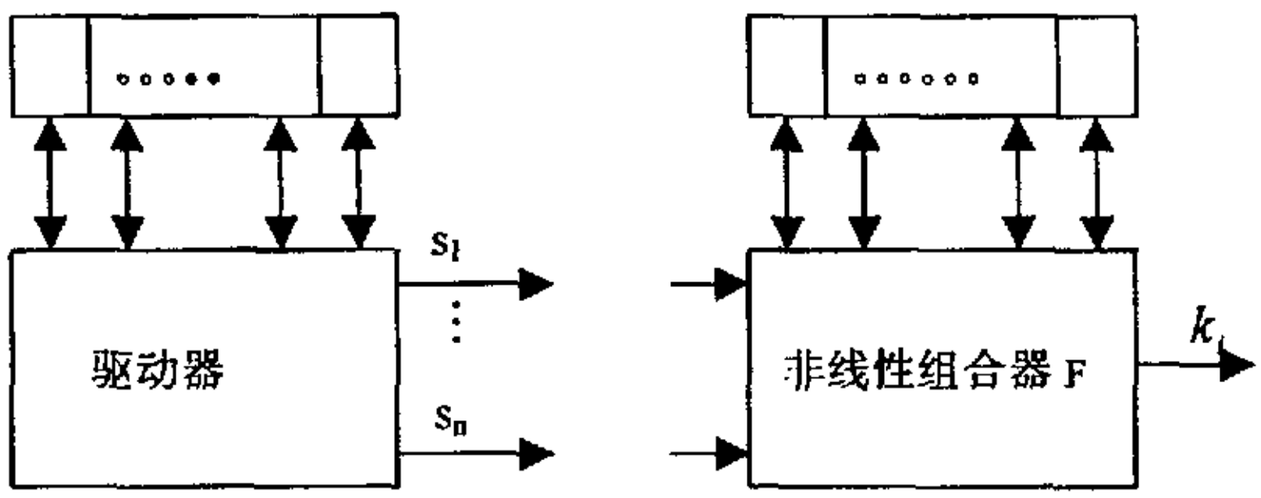


图 2.3 密钥流生成器结构

Fig.2.3 The key stream generator structure

从图中可以看出密钥流生成器有两部分组成：驱动部分和非线性部分。驱动部分产生控制生成器的状态序列$s_1, s_2, \cdots, s_n$，它由一个和多个长周期线性反馈移位寄存器构成，它将控制生成器的周期和统计特性。非线性组合部分对驱动器的各个输出序列进行非线性组合，提高生成器输出序列的统计特性、线性复杂度和不可预测性等，从而保证输出序列的强度。

为了保证输出密钥流的强度，对组合函数 F 有以下要求：

① F 将驱动序列变换位滚动密钥序列，当输入位二元随机序列时，输出序列也为随机序列；

② 当输入序列的周期给定时，组合函数 F 使输出序列的周期尽可能大；

③ 当输入序列的复杂度给定时，组合函数 F 使输出序列的复杂度尽可能大；

④ 组合函数 F 的信漏极小化（从输出序列难以提取密钥流生成器的结构信息）；

⑤组合函数 F 应便于工程实现，且工作速度极高；

⑥在需要时，组合函数 F 易于在密钥下控制工作。

解决在 LFSR 基础上非线性化的最常用方法是：非线性滤波序列、钟控序列和非线性组合序列生成器。在下一章中，我们将讨论如何用混沌系统来构造密钥流生成器。

2.4 小结

本章介绍了序列密码的基本原理之后，讨论了序列密码中密钥序列主要的特性。之后介绍了作为现代序列密码理论基础的线性反馈移位寄存器理论及其 m-序列的特性，最后简单介绍了以移位寄存器为基础的序列密钥流生成器的一般结构。

3 混沌理论基础

目前混沌已成为当今学术研究的热点和前沿课题，其涉及自然科学与社会科学的几乎各个领域。与 n-LFSR 产生的序列相比，混沌序列具有更好的随机性、周期性长、保密性及复杂度高等特点，更适合与密码学的应用。本章主要介绍混沌的概念、特点，并给出一些常见的混沌模型，为后面的研究做准备。

3.1 混沌的起源与应用前景

3.1.1 混沌学的起源[27]

本世纪六十年代混沌理论产生于数学与物理领域，它与相对论、量子论一起被誉为二十世纪三大科学革命。它打破了确定理论和随机理论之间不可逾越的界限，揭示了自然界及人类社会普遍存在的复杂性，是有序与无序的统一，确定与随机的统一。

1963 年，美国气象学家 E.N.Lorenz 在研究大气对流模型时，通过长期反复的数值实验和计算机模拟，在耗散系统中首先发现了混沌运动。1963 年它发表了著名论文《确定性非周期流》，以后又陆续发表了三篇论文，这组论文成为研究耗散系统混沌现象的经典文献，为以后的混沌研究开辟了道路。

20 世纪 70 年代开始，混沌学研究终于在多个学科领域同时展开，形成了世界性的热潮。1971 年，法国的 D.Ruelle 和荷兰的 F.Takenes 联名发表了著名论文《论湍流的本质》，在学术界第一次提出用混沌描述湍流形成机理的新观点，并证明了 Lev D.Laudau 关于湍流发生机制的权威理论的不正确性，起着重要解放思想的作用。生物学家，特别是种群生态学家，对建立混沌学有着特殊贡献，他们在研究种群演化的动力学材料中建立的 Logistic 方程的数学模型，是 70 年代研究混沌十分理想的典型“标本”。1973 年，法国数学家 B.Mandelbrot 正式提出了分形与分形几何的概念，他的工作为混沌探索者们描绘种种不规则的、回转曲折的相空间以理想的工具，强有力地推动混沌走向高潮。1975 年，正在美国马里兰大学攻读博士学位的华人李天岩和他的导师 J.Yorke 联名发表了一篇震动学术界的论文《周期 3 蕴含着混沌》[28]，这是一个关于混沌的数学定理，定理描述了混沌的数学特征，为以后一系列的研究开辟了方向。1977 年，第一届国际混沌会议在意大利召开，标志着混沌科学地诞生。

20 世纪 80 年代以来混沌学研究出现了更大的热潮，《科学美国人》、《科学》、《新科学家》、《自然》的杂志纷纷介绍混沌理论，专业学术刊物包括我国的《物理学报》、《物理学进展》等也大量的刊登混沌学研究的论文。20 多年来，混沌研

究的论文发表了7000多篇，出版了专著和文集近300部，其中也包括了以郝柏林院士为代表的一大批我国学者的研究成果。如今，对混沌现象的认识，是非线性科学最重要的成就之一，混沌概念与分形，孤立子、元细胞自动机等概念并行，成为探索复杂性的重要范畴。

3.1.2 混沌学的应用前景

进入20世纪90年代后，混沌科学与其他科学相互渗透，无论在生物学、生理学、心里学、数学、物理学、化学、电子学、信息科学，还是天文学、气象学、经济学、甚至音乐、艺术等领域，混沌都得到了广泛的应用。混沌在现代科学技术起着十分重要的作用，正如混沌科学倡导者之一，美国海军官员M.Shlesinger所说，“20世纪科学将永远铭记的只有三件事，那就是相对论、量子力学和混沌”第一次混沌国际会议主持人之一，物理学家J.Ford 认为混沌就是20世纪物理学第三次最大的革命。与前两次革命相似，混沌也与相对论及量子力学一样冲破了牛顿力学的教规。他说：“相对论消除了关于绝对空间与时间的幻想；量子力学则消除了关于可控测量过程的牛顿式的梦；而混沌则消除了拉普拉斯关于决定式可预测性的幻想。

混沌应用可分为混沌综合和混沌分析。前者利用人工产生的混沌从混沌动力学系统中获得可能的功能，如人工神经网络的联想记忆等；后者由复杂的人工和自然系统中获得的混沌信号并寻找隐藏的确定性规则，如时间序列数据的非线性确定性预测等。混沌的具体的应用[29]可概括如下：

① 优化：利用混沌运动的随机性、遍历性和规律性寻找最优点，可用于系统辨识、最优参数设计等众多方面。

② 神经网络：将混沌与神经网络相融合，使神经网络由最初的混沌状态逐渐退化到一般的神经网络，利用中间过程混沌状态的动力学特性使神经网络逃离局部极小点，从而保证全局最优，可用于联想记忆、机器人的路径规划等。

③ 图像数据压缩：把复杂的图像数据用一组能产生混沌吸引子的简单动力学方程代替，这样只需记忆存储这一组动力学方程组的参数，其数据量比原始图像数据大大减少，从而实现了图像数据压缩。

④ 高速检索：利用混沌的遍历性可以进行检索，即在改变初值的同时，将要检索的数据和刚进入混沌状态的值相比较，检索出接近于待检索数据的状态。这种方法比随机检索或遗传算法具有更高的检索速度。

⑤ 非线性时间序列的预测：任何一个时间序列都可以看成是一个由非线性机制确定的输入输出系统，如果不规则的运动现象是一种混沌现象，则通过利用混沌现象的决策论非线性技术就能高精度地进行短期预测。

⑥ 模式识别：利用混沌轨迹对初始条件的敏感性，有可能使系统识别出只

有微小区别的不同模式。

⑦ 故障诊断：根据由时间序列再构成的吸引子的集合特征和采样时间序列数据相比较，可以进行故障诊断。

⑧混沌保密通信：利用混沌信号的编码和解码技术实现混沌信号的保密通讯。此研究已经列入了美国国防的研究计划并正在加紧研制中。

⑨混沌加密：利用混沌序列的非周期性和伪随机特性，将混沌序列作为密钥流和原始明文序列进行逐位异或而得到加密密文。

当然混沌还可用在其它方面。例如，在心脏HRV（心率变异性）的研究方面、语言加工信息的研究方面、对人脑功能以及处理信息的机理方面、流行病数学模型分析方面等，这里就不一一赘述。

混沌学作为一门科学毕竟只有20 余年，因此远未成为一门成熟的科学. 可以预料，混沌学最终将成为人类观察整个世界的一个基本观点，将对人类思维起到解放的作用!

3.2 混沌的定义[30]

混沌(chaos)是非线性系统特有的一种运动形式；它是由确定性系统产生且明感依赖于初始条件的往复稳态非周期运动，类似于随机震动而具有长期不可预测性。

由于混沌系统的奇异性和复杂性至今尚未被人们彻底了解，因此至今混沌还没有一个统一的定义。目前，已有的定义是从不同的侧面反映了混沌运动的性质。

① Li-Yorke 的混沌定义

区间 I 上的连续自映射 $f(x)$，如果满足下面条件，便可确定它有混沌现象：

1). f 的周期点的周期无上界

2). 闭区间 I 上存在不可数子集 S，满足

a. $\forall x,y \in s$，$x \neq y$ 时，$\limsup_{n\to\infty}|f^n(x)-f^n(y)|>0$

b. $\forall x,y \in s$，$\liminf_{n\to\infty}|f^n(x)-f^n(y)|=0$

c. $\forall x \in s$ 和 f 的任意周期点 y，有 $\limsup_{n\to\infty}|f^n(x)-f^n(y)|>0$

② Melnikov 的混沌定义

如果存在稳定流形和不稳定流形且这两种流形横截相交，则必存在混沌。

③ Devaney 的混沌定义

在拓扑意义下，混沌定义为：设 V 是一度量空间，映射 $f:V\to V$，如果满足下面 3 个条件，便函称 f 在 V 上是混沌的。

1). 对初始条件敏感依赖，即($\exists\delta>0$，$\forall\varepsilon>0$，$x\in V$，$\exists y\in U(I)$ 和 $n\in N$，s.t.，$d(f^n(x),f^n(y)>\delta)$)

2). 拓扑传递性(∀开集 Z，Y∈V，存在 k >0，s. t.，) $f^k(z)\cap Y\neq\Phi$

3). f 的周期点在 V 中稠密。

3.3 混沌运动的特征

混沌运动是一种不稳定有限定常运动，即为全局和局部不稳定的运动。这个定义给出了混沌得两个主要特征：不稳定性（该性质可用平均Lyapunov指数大于零来精确刻画）和有限性。或除了平衡、周期和准周期以外的有限定常运动称为混沌运动。这里所谓的定常运动，指的是运动状态在某种意义上（以相空间的有限域为整体来看）不随时间变化。

混沌运动具有通常确定性运动所没有的几何和统计特征，如局部不稳定而整体稳定、无限相似、连续的功率谱、奇怪吸引子、分维、正的Lyapunov指数、正的测度熵等。为了与其他复杂现象区别，一般认为混沌应具有以下几个方面的特征，它们之间有着密不可分的内在联系。

①内随机性：单一频率的输入产生具有连续功率谱的输出。这种遍历性不是出随机外因引起的，而是由确定方程（内因）直接得到的。

② 整体稳定局部不稳定：混沌态与有序态的不同之处在于，它不仅具有整体稳定性，还具有局部不稳定性。稳定性是指系统受到微小的扰动后系统保持原来状态的属性和能力，一个系统的存在是以结构与性能相对稳定为前提。但是，一个系统要进化，要达到一个新的演化状态又不能稳定性绝对化，而应在整体稳定的前提下允许局部不稳定，这种局部不稳定或失稳正是进化的基础。在混沌运动中这一点表现的十分明显。所谓的局部不稳定是指系统运动的某些方面（如某些维度、熵）的行为强烈地依赖于初始条件。

③对初始条件地敏感依赖性：初值的微小地变化，经过很长的时间后，运动可能相差甚远。这意味着混沌运动具有Lyapunov指数下的不稳定。随着时间的推移，任意靠近的各个初始条件将表现各自独立的时间演化，即存在对初始条件的敏感依赖性。Lornez发现，模拟大气动力学的微分方程的解是混沌的，那么就不可能进行长时期的天气预报，因为一个任意小的扰动，犹如蝴蝶翅膀的震动，都有可能在将来某个时候改变地球另一边的天气，这就是著名的蝴蝶效应。

④长期不可预测性： 混沌具有正的Lyapunov指数。由于初始条件的微小差异可能对以后的时间演化产生巨大的影响，因此不可能长期预测将来某一时刻的动力学特性。

⑤奇异吸引子及其分形结构：耗散系统的有效体积在演化过程中将不断收缩至有限分维内（吸引子），耗散是一种整体稳定性因素，而轨道又是不稳定，这就使它在相空间的形状拉伸、扭曲和折叠，形成具有精细的无穷嵌套的自相似结构（分形）。混沌吸引子（奇异吸引子）具有分维性质。

⑥ 轨道不稳定性及分岔：长时间动力运动的类型在某个参数或某个组参数发生变化时也发生变化。这个参数值（或这组参数值）称为分岔点，在分岔点处参数的微小变化会产生不同定性性质的动力学特性，所以系统在分岔点处是结构不稳定的。

⑦普适性：在混沌的转变中出现某种标度不变性，代替通常的空间或时间周期性。所谓普适性，是指在趋向混沌时所表现出来的共同特性，它不依具体的系数以及系统的运动方程而变。普适有两种，即结构的普适性和测度的普适性。前者是指趋向混沌的过程中轨线的分岔情况与定量特性不依赖于该过程的具体内容，而只与它的数学结构有关；后者指同一映象或迭代在不同测度层次之间嵌套结构相同，结构的形态只依赖于非线性函数展开的幂次。

3.4 刻划混沌的特征量[31,32]

混沌来自于系统的非线性性质，但是非线性只是产生混沌的必要条件而非充分条件。混沌研究中，人们关心两个基本问题：（1）以什么判断给定一个系统它具有混沌运动？（2）能否用数学语言说明混沌运动并对它进行定量刻划？混沌复杂性可通过上一节述及的各种特征体现出来，如何判断系统出现混沌，依然是混沌学所研究的重要课题。目前，多采用数值实验来识别动力系统是否存在混沌运动，然后通过工程实验加以验证。本节归纳并阐述从定量角度刻划混沌运动特征的一些方法。

3.4.1 Poincare 截面法

早在十九世纪末，Poincare 就提出了一种方法 Poincare 截面法(Poincare surface of section)，对分析多变量自治系统的运动很有用。基本思想是在多维相空间 $(x_1, dx_1/dt, x_2, dx_2/dt, \cdots, x_n, dx_n/dt)$ 中适当选取一截面，在此截面上某一对共扼变量如 $x_1, dx_1/dt$ 取固定值，称此截面为 Poincare 截面。观测运动轨迹与此截面的截点（Poincare 点），设它们依次为 $P_0, P_1, \cdots, P_n, \cdots$。原来相空间的连续轨迹在 Poincare 截面上便表现为一些离散点之间的映射 $P_{n+1} = TP_n$。由它们可得到关于运动特性的信息。如不考虑初始阶段的暂态过程，只考虑 Poincare 截面的稳态图象，当 Poincare 截面上只有一个不动点和少数离散点是，运动是周期的；当 Poincare 截面上是一封闭曲线时，运动是准周期的；当 Poincare 截面上是成片的密集点时，且有层次结构，运动便是混沌。

3.4.2 功率谱法

谱分析是研究振动和混沌的一个重要手段。根据 Fourier 分析，任何周期为 T 的周期运动 x(t)都可以展成 Fourier 级数。其系数与相应的频率的关系为离散的分立谱，而非周期运动的频率是连续谱。对于随机信号的样本函数，$x(t)$ 的功率谱密

度函数定义为：

$$S_x(\omega)=\int_{-\infty}^{\infty}R_x(\tau)e^{-i\omega\tau}d\tau \tag{3.1}$$

其中 $R_x(\tau)$ 为 $x(\tau)$ 的自相关函数，即：

$$R_x(\omega)=E\{x(t),E(t+\tau)\}=\lim_{T\to\infty}\frac{1}{T}\int_0^T\widetilde{x}(t)\widetilde{x}(t+\tau)dt \tag{3.2}$$

$$\widetilde{x}(t)=x(t)-\lim_{T\to\infty}\int_0^T x(t)dt \tag{3.3}$$

τ 为采样间隔。

对于周期运动，功率谱只在基频及其倍频处出现尖峰。准周期对应的功率谱在几个不可约的基频以及由他们叠加的频率处出现尖峰。混沌运动的功率谱为连续谱，即出现噪声背景和宽峰。由于 $R_x(\tau)$ 与 $S_x(\omega)$ 互为 Fourier 正、反变换，它表示序列相关程度。因此在规则运动情况下，表示运动的函数的序列的自相关函数 $R_x(\tau)$ 具有常数数值和周期振荡，在混沌运动情况下，$R_x(\tau)$ 将指数地迅速减到零。

3.4.3 Lyapunov 指数

Lyapunov 指数在混沌系统研究中的研究意义是：$\lambda>0$，相空间运动轨迹迅速分离发散，长时间运动行为对初始条件敏感，即进入混沌状态；$\lambda=0$ 表示沿着轨迹低于指数速度运动，相当于没有混沌；$\lambda<0$ 表示相空间的轨迹是收缩的，对初始条件不敏感。因此，即使 Lyapunov 指数的大小不知道，Lyapunov 指数的符号类型也能提供动力系统的定性情况。

对于混沌动力系统，λ 的大小与系统的混沌程度有关，假设系统从相空间中某半径足够小的超球开始演变，则第 i 个 Lyapunov 指数定义为：

$$\lambda_i=\lim_{t\to\infty}\log(r_i(t)/r_i(0)) \tag{3.4}$$

式 3.4 中：$r_i(t)$ 为 t 时刻按长度排在第 i 位的椭圆轴的长度；$r_i(0)$ 初始球的半径。换言之，在平均的意义下，随时间的演变，小球的半径会作出如下的改变。

$$r(t)\propto r_i(0)e^{\lambda_i t} \tag{3.5}$$

下面具体介绍一维混沌系统、高维混动系统、最大的 Lyapunov 指数的计算方法。

①一维混沌系统 Lyapunov 指数的计算

考虑一维映射：$x_{n+1}=F(x_n)$，假设 x_n 有偏差 dx_n，并导致 x_{n+1} 偏差 dx_{n+1}，则：

$x_{n+1}+dx_{n+1}=F(x_n+dx_n)\approx F(x_n)+d_n.F^{'}(x_n)$，即：$dx_{n+1}=dx_n.F'(x_n)$

设轨道按指数规律分离，即：

$$|dx_{n+1}|=|dx_n|.e^{\lambda} \tag{3.6}$$

其中λ为 Lyapunov 指数。为了得到稳定的值，通常要取足够的迭代次数：

$$\begin{aligned} dx_n &= d_{n-1}.F'(x_{n-1}) \\ &= dx_{n-2}.F'(x_{n-2}).F'(x_{n-1)}=\cdots \\ &= dx_0.\prod_{i=0}^{n-1}F'(x_i) \end{aligned}$$

因此：

$$\lambda=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln|F'(x_i)| \tag{3.7}$$

② 高维混沌系统 Lyapunov 指数的计算

下面以二维映射为例说明高维混沌系统 Lyapunov 指数的计算方法。设二维混沌系统为：

$$\begin{cases}x_{n+1}=f(x_n,y_n)\\ y_{n+1}=g(x_n,y_n)\end{cases}\quad 或\quad \begin{cases}\dot{x}=f(x,y)\\ \dot{y}=g(x,y)\end{cases} \tag{3.8}$$

设初值(x_0,y_0)及偏差$(\delta x_0,\delta y_0)$，则：

其中 $J_i=\begin{bmatrix}\frac{\partial f}{\partial x} & \frac{\partial f}{\partial y}\\ \frac{\partial g}{\partial x} & \frac{\partial g}{\partial y}\end{bmatrix}_{(x,y)=(x_i,y_i)}$，定义$J=J_0J_1.\cdots J_{n-1}$的特征值维$p_1,p_2$，则：

$$\lambda_i=\frac{1}{n}\ln|p_i| \quad ，\ i=1,2 \tag{3.9}$$

③最大的 Lyapunov 指数的计算

既然判断系统是否混沌可由是否有一个 Lyapunov 指数是正的作出判断，因此只要求出最大 Lyapunov 指数，看它是否为正，就可以判断系统是否做混沌运动，这样可以大大减少计算量。

设两条相轨起点差距为d_0，经过时间τ后，呈指数分离，差距为d_t即：

$$d_\tau = d_0 e^{\tau\lambda} \tag{3.10}$$

则

$$\lambda = \frac{1}{\tau}\ln\frac{d\tau}{d_0} \tag{3.11}$$

定义为 Lyapunov 指数。

数值计算时，从一条参考轨迹上找一个起点，算出相邻相轨的d_0、d_τ，若d_τ不按指数增长，另找新起点算d_0、d_τ，为避免计算时出现发散，经过时间τ后，选取一个新起点，但与参考相轨的距离保持为d_0。这样每次都是从距离为d_0的两状态出发，得到一系列$d_1, d_2, \cdots, d_j, \cdots$最后按下式平均，得到最大 Lyapunov 指数。

$$\lambda_{\max} = \lim_{n\to\infty}\frac{1}{n\tau}\sum_{i=1}^{n}\ln\frac{d_i}{d_0} \tag{3.12}$$

当d_0很小，而循环次数 n 极大时，只要τ不太大，计算结果就与τ的大小无关。得到一个可靠的λ_{max}要有足够的。系统有正的 Lyapunov 指数指数，说明系统出路混沌运动状态。

3.4.4 分维数分析法

分形理论是描述混沌信号的另一种手段，是没有特征长度但具有一定意义的自相似图形的总称。分形最初是 Mandelbrot 在研究诸如弯曲的海岸线等不规则曲线时提出的，之后人们发现自然界普遍存在分形现象，分形最主要的特性是自相似性，即局部与整体以某种相似。

混沌的奇怪吸引子具有不同于通常集合形状是无限层次的自相似结构。这种几何结构可用分维来描述，这样可以通过计算奇怪吸引子的空间维数来研究它的集合性质。

除个别奇怪吸引子的维数接近整数外（如 Lorenz 吸引子的分维约为 2.07），大部分奇怪吸引子具有分数维数。它是表征奇怪吸引子这种具有自相似结构特征的指标之一。分维定义很多，常有以下几种：

① Hausdorff 维数： 它可以用来描述空间、集合以及吸引子的几何性质。n 维空间中的子集的 Hausdorff 维数定义为：

$$d_h = \lim_{a\to 0}\frac{\ln N(a)}{\ln(1/a)} \tag{3.13}$$

其中，N(a)是覆盖集合 s 所需边长为a的 n 维超立方体的最小数目。

Hausdorff 维数的计算一般相当困难，所以说，其在理论上的意义远大于实际意义。

② 盒维数：是应用最广泛的维数概念之一，是因为这种维数的数学计算及经验估计相对容易些。设 S 是 n 维空间中的任意非空有界子集，对每一$r \to 0$，N(s,r)表示用来覆盖 S 的半径为 r 的最小的闭球 数，如果$\lim_{r\to 0}\frac{\ln N(S,r)}{\ln(1/r)}$存在，则 S 的盒维数为：

$$d_b = \lim_{r\to 0}\frac{\ln N(S,r)}{\ln(1/r)} \tag{3.14}$$

盒维数有许多等价的定义，主要在于盒子的选取上，在上述中的盒子选择为闭球，其实根据实际情况可以选择盒子为线段、正方形或立方体。

盒维数特别合适科学计算，数值计算 Logistic 映射$x_{n+1}=3.57x_n(1-x_n)$吸引子的盒维数大约为 0.75(选$r=3\times10^{-6}$)。

③ Lyapunov 维数：从几何直观考虑，具有正 Lyapunov 指数和负 Lyapunov 指数的方向都对张成吸引子起作用，而负 Lyapunov 指数对应的收缩方向，在抵消膨胀方向的作用后，提供吸引子维数的非整数部分。因此，将负 Lyapunov 指数从最大的λ_1开始，把后继的 Lyapunov 指数一个个加起来。 设加到λ_K时，和 $\sum_{i=1}^{K}\lambda_i$ 为正数，下一个λ_{K+1}后，和$\sum_{i=1}^{K}\lambda_i$ 成为负数。利用线性插值确定维数的非整数部分。吸引子的 Lyapunov 指数定义为：

$$d_L = K+\frac{1}{\lambda_{K+1}}\sum_{i=1}^{K}\lambda_i \tag{3.15}$$

其中 K 为使 $\sum_{i=1}^{K}\lambda_i>0$ 成立的最大整数。

Lyapunov 维数对描述混沌吸引子非常有用，对 n 维相空间来说有以下结论：

定常吸引子：$\lambda_1<0,\lambda_2<0,\ldots\lambda_n<0$，此时 Lyapunov 维数为 0，对应于平衡点（不动点）。

周期吸引子：$\lambda_1=0,\lambda_2<0,\lambda_3<0,\ldots\lambda_n<0$，此时 Lyapunov 维数为 1，对应于极限环（周期点）。

准周期吸引子：$\lambda_1=0,\lambda_2=0,\ldots\lambda_k=0,\lambda_{k+1}<0,\ldots\lambda_n<0$，此时 Lyapunov 维数为 k，对应于环面（准周期吸引子）。

混沌吸引子：有$0<k<n$且$S_k<-\lambda_{k+1}\ni\lambda_{k+1}|$，此时 Lyapunov 维数总是分数（$k<d_L<k+1$）。

3.4.5 Kolmogorov 熵（简称为 K 熵）

运动熵可用于混沌程度的识别及其混沌程度的整体度量[33]。混沌运动的初态敏感性，使得相空间中相邻的相轨迹以指数速率分离，初始条件包含的信息会在混沌运动过程中逐渐丢失。另一方面，如果两个初始条件充分靠近且不能靠测量

来区分，但随着时间的演化，他们之间的距离按指数速率增大，使这两条开始被认为“相同的”轨迹最终能区分开来。从这个意义上，混沌运动产生信息。将所有时间的信息产生率作指数平均，即得到 K 熵。

由 K 熵的取值可以判断系统运动的无规则运动的程度。对于确定性系统规则运动（包括不动点、极限环、环面），其 K 熵为 0；对于随机运动，其 K 熵趋于无穷；K 熵为一正数的为混沌运动，K 熵值越大，混沌程度越严重。

3.4.6 混沌系统示例

此处以经典 Logistic 映射 $x_{n+1}=1-ux^2{}_n$ 为例，给出有关混沌吸引子刻划的一些数值计算结果图（见图 3.1-3.4）。如波形图和功率谱（$u=2$ 时），以及 Lyapunov 指数和分岔图等。

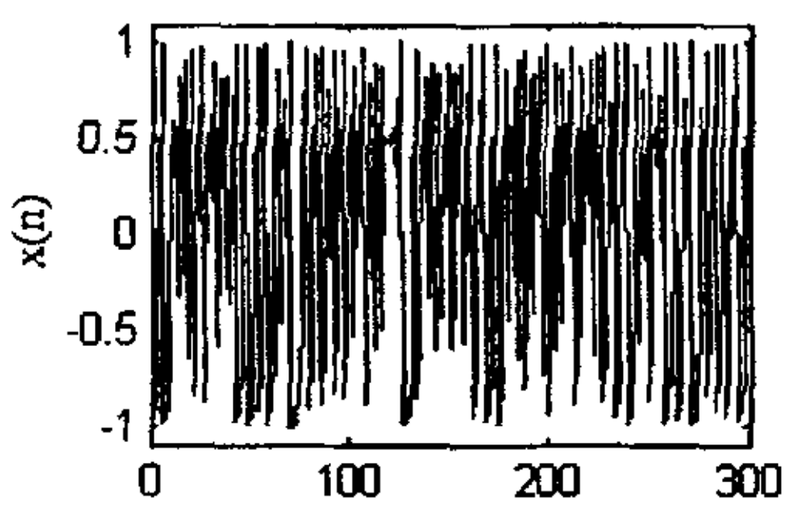


图 3.1 波形图

Fig 3.1 Waveform diagram of x(t)

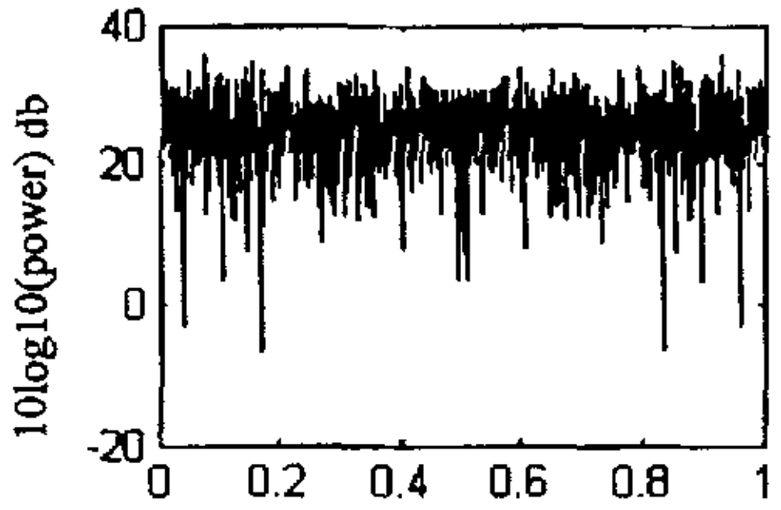


图 3.2 功率谱

Fig 3.2 Power spectrum diagram

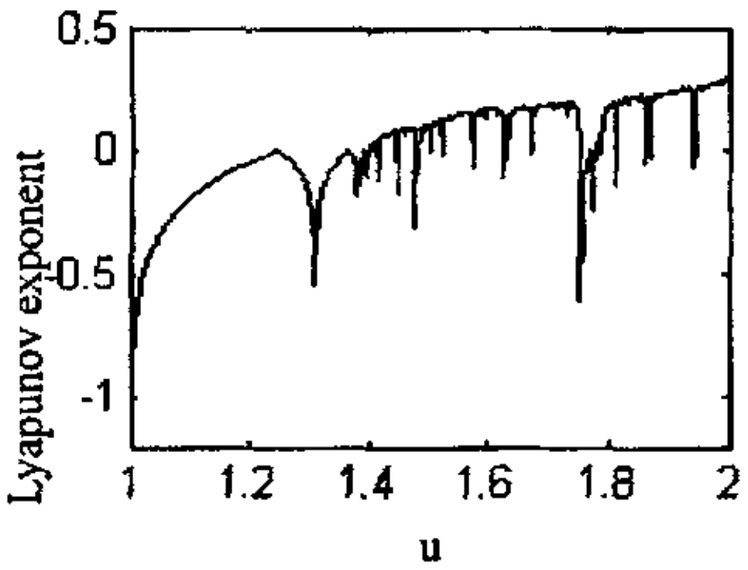


图 3.3 Lyapunov 指数曲线

Fig 3.3 Lyapunov exponent diagram

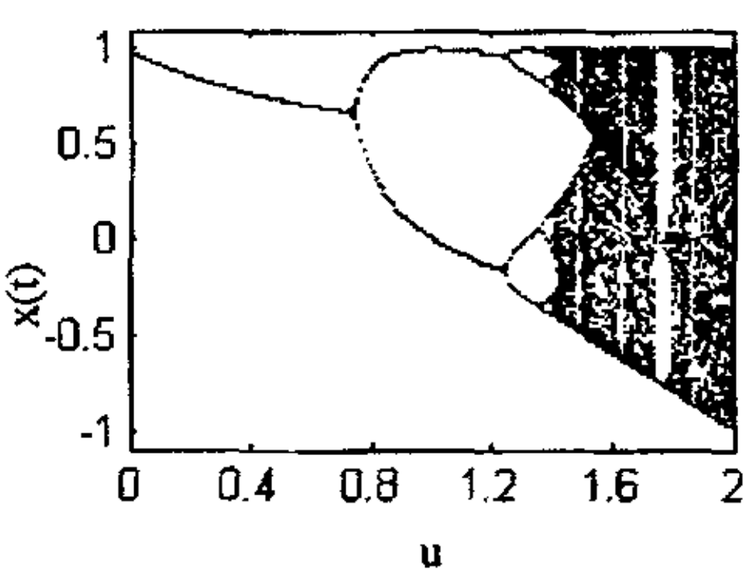


图 3.4 分岔图

Fig 3.4 Bifurcation diagram

3.5 常见的混沌模型

混沌密码技术离不开混沌模型，因此先介绍一下常见的混沌模型。

3.5.1 离散系统混沌模型

① 抛物线映射

抛物线映射是一类混沌映射的统称，通常所说的虫口模型和 Logistic 映射：

$$x_{n+1} = px_n(1-x_n) \tag{3.16}$$

都是抛物线映射。由于它是一维区间映射，却能产生复杂的混沌行为，且研究比较方便，很多文献都对它进行了详尽的阐述。

② Hénon 映射　Hénon 映射的方程为：

$$\begin{cases} x_{n+1} = -px_n^2 + y_n + 1 \\ y_{n+1} = qx_n \end{cases} \tag{3.17}$$

当 p=1.4, q=0.3 时，系统产生混沌现象，图 3.5 为 Hénon 混沌吸引子。

③Arnod 's Cat 映射（Arnod 映射）

$$\begin{cases} x_{n+1} = x_n + y_n \pmod 1 \\ y_{n+1} = x_n + 2y_n \pmod 1 \end{cases} \tag{3.18}$$

它是定义在[0,1]×[0,1] 上的迭代映射，其中（mod 1）运算表示舍去实数的整数部分而只保留小数。

3.5.2 连续系统混沌模型

① Lorenz 方程

$$\begin{cases} \dot{x}_1 = -\sigma x_1 + \sigma x_2 \\ \dot{x}_2 = -x_2 + rx_1 - x_1x_3 \\ \dot{x}_3 = -bx_3 + x_1x_2 \end{cases} \tag{3.19}$$

当$\sigma = 10$，$r = 28$，$b = 8/3$时的混沌吸引子见图 3.6；

②Chen 电路

$$\begin{cases} \dot{x}_1 = -ax_1 + ax_2 \\ \dot{x}_2 = cx_2 + (c-a)x_1 - x_1x_3 \\ \dot{x}_3 = -bx_3 + x_1x_2 \end{cases} \tag{3.20}$$

当$a = 35, b = 3, c = 28$时，系统的混沌吸引子见图 3.7

③ Duffing 方程

$$\ddot{x} + p_1\dot{x} + p_2 x + p_3 x^3 = q\cos wt \tag{3.21}$$

当 $p_1 = 0.4$，$p_2 = -1.1$，$p_3 = 1.0$，$w = 1.8$，$q = 2.1$ 时的混沌吸引子见图 3.8

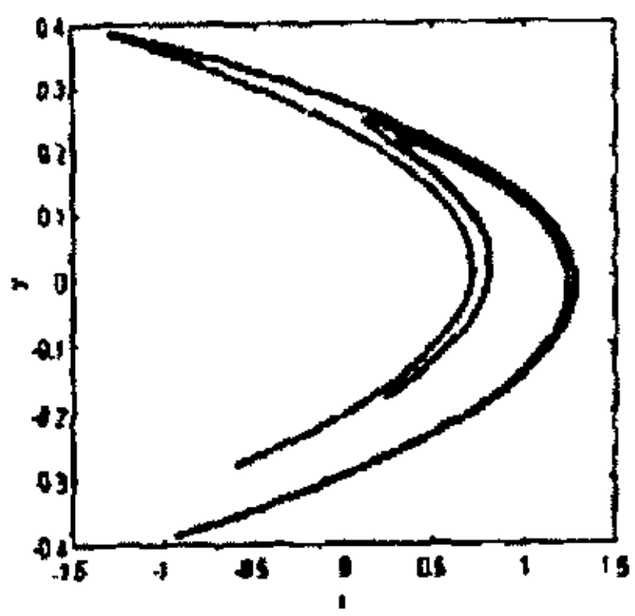


图3. 5 Hénon混沌吸引子

Fig.3.5 Hénon chaotic attractor

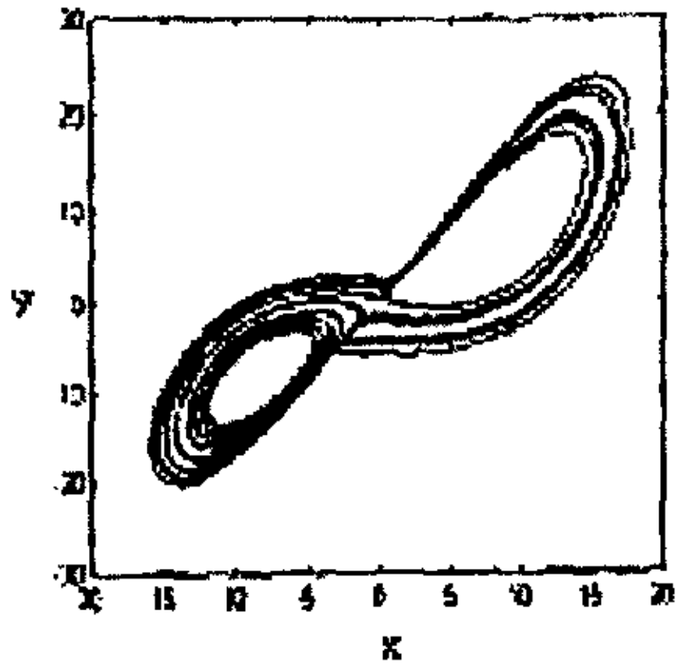


图3. 6 Lorenz混沌吸引子

Fig.3.6 Lorenz chaotic attractor

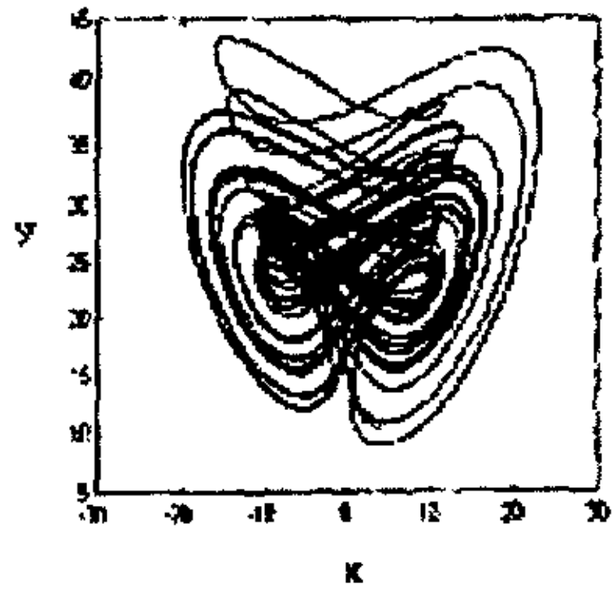


图3. 7 Chen混沌吸引子

Fig.3.7 Chen chaotic attractor

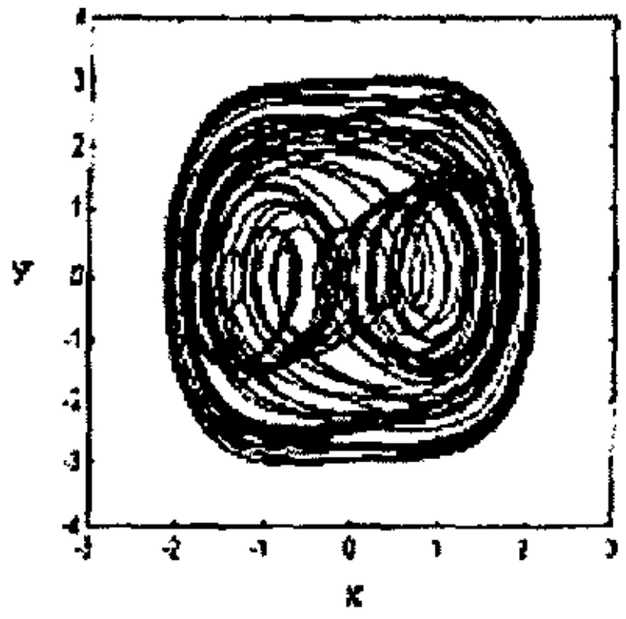


图3. 8 Duffing混沌吸引子

Fig.3.8 Duffing chaotic attractor

3. 6 小结

本章简单介绍了混沌的起源、应用、定义以及特征，详细讨论了刻画混沌的特征量，最后给出了一些常见的混沌模型。

4 混沌序列密码设计与实现

混沌系统是一种高复杂的非线性动态系统，具有对初始条件和混沌参数非常敏感性，生成的混沌序列具有非周期性、宽噪声和伪随机性的特性。因此系统可被应用于保密通信领域，也可作为加密的一种方法[35-38]。

目前，利用混沌映射[30-40]产生混沌序列的理论研究已经很成熟。但是，混沌序列发生器总是在有限精度下实现，混沌迭代过程必将退化为周期序列。本章结合混沌技术和传统密码技术，提出了一种混合混沌序列密码的设计方法，可以克服有限精度效应对混沌系统的影响，从而改善混沌序列特性。通过理论分析和仿真结果表明，这种混合混沌序列具有随机性好、实现容易、周期长等优点。此外，在较低实现精度下，能够得到周期极大的序列，为在低成本下得到比较实用的序列密码提供了一种新的思路。

4.1 混沌序列加密原理和方法

4.1.1 利用混沌序列加密的可能性

序列加密具有效率高、可以扰乱明文统计特性、不存在误差传递特点[19,41]，因而成为当前最广泛使用的密码系统之一。序列密码的安全性取决于密钥序列。所以，如何产生周期足够长的密钥序列是现代序列密码研究的主要课题之一。

如前一章所述，混沌系统是确定性非线性系统产生的类似随机性的行为，它属于确定性系统而又难于预测。混沌系统对初值和系统参数极端敏感，相同的混沌系统在具有微小差别的初始条件下，系统的长期行为将发生巨大的变化，混沌系统长期行为不可预测。只要系统参数和初始条件给定，混沌现象本身可以重复，混沌现象具有伪随机性、类噪声。混沌现象的上述特性，将会在信息加密中得到广泛的应用[42]。

利用混沌系统，可以产生数量众多、非相关、类似噪声、又可以再生的混沌序列，这种序列难于重构和预测，从而使密码分析者难以破译，因而非常适合与信息的加密处理，其随机性、抗破译能力均优于传统的序列密码。这些特性使得混沌序列能够成为一种的加密序列。

4.1.2 混沌序列加密方法

如图 4.1 所示，利用混沌系统产生混沌序列，再对混沌序列进行适当的处理后得到的序列与明文进行作用，得到密文。密钥取为混沌系统的初始状态或（和）参数。解密是加密的逆过程。

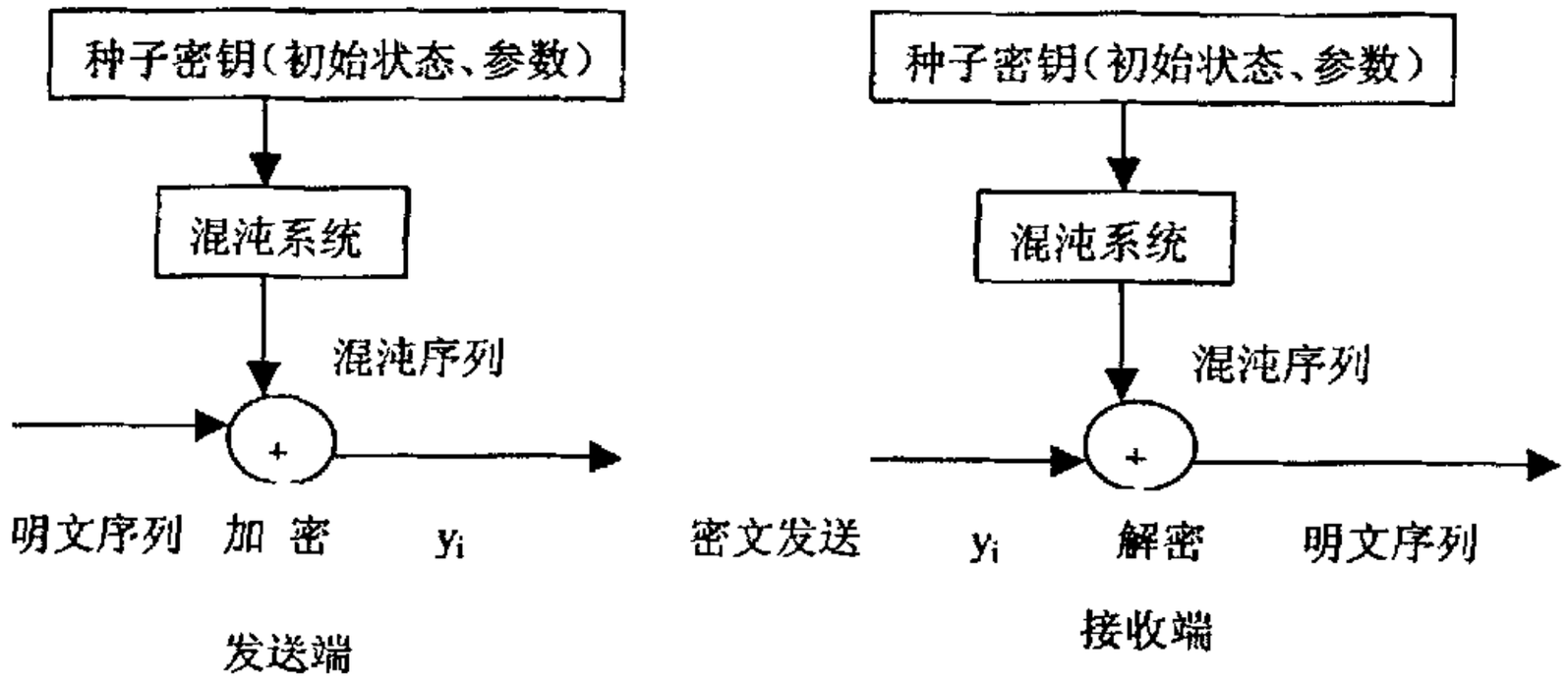


图 4.1 混沌序列加密和解密方法

Fig.4.1 Chaotic stream encryption and decryption method

4.1.3 混沌加密与传统加密原理的比较

Shannon 早在其经典文章[43]中就已将类似于混沌理论具有的如混合、初值参数敏感性等基本特性应用到密码学中，并提出了密码学中用于指导密码设计的两个基本原则：扩散（Diffusion）和扰乱（Confusion）。扩散是将明文冗余度分散到密文中使之分散开来，以便隐藏明文的统计结构，实现方式是使得明文的每一位影响密文中多位的值。扰乱则是用于掩盖密钥和密文之间的关系，使密钥和密文之间的统计关系变得尽可能复杂，导致密码攻击者无法从密文推理得到密钥。

混沌的轨道混合（Mixing）特性（与轨道发散和初值敏感性直接相联系）对应于传统加密系统的扩散特性，而混沌信号的类随机特性和对系统参数的敏感性对应于传统加密系统的扰乱特性[44]。可见，混沌具有的优异混合特性保证了混沌加密器的扩散和扰乱作用可以和传统加密算法一样好。

目前还没有建立一套关于混沌与密码学深层次关系的理论。它们之间最重要的区别在于：密码学系统工作在有限离散集，而混沌却工作在连续实数集。表 4.1.2 给出了混沌系统与传统密码算法的相似点与不同之处[44]。由于传统加密系统建立了一套分析系统安全性和加密系统性能的理论，密钥空间的设计方法和实现技术亦比较成熟，从而能保证系统的安全性[45]。而目前混沌加密系统缺少这样一个评估算法安全性和性能的标准，这恐怕是混沌加密算法现阶段还不能被广泛采纳和接受的一个重要原因。

表 4.1 混沌理论与密码学的相似与不同之处

Table 4.1 Similarities and differences between chaotic theory and cryptography.

	混沌理论	传统密码学
相似点	对初始条件和控制参数的极端敏感性	扩散
	类似随机的行为和长周期的不稳定轨道	伪随机信号
	混沌映射通过迭代，将初始域扩散到整个相空间	密码算法通过加密轮产生预期的扩散和混乱
	混沌映射的参数	加密算法的密钥
不同点	混沌映射定义在实数域内	加密算法定义在有限集上
	?	密码系统的安全性和性能

关于如何选取满足密码学特性要求的混沌映射是一个需要解决的关键问题。L. Kocarev 等在文献[46]中给出了在这方面的一些指导性建议。选取的混沌映射应至少具有如下三个特性：混合特性（Mixing property）、鲁棒混沌（Robust chaos）和具有大的参数集（Large parameter set）。需要指出具有以上属性的混沌系统不一定安全，但不具备上述属性则得到的混沌加密系统必然是弱的。

①混合特性：将明文看作初始条件域，则混合属性是指将单个明文符号的影响扩散到许多密文符号中去，显然，该属性对应密码学中的扩散属性。具有混合属性的系统具有较好的统计特性，当迭代次数 $n \to \infty$ 时，密文的统计性质不依赖于明文的统计性质，从而由密文的统计结构不能得到明文的结构。

②鲁棒混沌：鲁棒混沌是指在小的参数扰动下，系列仍保持混沌状态。但是，一般来讲大多数混沌吸引子不是结构稳定的，而非鲁棒混沌的系统具有弱密钥。

③大的参数集：密码系统安全性的一个重要的衡量指标是 Shannon 熵，即密钥空间的测度，在离散系统中常用 $\log_2 K$ 近似，其中 K 为密钥的数目。因而，动力系统的参数空间越大，离散系统中反应的 K 就越大。

综上所述，选择混沌系统中，我们应该考虑在大的参数集中具有鲁棒混沌混合属性的系统。

4.2 Logistic 映射及其特性[46,47,48]

4.2.1 Logistic 映射及其特性

由于 Logistic 映射算法简单，对其研究也最为透彻，在下一节中我们要把它应用于传统的序列密码，所以在这里我们进行比较详细的讨论。

离散时间动态系统的 Logistic 映射的定义为：

$$x_{n+1} = f(x_n) = 1 - \mu x_n^2 \tag{4.1}$$

其中 x_n 是状态，f 把当前状态 x_n 映射到下一个状态 x_{n+1}。μ 是参数，若选择参数 μ 限制在[0, 2]区间内，则式 4.1 将是从线段 $I=[-1,+1]$ 到它本身的一个非线性映射。当 μ 逐渐增大时，迭代出现多次突变。研究表明，当 $0<\mu<0.75000$ 时迭代过程将迅速地趋于一个定值 x^*（稳定不动点），即迭代过程为稳定地 1 周期，当 μ 增大到 0.75000 时，迭代出现 2 点周期分岔；μ 增大到 1.25000 时，出现 4 点周期分岔，尔后相继出现稳定的 2^n 点周期（$n=3,4,5\cdots$），这种 2^n 倍周期分岔随 μ 的增大愈来愈快；当 $\mu \to \mu_\infty = 1.40115$ 时，迅速达到周期 $N \to \infty$；当 $\mu > \mu_\infty$，多次迭代结果看起来时分布在一定区间内的随机数，即进入了混沌状态。区间 $[\mu_\infty, 2]$ 称为混沌区。

我们选取参数 μ=2, 则迭代方程为：

$$x_{n+1} = f(x_n) = 1 - 2x_n^2 \tag{4.2}$$

此时 Logistic 映射的输入输出部分都分布在区间[-1, 1]上，为满映射，可任意选取一个初始 x_0，迭代产生一个序列来计算系统 4.2 的 Lyapunov 指数。这里选取初始值 $x_0 = 0.4$，迭代得到一个序列，计算 Lyapunov 指数为：

$$\lambda \approx \lim \frac{1}{k} \sum_{i=0}^{k-1} \lg |f'(\mu, x_i)| = \lim \frac{1}{k} \sum_{i=0}^{k-1} \lg |-2\mu x_i| = 0.69350 \tag{4.3}$$

计算结果表明，该系统的 Lyapunov 指数大于 0，故系统 4.2 是混沌系统，所产生的序列为混沌序列。

下面我们对它的概率密度、均值、自相关性、互相关性进行定性分析。

文献[49]证明了系统 4.2 所产生的混沌序列的概率分布密度函数 PDF（Probability Density Function）为：

$$\rho(x)=\begin{cases}\dfrac{1}{\pi\sqrt{1-x^2}}, & -1<x<1\\ 0, & else\end{cases} \tag{4.4}$$

$\rho(x)$是不依赖于初始值，所以式（4.4）表达的混沌系统具有普遍性。图 4.2 是分布函数的数值模拟结果。

利用概率密度函数，可以容易的计算出 Logistic 映射所产生的混沌序列一些统计特性：平均值：

$$\bar{x}=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N=i}x_i=\int_{-1}x\rho(x)=0 \tag{4.5}$$

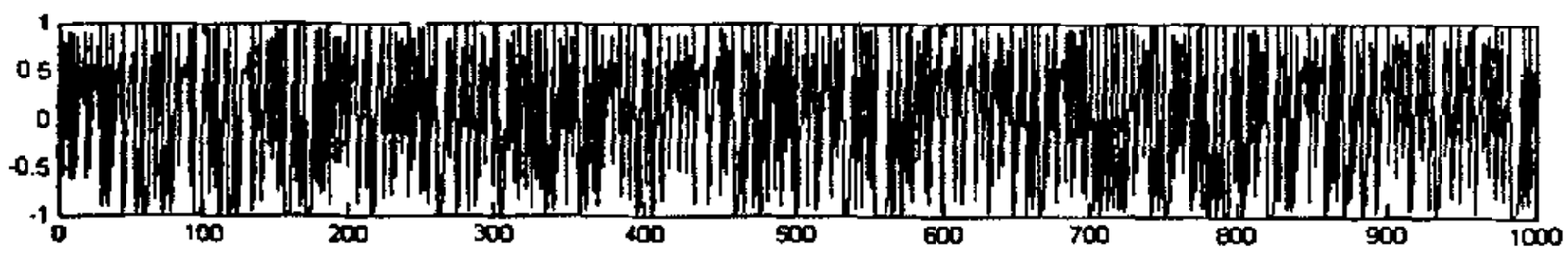


图 4.2 Logistic 映射分布函数图

Fig.4.2 Logistic map distribution function.

对于自相关函数$ac(m)$，当自相关间隔$m=0$时，

$$ac(m)=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N=1}x_i^2-\bar{x}^2=\int_1x^2\rho(x)-0=\int_{-1}\frac{x^2}{\pi\sqrt{1-x^2}}dx=$$

$$\frac{1}{\pi[\arcsin x-0.5(\pi\sqrt{1-x^2}+\arcsin x)]}\Bigg|_{-1}^{1}=0.5 \tag{4.6}$$

当自相关间隔$m\neq0$时，

$$ac(m)=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N=i}x_ix_{i+m}-\bar{x}^2=\int_1xf^m(x)\rho(x)dx-0=0 \tag{4.7}$$

式中$f^m(x)=f(f\cdots f(x)\cdots)$，图 4.3 是其数值模拟图。

独立选取 2 个不同的初始值x_{01}和x_{02}，他们分别产生 2 个混沌序列的互相关函数为：

$$ac_{12}(m)=\lim_{N\to\infty}\frac{1}{N}\sum_{t=0}^{N=t}x_{1t}x_{2t+m}-\bar{x}^2=\int_1\int_1 x_1 f^m(x_1)\rho(x_1)\rho(x_2)dx_1dx_2-0=0 \qquad (4.8)$$

式中 $f^m(x)=f(f\cdots f(x)\cdots)$。图 4.4 是其数值模拟图。

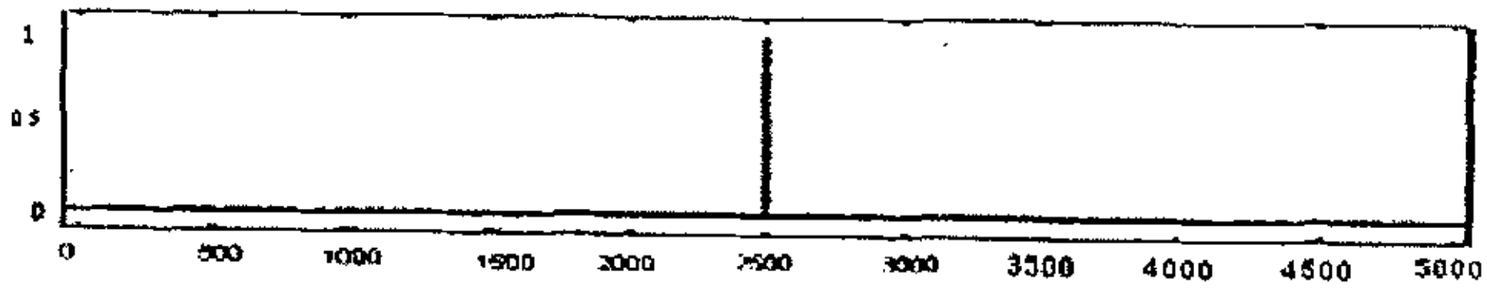


图 4.3 Logistic 映射的白相关函数

Fig. 4.3 Logistic map auto-correlation function

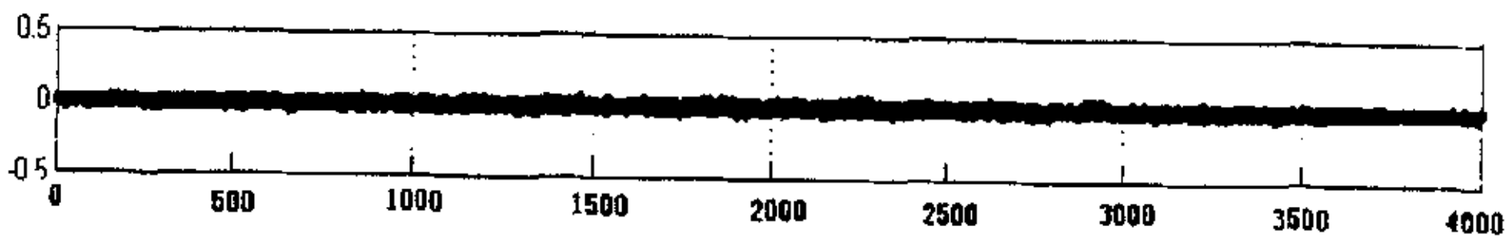


图 4.4 Logistic 映射的互相关函数

Fig.4.4 Logistic map cross-correlation function

从以上的统计特性和数值模拟图可以看出，Logistic 映射在参数 $\mu=2.000$ 是产生的混沌序列均值为 0，自相关是 δ 函数，互相关为 0，其概率统计特性与白噪声一致的。

4.2.2 混沌序列的生成

从 Logistic 映射生成混沌序列可以有以下几种方法：

① 实数值序列，即 $\{x_k,k=0,1,2,3\cdots\}$ 是混沌映射的轨迹点所形成的序列；

② 二值序列，可以通过定义一个阈值 Sign，有上述的实数值混沌序列得到；

$$Sign(x_k)=\begin{cases}0 & ,\ -1\le x_x<0\\ 1 & ,\ 0\le x_k\le 1\end{cases} \qquad (4.9)$$

二值序列即为 $\{Sign(x_k),k=0,1,2,3\cdots\}$。因此，该值序列也具有混沌特性。

③比特序列，同样由实数值混沌序列得到。所不同的是，比特序列是通过对 $\{x_k,k=0,1,2,3\cdots\}$ 中的 x_k 改写为 L-bit 的浮点数形式得到的；

$$|x_k|=0.b_0(x_k)b_1(x_k)\cdots b_i(x_k)b_{L-1}(x_k) \qquad (4.10)$$

其中 $b_i(x_k)$ 是 $|x_k|$ 的第 i 位。所得的序列为：

$$\{b_i(x_k), i=0,1,2\cdots,L-1; k=0,1,2,3,\cdots\} \tag{4.11}$$

④$2^K$值序列，可通过定义一个阈值函数Γ，由上述的实数值混沌序列得到

$$\Gamma(x)=\begin{cases}00\cdots00 & 0\le x\le \dfrac{1}{2^K}\\ 00\cdots001 & \dfrac{1}{2^K}\le x\le \dfrac{2}{2^K}\\ \vdots & \\ 11\cdots10 & \dfrac{2^K-2}{2^K}\le x\le \dfrac{2^K-1}{2^K}\\ 11\cdots11 & \dfrac{2^K-1}{2^K}\le x\le 1\end{cases} \tag{4.12}$$

4.2.3 混沌序列存在的问题[50]

混沌从发现起，它的随机性就十分引人注目。混沌序列应用于密码的研究是从 1989 年[51]提出后发展起来的。十多年来，存在的主要问题是：(1)混沌函数的短周期，为获得相同的周期，有限精度的混沌函数内部要比移位寄存器使用多一倍的存贮器数目。(2)混沌序列的生成器总是在有限精度器件实现的，使得任何混沌序列最终是周期的。因此，有限精度效应是混沌序列从理论走向应用的主要障碍。(3) 现有的混沌序列的研究对于所生成序列的周期、伪随机性、复杂性等的估计不是建立在（连续状态空间）统计分析上，而是通过实验给出，故难于保证其每个实现序列的周期性、伪随机性和复杂性都足够高，因而不能使人放心的采用它来加密。

本章在 4.3 节提出混合混沌序列，可以克服有限精度对混沌系统的影响。对这类混合混沌序列的周期、平衡、相关性以及线性复杂等特性进行了系统的分析，为混合混沌序列密码的设计打下基础。

4.3 混合混沌序列及其性能分析

4.3.1 混合混沌序列的产生

混合混沌序列产生方法如图 4.5 所示。该方法是混沌序列发生器和 m-序列发生器以异或方式结合的，我们称之为混合混沌系统。m-序列具有良好的随机性，其理论特性已在第 2 章详细阐述。目前，产生混沌序列的方法很多，例如：Logistic 映射、Tent 映射、Chebyshev 映射等。其中，Logistic 映射算法简单，对其研究也最为透彻，在 4.2 节已经做详细的讨论。因此图中的混沌序列选用 Logistic 映射。

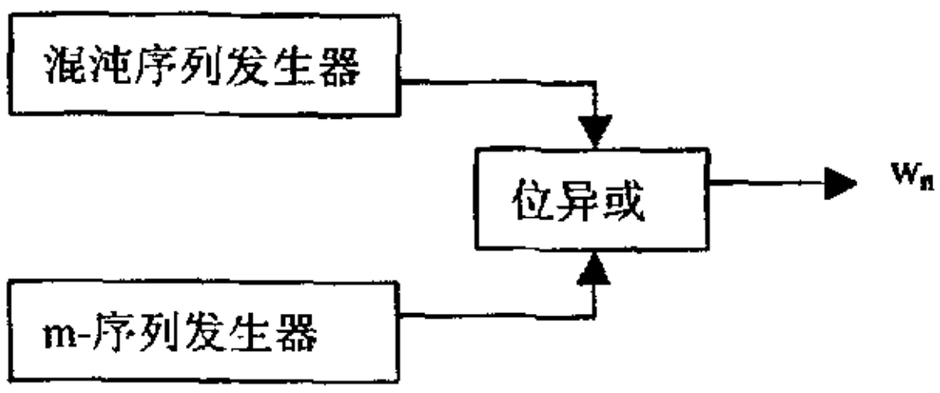


图 4.5 混合混沌序列产生方框图

Fig.4.5 The structure of mixed chaotic stream generator

4.3.2 混合混沌序列的性能分析

①初值敏感性

Logistic 混沌系统的一大特点是对初始值有极其敏感的依赖性。因此通过改变 Logistic 混沌系统参数及其初始值便可以得到数量巨大的平移相异的混沌序列，即混沌序列的码量大，混沌序列的这一优点很适合于密码系统。取两个 Logistic 映射的初值仅相差 10^{-14}, m-序列的级数 L=42。在任意选取初值。经过大约 43 次迭代后，混合混沌序列一分为二，成为两个平移相异的序列，说明混沌混合系统仍然保持了 Logistic 混沌映射的初始敏感性。

②周期

定理 4.1： 图 4.5 所示的混合混沌系统中，设 m-序列的周期为 T 和混沌序列的周期为 Q，并且 $Q \neq T$，则混合混沌序列的周期 P 是 m-序列周期 T 和混沌序列周期 Q 的最小公倍数。即 $P = \lceil Q.T \rceil$ 其中 $1 \le Q \le Q_s$，Q_s 混沌迭代函数的状态总数。

证明： 系统输出周期 P 是 m-序列周期 T 和混沌序列周期 Q 的最小公倍数，即 $P = \lceil Q.T \rceil$。在二元域上异或就是相加运算，由于 m-序列的运行状态与混沌序列的运行状态独立，且 m-序列的状态数和混沌序列状态数不等，所以包括状态数为 Q 的混沌序列和状态数为 T 的 m-序列的全系统，从某一初始态起回到初始态经历的状态数只可能是 Q 和 T 的最小公倍数，若 Q 与 T 互素，则系统输出序列的周期 $P = QT$。

理论上 Logistic 混沌序列是非周期的，由于任何混沌序列只能用有限精度设备来生成。所以混沌序列的状态数实质都是有限的。设代表 Logistic 混沌序列在某个初值下的有限状态数（即周期），受有限精度效应的影响，混沌系统可能出现不动点，即 Q 的最小值为 1，若设混沌序列的最大状态数为 Q_s，则在不同的初始条件下 $1 \le Q \le Q_s$。证毕。

大量的仿真实验也证实了定理 4.1 的正确性。尽管难以控制混沌序列的周期，但可以通过选择 m-序列的周期来满足实际应用中对序列周期的要求。显然，图 4.5 的混合混沌系统有效克服了混沌系统因有限精度效应而产生的短周期行为，使混

合混沌系统可用数字化的方法实现。

③平衡性

定理 4.2： 在图 4.5 的混合混沌系统中，若混合混沌序列为 0-1 的二元序列，则在 m-序列的一个周期之内，混合混沌序列中 0-1 出现次数均值的差不大与 1.

证明： 设 m-序列的级数为 L，则周期为 2^L-1，在一个周期内 m-序列中“0”个数为 $2^{L-1}-1$ 个，“1”的个数为 2^{L-1}。又设混沌序列中，出现“1”概率为 $P(1)$，出现“0”的概率为 $P(0)$，且 $P(0)+P(1)=1$。因此，在一个 m-序列的周期中“1”的出现次数的均值为：

$$num(1)=(2^{L-1}-1)P(1)+2^{L-1}P(0)=2^{L-1}-P(1)$$

“0”的均值为：

$$num(0)=(2^{L-1}-1)P(0)+2^{L-1}P(1)=2^{L-1}-P(0)$$

两者之差为

$$\Delta num=|num(1)-num(0)|=|P(0)-P(1)|<1$$

证毕。

定理 4.3： 在图 4.5 所示的混合混沌系统中，若混合混沌序列为 0-1 的二元序列，则在 m-序列的一个周期 T 内。“00”、“01”、“10”、“11”出现次数任意两者均值的差不大于 1。

证明： 设 m-序列的级数为 L，则周期为 2^L-1。由 m-序列的平衡性可知，“00”的个数为 $2^{L-2}-1$ 次，“01”、“10”、“11”的个数为 2^{L-2} 次。又设混沌序列中，出现“00”的概率为 P(00)，出现“01”的概率为 P(01)，出现“10”的概率为 P(10)，出现“11”的概率为 P(11)，且 P(00)+P(01)+P(10)+P(11)=1. 因此“00”出现的概率均值为：

$$num(00)=(2^{L-2}-1)P(00)+2^{L-2}(P(01)+P(10)+P(11))=2^{L-2}-P(00)$$

同理，“01”、“10”、“11 出现次数的均值分别为：

$$num(01)=(2^{L-2}-1)P(01)+2^{L-2}(P(00)+P(10)+P(11))=2^{L-2}-P(01)$$

$$num(10)=(2^{L-2}-1)P(10)+2^{L-2}(P(00)+P(01)+P(11))=2^{L-2}-P(10)$$

$$num(11)=(2^{L-2}-1)P(11)+2^{L-2}(P(00)+P(10)+P(01))=2^{L-2}-P(11)$$

故任意两者之差

$$\Delta num=|num(i)-num(j)|=|P(i)-P(j)|<1$$

其中 $i,j=00,01,10,11, i\neq j$

证毕。

定理 4.2、4.3 从理论上确保了混合混沌序列有良好的平衡性。下一节我们将对其做统计实验，理论分析与统计实验结果是相吻合的。

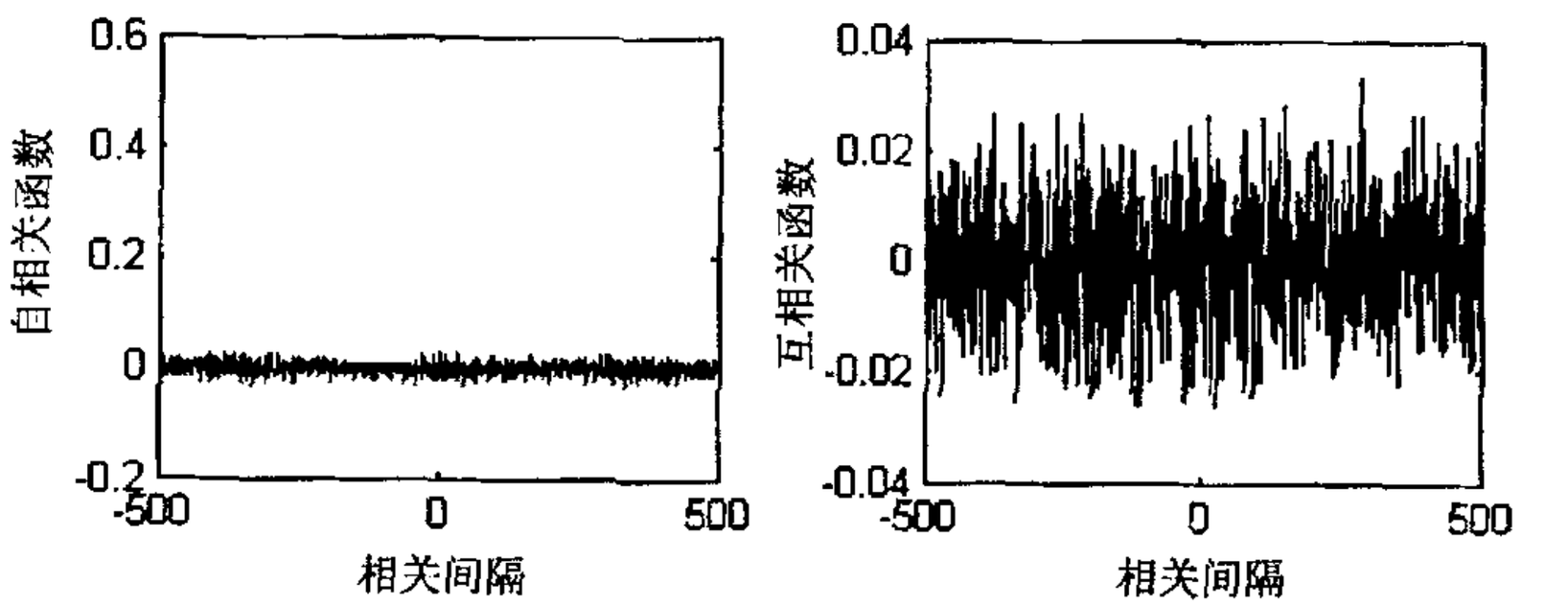
④相关性

混沌序列的非周期互相关函数为：

$$C_{a^{(1)},a^{(2)}}(l)=\begin{cases}\dfrac{1}{N}\sum_{i=0}^{N-1-l}a_i^{(1)}(a_{i+l}^{(2)})^*, 0\le l<N\\ \dfrac{1}{N}\sum_{i=0}^{N-1+l}a_{i-l}^{(1)}(a_i^{(2)})^*, 1-N\le l<0\\ 0, |l|\ge N\end{cases} \tag{4.13}$$

式中，N 为序列长度，当 $a^{(1)}=a^{(2)}$ 时，上式表示的函数是序列的非周期自相关函数。

在密码学中，要求伪随机序列具有类似 δ 的自相关和为零的互相关。m-序列具有十分理想的周期自相关函数，但具有好的互相关特性的 m-序列数量很少。目前，研究混合混沌序列的周期相关特性的有效方法是随机选择一些序列作为样本进行大量统计计算。1000 组长度为 1024bit 的混合混沌序列周期自相关、互相关的均值分别如图 4.6。由图 4.6 可知，混合混沌序列具有近似 δ 的自相关函数和近似为零的互相关函数。



(a) 自相关函数　　(b) 互相关函数

图 4.6 .混合混沌序列相关函数

Fig. 4.6 The Correlation function of mixed chaotic sequences: (a) self-correlatin (b) cross-correlation.

4.3.3 混合混沌序列的优点

将 Logistic 离散混沌映射产生的混沌序列与 m-序列以异或方式得到的混合混沌序列能集成 Logistic 混沌序列和 m-序列的优点，克服两者的缺点归纳起来有三点：其一是加大了序列的复杂度。我们知道，m-序列很容易被破译，引入混沌技术后，那么破译该序列的难度将加大，这是因为混沌是一种复杂的非线性动力行

为，和传统的 m-序列结合起来得到的混合混沌序列，要难于破译得多；其二是由于混沌对初始条件的极端敏感性，可以得到大量非相关、随机性好的混合混沌序列，且这些序列在同样的精度上，通过同样的混沌初始条件、同样的反馈多项式和初态，采用同样的时钟控制，就可以再生。其三是容易获得极大的周期的混合混沌序列。以上三点说明了在传统序列密码中引入混沌的好处。

4.4 混合混沌加密系统的设计与实现

文献[52-53]详细介绍收缩密钥流生成器和自收缩密钥流生成器的设计和性能分析，并且也指出了两类密钥流生成器的等价性，但随后文献[54-55]中出现了这两类生成器的一些攻击方法，这些方法表明，收缩式密钥流生成器和自收缩式密钥流生成器都是不安全的。我们已经详细的讨论了混合混沌序列的性质，结合文献[52-53]我们给出具体的混合混沌系统设计与实现，并进行相应的仿真实验。

4.4.1 密钥流生成器结构

混合混沌密钥流生成器的结构图见图 4.7。

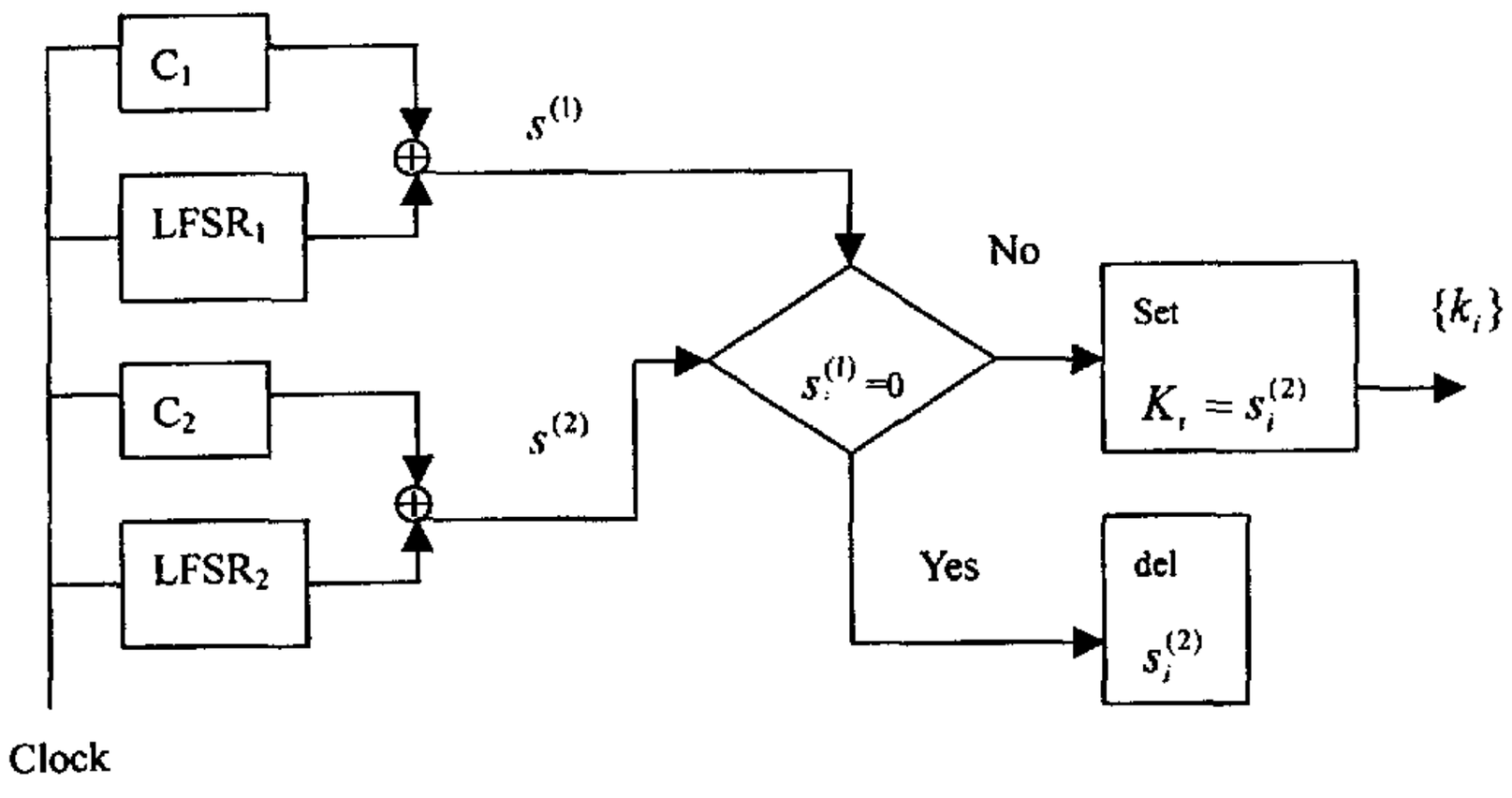


图 4.7 混合混沌密钥流生成器

Fig.4.7 The generator of mixed chaotic key stream

具体过程描述如下：

输入：两个线性反馈移位寄存器 $LFSR_1$ 和 $LFSR_2$，及其初态 $m_0^{(1)}, m_0^{(2)}$；一个数字混沌系统及其两个初值 $x_0^{(1)}, x_0^{(2)}$。

对 $i=1,2,\cdots$，完成如下步骤：

① 移位 $LFSR_1$，产生序列 $\{m_i^{(1)}\}$；

② 移位 $LFSR_2$，产生序列 $\{m_i^{(2)}\}$；

③ 给定初始值 $x_0^{(1)}$，产生数字混沌序列 $\{a_i^{(1)}\}$；

④ 给定初始值 $x_0^{(2)}$，产生数字混沌序列 $\{a_i^{(2)}\}$；

⑤ 作运算 $s_i^{(1)} = m_i^{(1)} \oplus a_i^{(1)}, s_i^{(2)} = m_i^{(2)} \oplus a_i^{(2)}$；

⑥ 若 $s_i^{(1)} = 1$；则置 $k_i = s_i^{(2)}$；若 $s_i^{(1)} = 0$；则删去 $s_i^{(2)}$。

输出：混合混沌序列 $\{k_i \mid i = 1,2,\cdots\}$。

混合混沌系统和两个 LFSR 通过时钟控制，使它们同时开始启动。两个子系统输出的序列 $\{s_i^{(1)}\}$ 和 $s_i^{(2)}$ 也是通过时钟来保持同步，从而用一个序列来选择另一个序列。

4.4.2 混合混沌序列性能分析仿真

本节我们主要利用计算机仿真实验来研究混合混沌加密系统的序列性能，目的是用实验证实 4.3 节中给出的相关结论，同时力图获得对工程应用上的一些具体指导。工作平台为 MATLAB6.1, 实现精度取 16 位，为了作一比较，我们在同样的实验条件下，也对 m-序列、Logistic 混沌序列的“0”、“1”的相关性能均作了实验。

以下是实验参数的设置：

1) m-序列：

反馈多项式：$p(x) = x^{31} + x^3 + 1$；

LFSR 的初始状态：10100101101011010101100110111001

2) Logistic 映射有（4.2）式给出，其数字混沌序列出 4.2.2 节中的第 2 种方法变换而成。

3) 混合混沌加密系统的序列：

C1，C2 分别取 Logistic 混沌映射不同的初始值而得到不同的混沌序列；

$LFSR_1$ 的反馈多项式：$p_1(x) = x^9 + x^4 + 1$；初始态为 1010110011；

$LFSR_2$ 的反馈多项式：$p_2(x) = x^{11} + x^2 + 1$；初始态为 10011100101；

4）序列长度分别为 200，1000，2000，3000，4000 和 5000。

① 0-1 平衡性

我们用 $|k_1 - k_0|/n$ 来表示序列的 0-1 平衡性，其中，k_1 和 k_0 分别是“1”和“0”在序列中出现的次数，n 表示序列的长度。从表 4.2 的数据结果看，在较低实现精度下，随着序列长度的增加，混合混沌序列的“0”、“1”均衡性明显优于 m-序列和 Logistic 混沌序列，与理论相符。

表 4.2 二值序列平衡性实验

Table4.2 0-1 Sequences balance experiment.

分项统计		序列长度 N				
		500	1000	2000	3000	5000
m-序列	0 的个数	236	476	959	1558	2571
	1 的个数	264	524	1041	1442	2427
	$\|k_0-k_1\|/n$	0.0560	0.0480	0.0410	0.0387	0.0284
Logistic 序列	0 的个数	233	471	1049	1568	2599
	1 的个数	267	529	951	1432	2401
	$\|k_0-k_1\|/n$	0.0680	0.0580	0.0480	0.0453	0.0396
混合混沌序列	0 的个数	234	483	1029	1534	2551
	1 的个数	266	517	971	1466	2449
	$\|k_0-k_1\|/n$	0.640	0.0340	0.0290	0.0227	0.0204

② 游程特性

游程特性即 Golomb 提出的序列随机性公设的第 2 条。4.3 节我们已经分析了混合混沌序列是均匀分布，并且也分析了游程分布类似于随机序列的游程分布，即长为 i 的游程出现的概率为 $1/2^i$，且 0-游程与 1-游程各占游程总数的一半。我们对三种序列分别取不同值进行了游程特性实验。表 4.3 是游程分布的平均值，从表 4.3 中的数据可以看出，在较低实现精度下，m-序列的游程特性比 Logistic 序列的游程特性稍微好，混合混沌序列的游程特性比 m-序列和 Logistic 序列的游程特性要好，更加接近于 Golomb 提出的随机公设 2。

③ 相关性

上一节我们已经给出了序列的非周期互相关函数，对于图 4.7 的系统来说，是有一个混合混沌序列去选择另一个混合混沌序列的，所以所得的最后序列也具有自相关旁瓣和互相关旁瓣的期望值都为 0。表 4.4 给出了不同混沌初始值和选择不同的 LFSR 的反馈多项式时，所得混合混沌序列的最大和平均归一化部分自相关旁瓣(绝对值)结果。其中序列长度取 3000 比特，相关间隔 τ 从-1000 到 1000，实现精度是 16 位。从表 4.4 的数据结果看出，在较低的精度下，混合混沌序列还保持较理想的自相关性。

表 4.3 二值序列游程特性

Table 4.3 0—1 sequences runlength property.

分项统计		序列长度 N				
		500	1000	2000	3000	5000
m-序列	1 游程	0.6286	0.6232	0.5083	0.489	0.5098
	2 游程	0.3286	0.3116	0.2126	0.2354	0.2336
	3 游程	0.0286	0.0580	0.2089	0.1529	0.1501
	4 游程	0.0143	0.0072	0.0628	0.0640	0.0631
	5 游程	0.0323	0.0391	0.0340	0.0311	0.0301
Logistic 映射序列	1 游程	0.6636	0.6316	0.597	0.5563	0.5120
	2 游程	0.3864	0.3368	0.3352	0.2441	0.2390
	3 游程	0.0909	0.1053	0.0864	0.1629	0.1601
	4 游程	0.0759	0.0526	0.0547	0.0680	0.0590
	5 游程	0.0425	0.0401	0.0423	0.0386	0.0320
混合混沌序列	1 游程	0.5490	0.5207	0.4870	0.4857	0.4950
	2 游程	0.1960	0.2031	0.2394	0.2274	0.2374
	3 游程	0.1131	0.1027	0.0978	0.0997	0.1189
	4 游程	0.0971	0.0897	0.0712	0.0686	0.0675
	5 游程	0.0301	0.0297	0.0254	0.0249	0.0305

表 4.4 混合混沌序列的自相关特性

Table 4.4 Mixed chaotic sequences's auto-correlation property.

混沌初始值 $x_0^{(1)}, x_0^{(2)}$	$x_0^{(1)} = 0.831$	$x_0^{(1)} = 0.187$	$x_0^{(1)} = 0.108$
	$x_0^{(2)} = 0.129$	$x_0^{(2)} = 0.129$	$x_0^{(2)} = 0.728$
LFSR 反馈多项式 $p_1(x), p_2(x)$	$p_1(x) = 1 + x + x^7$	$p_1(x) = 1 + x + x^7$	$p_1(x) = 1 + x^4 + x^9$
	$p_2(x) = 1 + x^4 + x^9$	$p_2(x) = 1 + x^4 + x^9$	$p_2(x) = 1 + x^2 + x^{11}$
最大自相关旁瓣	0.0679	0.0697	0.0568
平均自相关旁瓣	0.0457	0.0509	0.0401

④周期性

从理想上说，混沌系统所产生的序列周期是无限长的。但是在实际应用中，计算机或数字电路的有限字长恶化序列的各项性能，从而使任何混沌序列都具有周期性。因此，如何克服有限精度效应使混沌应用于密码和保密通信系统是一个关键性问题。Gernak[56]采用可编程组合电路对混沌映射的系统变量或参数随机扰动来增大周期，周红[57]等人提出 m-序列的扰动来实现有限精度混沌系统。本章提出的混沌系统和传统序列密码相结合的方法，我们已经在 4.3.2 节作了证明。对于图 4.7 的系统，假设$\{s_i^{(1)}\}$的周期为T_1,$\{s_i^{(2)}\}$的周期为T_2，同理，我们可以证明其计算最终输出的二进制混合混沌序列$\{k_i\}$的周期为

$$lcm(T_1,T_2)。\tag{4.13}$$

T_1、T_2可由定理 4.2 计算得到。

显然，混合混沌序列的周期不好确定，但我们知道随着时间精度的增大，混沌序列的周期也随之增大。因此，有两个因素影响图 4.7 输出序列的周期：实现精度和 LFSR 的级数。要想增大图 4.7 周期所采取的措施或是提高实现精度，或是增大 LFSR 的级数，一般高精度的实现系统必然以高成本为代价，因此要想进一步获得更大周期的混合混沌序列，可用较低精度的实现系统通过增大 LFSR 的级数来增大周期，且其周期随 LFSR 的级数增大呈指数递增。从(4.13)式可以看出，对子系统的序列的周期取了两次最小公倍数，因此，最终输出的混合混沌序列将是非常的大，如果遇到子系统输出的序列的周期值为素数的时候，最终输出的混合混沌序列的周期的增大效果更明显。因此，虽说在有限的精度实现条件下，所有的序列会出现周期，但在增大混沌序列的周期方面，本章提出的混合混沌方法将比文献[57]提出的 m-序列扰动的方法效果更明显，实现也比较简单，所用 LFSR 的级数也比文献[57]较小。

对于图 4.7,我们选择系统 C_1 的 Logistic 混沌映射的初值为 0.758,实现精度为 8 位，通过计算机仿真，测得的生成的数字混沌序列的周期为 5；我们选择系统 C_2 的 Logistic 混沌映射的初值为 0.107,实现精度为 8 位，通过仿真得到相应的数字混沌序列的周期为 7，我们选取 $LFSR_1$ 的反馈多项式：$p_1(x)=x^7+x+1$；$LFSR_2$ 的反馈多项式：$p_2(x)=x^9+x^4+1$，可以计算它们的周期分别为 127 和 511；根据式 4.13 我们可以计算出最终的混合混沌序列的周期为：46355，这个周期跟单纯的混沌序列 C_1 的周期相比较，周期增大了 9271 倍；跟单纯的混沌序列 C_2 的周期相比较，周期增大了 6622 倍；跟 $LFSR_1$ 所生成的 m-序列相比，增大了 365 倍，跟 $LFSR_2$ 所生成的 m-序列相比，增大了 90 倍。在如此低的实现精度和 LFSR 的级数如此小的情

况下，由以上分析可以看出所采用的混沌和传统序列密码相结合的方法，效果是明显。如果提高实现精度和 LFSR 的级数，那么得到的序列的周期就会更大的。

⑤ 线性复杂度

从理论上获得混沌序列的线性复杂度的表达式目前尚有困难。此处我们应用 B-M 算法来计算序列的线性复杂度。结果如表 4.5 所示。从表我们得知，混合序列具有理想的线性复杂度，即 $L \approx N/2$。

表 4.5 混沌序列的线性复杂度

Table 4.5 The linear complexity of mixed chaotic sequences.

线性复杂度	序列长度 N				
	256	512	1024	2048	4096
混合混沌序列	127	256	512	1024	2048

4.4.3 软件的设计

为了提高系统的安全性，对于图 4.7 密钥流生成器，$LFSR_1$ 和 $LFSR_2$ 的反馈多项式分别取为：$p_1(x) = x^{32} + x^7 + x^6 + x^2 + 1$，$p_1(x) = x^{32} + x^7 + x^5 + x^3 + x^2 + 1$。

软件的设计基于 window2000 平台，Visual C++ 6.0 开发环境，具体的加密和解密过程为：执行打开文件操作，文件打开成功后，在提示对话框中输入至少为 8 个字符的加密或解密口令，软件根据字符串自动生成密码序列，执行加密或解密操作，并可以保存加密文件后的文件。

在软件实现时，其中一个很关键的技术是如何将用户输入的口令（或称为密码）转换成加密系统的密钥并且转换是唯一的。本软件中，加密口令至少由 8 个字符构成，下面介绍如何将加密口令映射成图 4.7 中两个线性反馈移位寄存器 LFSR1 和 LFSR2 的初态 $m_0^{(1)}, m_0^{(2)}$ 和一个数字混沌系统的两个初值 $x_0^{(1)}, x_0^{(2)}$。

设有一 $k(k \geq 8)$ 个字符的口令字符串 $s = p_1 p_2 \cdots p_k$，将该字符分为 $s_1 = p_1 p_3 p_5 p_7, s_2 = p_2 p_4 p_6 p_8$，$s_3 = [p_5, \cdots p_m], s_4 = [p_m \cdots p_k]$,其中$m = [(5+k)/2]$。对于 $LFSR_1$ 的 32 位初态 $m_0^{(1)}$，因为对于字符串 s_1 中每个字符的二进制为 8 比特，那么 s_1 中的四个字符的二进制连接起来就可以构成 32 位作为初态 $m_0^{(1)}$，同理，字符串 s_2 的四个字符的二进制连接构成的 32 位作为初态 $m_0^{(2)}$。对于混沌 Logistic 映射的初值，将 s_3、s_4 中的每个字符转换成 ACSII 值，考虑到计算机中可打印的字符的 ACSII 码值是[32,126],因此将字符串的字符看作是[32,126]上的整数。为了处理方便将每个字符的整数值减 30 而映射到区间[2,96]，然后连接起来拼成(0,1)上的实数，就可以作为混沌 Logistic 映射的初值。

例如：有口令字符串 s=room2#desk，分解字符串 s=room2#desk 为子串 s_1=ro2d，s_2=om#e，s_3=2#d，s_4=esk。则按照上面的转换规则得：

$m_0^{(1)} = 01110010011011110011001001100100$，$m_0^{(2)} = 01101111110110100100011001100101$，$c_0^{(1)} = 0.200570$；$c_0^{(2)} = 0.718577$。

4.4.4 软件模拟实验

我们对如下两个明文分别进行加密实验：

明文 1 采用文献[58]中给出的明文：*Cryptologyist the science of overt secret writing (cryptography), of its authorized decryption (cryptanalysis), and of the rules which are in tum intended to make that unauthorized decryption more difficult (encryption security)*；

明文 2：*BBBBBBBBBBLLLLLLLLLLVVVVVVVVVV*；

口令字符串为：room2#desk。

由于通过混合混沌系统加密得到的密文含有不可打印的 ASCII 字符，因此为了形象地展示密文与明文之间的区别，我们使用二维图形来表达。在图 4.8 和图 4.9 中，横轴代表信息中字符出现的序号，纵轴代表对应字符的 ASCII 码值（范围 0～255）。从明文和密文的图形来看，明文的码值比较集中，但通过加密后，情况则大不相同，字符分布很均匀。也就是说，通过扩散、扰乱等作用后，密文中不包含明文的任何信息（包括明文的统计概率信息）。这正是我们想要达到的加密效果。图 4.10 和 4.11 为明文 2 的实验结果。

为了测试密文对密钥的敏感程度，对口令字符串改为：room2#desl；转换为系统的参数时，$c_0^{(2)}$ 变为 0.718578，（正确的是 0.718577）其余参数不变，则从密文 1 和密文 2 分别恢复出的内容见图 4.12 和图 4.13 所示，解密与原文完全不同，解密失败。加密系统对密钥是非常敏感的，而这一点正是密码学所要求的。

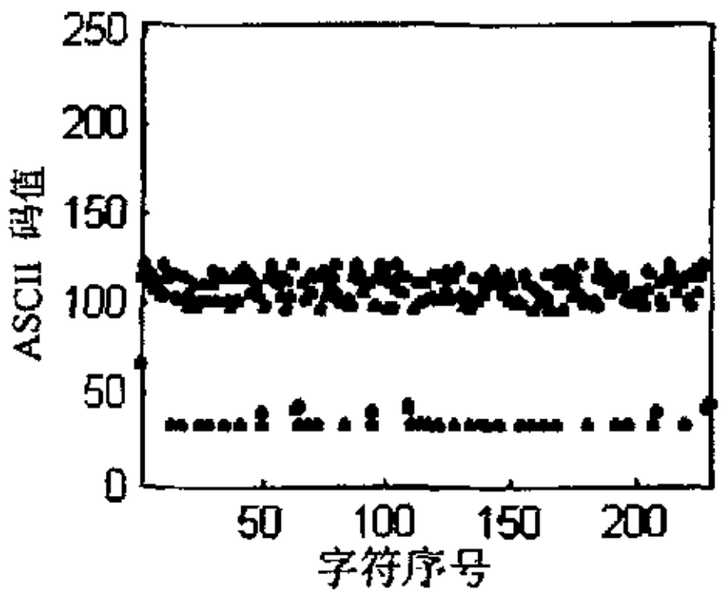


图 4.8 明文 1

Fig. 4.8 The first plaintext.

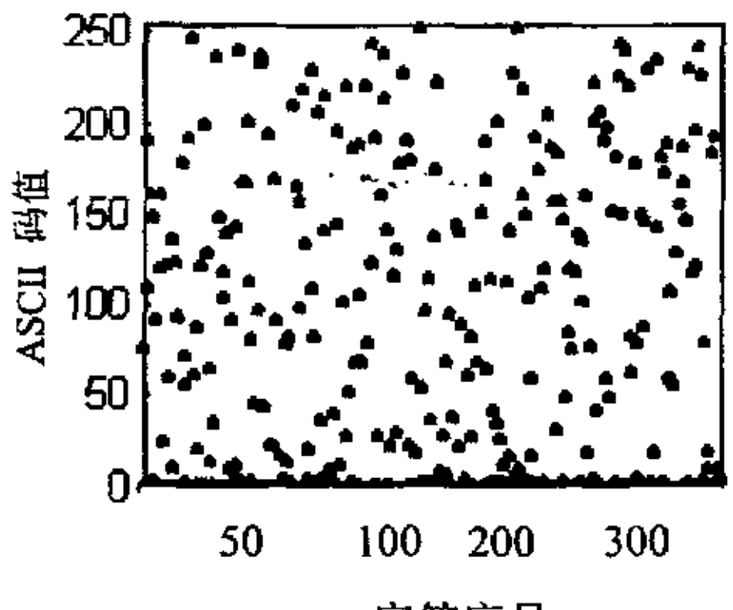


图 4.9 密文 1

Fig.4.9 The corresponding

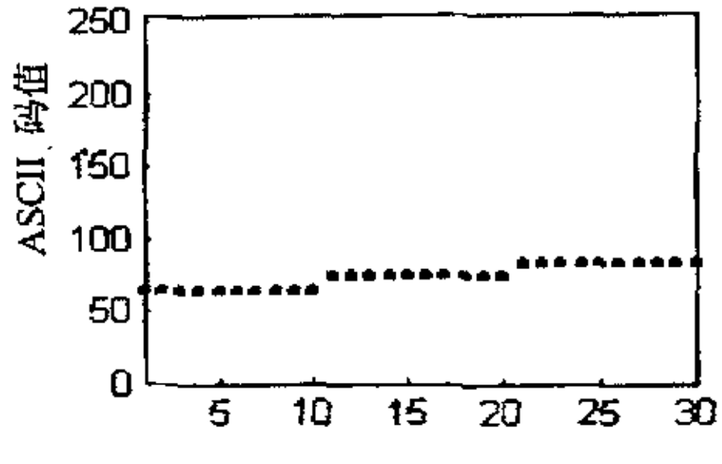


图 4.10 明文 2

Fig.4.10 The second plaintext.

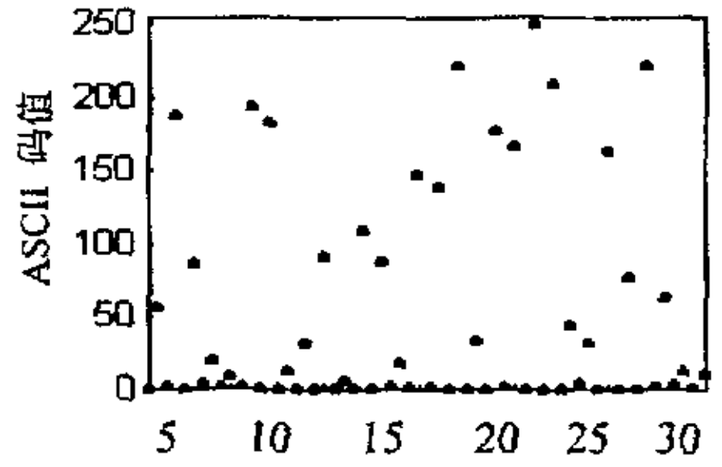


图 4.11 密文 2

Fig.4.11 The corresponding

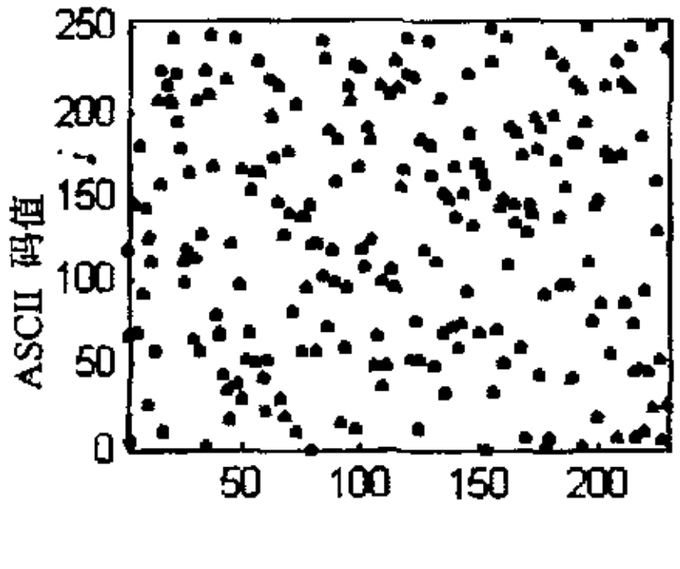


图 4.12 参数微小失配时
恢复出的明文 1

Fig.4.12 Decoded first plaintext using small mistake parameter.

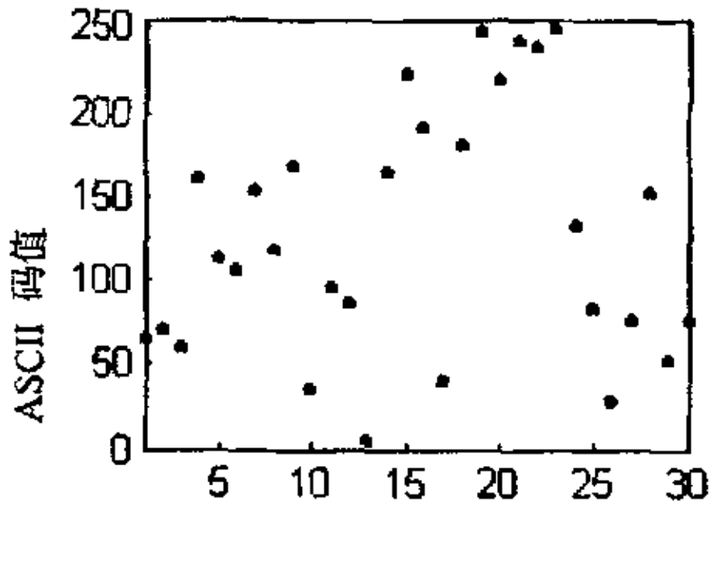


图 4.13 参数微小失配时
恢复出的明文 2

Fig.4.13 Decoded second plaintext using small mistake parameter.

4.4.5 混合混沌加密系统安全性分析

① 扩散和扰乱

在图 4.7 的混合混沌加密系统中用混合混沌序列原文进行异或，都可以看作是一定意义上的扩散。而 Logistic 混沌映射对参数的敏感性，则认为实现了扰乱。从这两点看，该加密系统符合 Shannon 提出的密码学设计具备的两个基本条件，即扩散和扰乱。

② 密钥空间

下面对加密系统的密钥空间进行估算。对于上面的算法，由于可供使用的 ASCII 字符集最多有 95 个，在实现精度为 4 位情况下，密码串的有最小为 8 个字符，则口令密钥空间最小为 95^8。假如 密码分析人员采用穷举方法以每秒 1,000,000 次的速度强制攻击加密文件，需要大约 210 年,这实际上是很难破译了。

注意我们还只是假定计算精度为 10^{-4} 位，实际上目前的计算机系统其计算精度远大于 10^{-4}，相应地密钥空间会变得更大，拥有足够大的密钥空间，这对于抵抗穷举攻击具有重要的意义。

③ 弱密钥

在图 4.7 的混合混沌系统中，如果系统参数 $c_0^{(1)}, c_0^{(2)}$ 为 0.5，则 Logistic 映射迭代的结果全部为 0.5,此时加密系统失效，为了克服这种弱密钥问题，可以在口令输入时，不允许用空格字符作为加密口令。

④ 密文对密钥的敏感依赖

在 4.4.4 节中的实验结果表明，加密系统对密钥是非常敏感的。使用微小差异的密钥就会产生截然不同的加密密文，或从密文中恢复出错误的明文。而这一点正是密码学所要求的。

⑤ 抵抗密码分析的能力

因为混沌序列是由确定性的方程产生，理论上可通过相空间重构的方法预测，典型的混沌时间序列，如 Logistic、Kent、Tent、Lozi、Henon、和 Lorenz 混沌时间序列在文献[59]中被成功预测，即使藕合的二维 Logistic 超混沌系统也被文献[60]成功预测。但是对于混合混沌系统，由于把混沌序列和 m-序列以异或形成混合混沌序列，用一个混合混沌序列随机的选择另一个混合混沌序列作为系统的最后输出序列，这可以抵抗通过相空间重构的方法预测混沌时间序列。

4.5 本章小结

本章概要地介绍了混沌加密的原理和方法，并对混沌密码和传统密码的加密原理进行了分析比较。提出了一种混沌和 m-序列相结合的混合混沌序列密码，给出了系统实现原理和算法描述，对混沌序列进行理论分析和计算机仿真，同时对该系统的产生安全性能进行了分析，如扩散扰乱特性、密钥空间、弱密钥问题和抗密码学分析等。结果表明，混合混沌序列随机性好，周期极大，在较低精度下序列的相关性能好，且并不要求 LFSR 的级数很高，这大大降低了实现了成本，因此无论从实用角度还是从序列的性能方面来说，都不失为一种优良的伪随机序列。

5. 基于混沌图像加密

基于混沌图像加密是混沌应用的重要方向之一，本章介绍了混沌图像加密的方法，利用第四章的混合混沌序列，提出了一种基于混合混沌的图像加密与解密算法，对该算法的进行了安全性详细的分析，并通过仿真具体论证了算法的可行性。

5.1 引言

随着 Internet 的迅速发展，信息传播的速度加快、容量增加，加上计算机、扫描仪、数字相机等设备的普及，使信息的获取和传播更加快捷、方便，信息的安全与保密因此变得非常重要，特别是对于图像、音乐、视频等多媒体信息，由于其数据量大，占用的频带宽并且具有一定的冗余性，传统的加密技术将其作为普通数据流进行加密，而不考虑多媒体数据的特点，因此有一定的局限性。另外，各种远程证券及股票交易、智能结算系统等也面临同样的安全与保密问题。本章即以图像加密为例，说明混沌在多媒体数据加密中的应用。

5.2 基于混沌的图像加密方法

基于混沌的图像加密就是利用混沌模型对图像进行某种变换，使得变换后的图像与原始图像存在视觉差异，从而实现图像加密。这里的视觉差异可以是颜色、亮度或轮廓等定性或定量的差异。图像置乱变换是一种经典的基于内容的图像加密方法。

图像置乱加密方法已有很多，如经典的 Arnold 变换、Hibert 曲线变换、E 曲线变换[61]、几何变换[62]、Fibonacci 变换[63]以及骑士巡游置乱变换[64]。这些方法置乱后的图像直观效果各不相同，但是他们都具有一定的确定性，同时在置乱过程中只改变象素点的位置，而不改变其大小，所以置换后的图像还是具有一定的规律性，一般来说，加密后图像置乱的程度越好，保密性就越高。

对于任一图像 I，设 I 的大小为 $n = M \times N$，且 I 中总共包含 k 种颜色，其中具有颜色 c_i 的象素个数为 n_i，$n_1 + n_2 + \cdots n_k = n$，则 I 的直方图 H 可以看作是一个具有 k 个元素的多重集 $S = (n_1.c_1, n_2.c_2, \cdots, n_k.c_k)$（其基数为 n）。显然，S 上的任意一个全排列 P_i 均对应一幅 $M \times N$ 图像 I_i，即 P_i 和 I_i 存在一一对应关系。

令集合 $X = \{1,2,\cdots,n\}$，则 X 的一个置换是指 X 到其自身的一个双射 $p: X \to X$。定义两个置换 p_1 和 p_2 的乘法运算为 $p_1.p_2 : X \to X$，$p_1.p_2(x) = p_2.p_1(x), x \in X$，则由 X 的所有置换组成的集合在该乘法运算下构成一个群，称为 X 上的对称群[61]，记

为 S_n。

置换 p 就是将 X 的一个排列变成另一个排列。由于图像与排列之间一一对应关系，可将集合 X 的元素看作是图像 I 中各元素顺序排列时的下标，则任何一个置换 p 都可看作是 I 到 $p(I)$ 的一个图像变换。因此，可利用排列变换对图像进行加密。

在传统的迭代乘积密码系统中，排列算子的主要任务就是对明文数据块中的元素进行置乱(也称为“重排”)，使得密文块看起来是随机的。不过，这些排列算子通常是事先确定好的,具有一定的解析表达式，而与密钥无关，这是一个明显的缺陷，使得某些迭代乘积密码系统特别容易受到差分密码分析的攻击，同时在迭代过程中，只改变象素点的位置，而不改变象素点的灰度值，使得置乱后的图像依然呈某种规律性，从而很容易引起攻击者的注意，增加受攻击的概率。而基于密钥的排列算法中，以密钥作为排列的参数，参数能够唯一地确定排列的性质。

基于密钥的排列可以在频域或空间域进行。排列变换可以是局部的，或是全局的。空间域的排列加密算法实现较为简单，因为不需要使用一般频域算法所必须的空间域到频域的变换，计算量相对较少。不过，空间域的局部随机置乱效果不是很好。频域算法的优势是，在频域中每一点的变化对整个数据集合都会产生一定的影响。如图像数据经过 DCT(Discrete Consine Transformation)变换得到的 DCT 系数中如果有一个发生改变，就会通过 IDCT(Inverse Discrete Consine Transformation)逆运算体现在所有的象素点中。相对于空间域算法，频域算法序列产生效率比较高。

5.3 基于混合混沌序列的多级图像加密方法

基于以上的讨论和在文献[61,65]的工作基础上，提出一种基于混合混沌序列的多级图像加密方法。在置乱之前，利用混沌序列的随机性扰动象素点的灰度值，然后在空间域图像进行置乱，以进一步提高系统的抗攻击能力。

5.3.1 算法描述

基于混合混沌序列的多级图像加密具体算法如下：

设图像 $I(i,j), i=0,1,\cdots,M-1, j=0,1,\cdots,N-1$

① 根据 Logistic 映射的初值 x_0 产生 2^K 值混沌序列 $\{b_i, i=0,1\cdots,M\times N-1\}$；

② 利用 2^K 值混沌序列 $\{b_i\}$ 改变象素点 (i,j) 的灰度值 $I(i,j)$，得 $I'(i,j)$；

③ 利用混合混沌镜像加密算法置乱图像 $I'(i,j)$，得到 $I''(i,j)$；

④ 图像 $I''(i,j)$ 即为加密后的图像。

解密算法如下：

① 利用混合混沌镜像加密算法置乱重建图像 $I''(i,j)$，得到 $I'(i,j)$；

② 根据 Logistic 映射的初值 x_0 产生 2^K 值混沌序列 $\{b_i, i=0,1\cdots, M\times N-1\}$；

③ 利用 2^K 值混沌序列 $\{b_i\}$ 改变象素点 (i,j) 的灰度值 $I'(i,j)$，得 $I(i,j)$；

④ $I(i,j)$ 即为加密后的图像。

5.3.2 算法设计

①修改图像象素点灰度值

设原始图像为 $I(i,j), i=0,1,\cdots,M-1, j=0,1,\cdots,N-1$，根据 Logistic 映射（式 4.2）的初值 x_0，产生实数值混沌序列 x_k，利用式（4.12）得到 2^K 值序列 $\Gamma(x_k)=b_{k-1}\cdots b_0$，对于某一个象素点 (i,j) 的灰度值 $I(i,j)$，假设 $0\le I(i,j)\le 255$，将它表示为二进制 $I_7I_6\cdots I_0$，然后利用 2^K 值混沌序列 $b_{k-1}\cdots b_0$ 来修改 $I_7I_6\cdots I_0$，一般情况下，假设 $1\le K\le 8$，这里以四值序列为例（$K=2$）。如果 $b_i=00$，I_7 和 I_6 均不变；如果 $b_i=01$，I_7 不变，I_6 取反；如果 $b_i=10$，I_7 取反，I_6 不变；如果 $b_i=11$，I_7 和 I_6 均取反。通过以上的变换就可得到新的二进制序列 $I_7'I_6'\cdots I_0'$，然后转换为十进制值，即可得 $I'(i,j)$。容易发现，以上的变换等价于下面表达式：

$$\begin{cases} I_i' = (I_i + b_{i-8+K}) \bmod 2 & 8-K\le i\le 7 \\ I_i' = I_i & 0\le i\le K \end{cases} \tag{5.1}$$

② 空间域置乱

通过修改象素点灰度值的得到加密后的图像，再利用混合混沌镜像加密算法对图像进行空间域置乱，达到二次加密的目的。

设 I' 表示尺寸为 $M\times N$ 象素的一级加密后的图像并且 $I'(x,y)$，$x=0,1,\cdots,M-1$，$y=0,1,\cdots,N-1$ 表示图像 I' 在位置 (x,y) 的灰度级。$b(k)$，$k\in\{0,1,\cdots M\times N-1\}$ 是由系统（4.7）生成的混合混沌比特序列。

定义操作 $Swapping_{b(k)}<I'(p,q),I'(r,s)>$，当 $b(k)=1$ 时交换 $I'(p,q)$ 和 $I'(r,s)$ 的值，$b(k)=0$ 时保留各自的值。

算法示意图如图 5.1 所示。

在图 5.1(a) 中只考虑位于图像上半部分的象素点，由密钥决定是否由它们和位于图像下半部分的相应象素点做置换。在图像的正中间好像水平放置着一面镜子。一个像点和它的镜像点是否做置换，取决于混合混沌序列 $b(k)$ 中相应比特值，$b(k)=1$ 做置换，$b(k)=0$ 则保持它们各自位置不变。类似的置换操作可参见图 5.1(b)-(d)。这里的核心问题是当“镜子”被放置在不同的位置时，如何做镜像点的置换。

容易证明，以混合混沌二值序列为密钥应用该算法后，可能的加密结果有 $2^{2\times M\times N}$ 种。因为在每一种镜像模式中都有 $1/2\times M\times N$ 对镜像点。在假设

$prob(b(k)=1)=prob(b(k)=0)=1/2$的情况下，图像矩阵中每一对镜像点是否要做位置置换都存在两种可能，在四种镜像模式内总共需要考察$2\times M\times N$对镜像点。那么就会出现$2^{2\times M\times N}$种置换结果[66]。

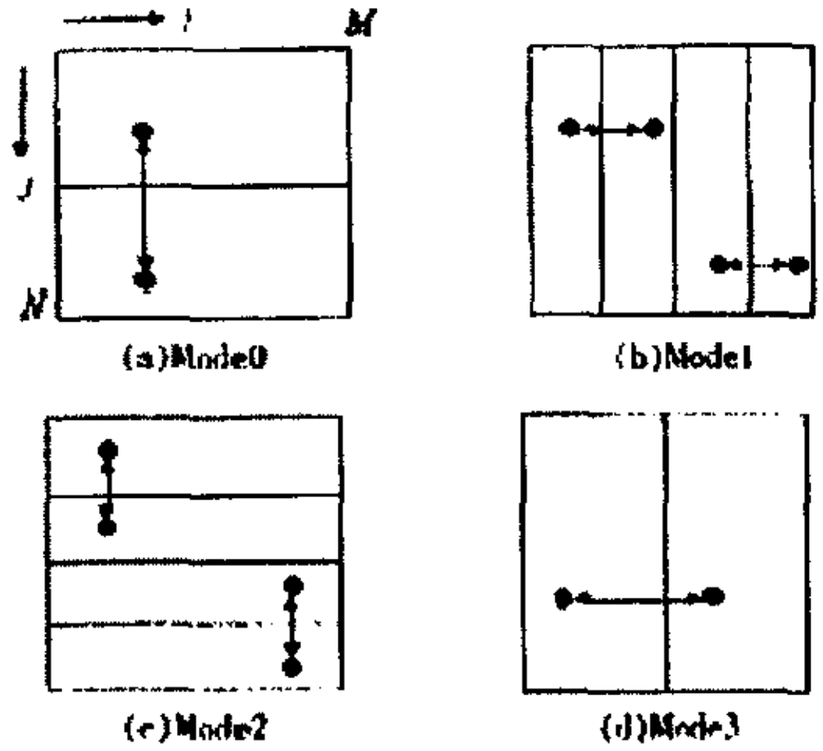


图 5.1 混合混沌镜像加密算法

Fig.5.1 Mixed chaotic mirror-like image encryption algorithm

如何标识图像块序列以及如何将它们显示到指定的位置是一个难点。我们采取的方法是把各图像块在二维空间的地址取出来，从左到右，从上到下的线性排序，生成一张子块地址索引表。用索引表来定位和查找图像块。在程序实现过程中，可以用图像块左上角的坐标作为该图像块的坐标。因此，只要构造存储所有图像块左上角点的坐标的一维 POINTS 结构数组，使数组下标序对应图像块的线性排列顺序，便实现了标识图像块并为其添加索引的功能。

设给定图像I'，w 为图像宽度，nTileSize 为子块大小，lTileNum 表示图像矩阵中包含的子块数量。图像分块算法用来将矩阵划分成一系列子块，POINTS 结构数组存储所有图像子块左上角的点坐标(x,y)，数组下标自然成为图像子块线性排列顺序的索引。

具体图像分块算法如下：

```
POINT   *point=new POINT[[lTileNum]；  //allocate tile array
 LONG   x=0,y=0；  //initialize the tile array
for(LONG   i=0;i<lTileNum;++i)
{POINT[i]. x=x  ；
POINT[i].y=y  ；
x+=nTileSize  ；
```

```
    if(x>w){x=0 ;
    y+=nTileSize ;
        }
}
```

有了这个标识各个图像子块左上角点坐标的 POINT 结构数组就可以方便的实现索引，虽然该表形式上是一维的，但其中存储的是各个图像块的二维坐标，这使得我们可以在二维空间内应用混合混沌镜像加密算法对这个一维数表进行变换，进而改变它所标识的各图像子块的空间排列顺序。

图 5.2 是对图像子块地址进行变换的例子。图 5.2 的索引表描述了一幅图像矩阵被划分为3×4个子块的情形。在图像矩阵的中央好像水平放置了一面镜子，从索引序号 0 开始依次处理图像矩阵上半部分各个子块。如图中阴影所示，对于索引序号为 3 的子块，按 Mode0 计算可得其镜像子块的索引序号为 9，查索引表得其二维地址分别为(0, 8)和(0, 24)。由于图 5.2(b)所示的符号矩阵中对应混合混沌比特序列的值为 1，因此交换两子块在索引表中的位置，更新索引表如图 5.2(c)。

在对“索引”应用过四种镜象模式，表中的块坐标经多次置换操作后，将处到一张打乱各图像块原来线性排列顺序的新地址索引表。然后，按照变换后的索引表中对子块位置排序顺序的重新标定排列图像子块。便是到加密图像 $I''(i,j)$。

③ 解密算法实现

解密算法和加密算法较为近似，差别在于，在加密算法中，空间域置乱算法作为最后一步，而在解密算法中，其为第一步，其他各部完全相同。

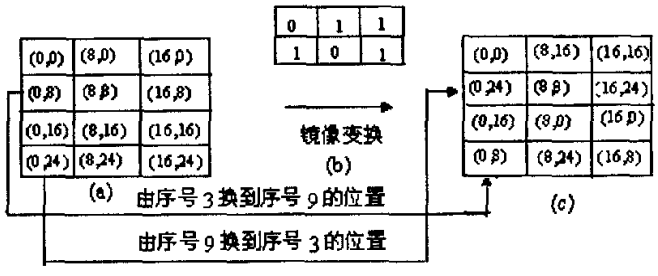


图 5.2 Model0 子块地址索引表变换示例

Fig.5.2 A demonstration of modelo's sub-block address index table transform

5.3.3 实验结果与结论

采用本文方法对 Lena 图像进行加密，图 5.3 为加密解密结果(口令字符串为 room2#desk)。我们对加密图像的安全性进程测试。由于混合混沌序列对初始值非常敏感，即使加密口令字符串很小的变化也会得到完全不同的图像字块排列顺序

和完全不同的象素灰度值，从而导致解密的结果错误。由于我们不仅在空域打乱图像的排列顺序，而且改变了图像象素点的灰度值，增强了加密图像的安全性。

本算法的优点在于：将混合混沌序列引入图像的加密算法中，充分利用混合混沌序列初始条件的敏感性、随机性好周期长等诸多特性，提出了基于空间域和改变图像象素点灰度值相结合多重图像加密算法。理论和实验证实：该算法具有加密算法简单，加密速度快，加密效果好和加密安全性高等特点。

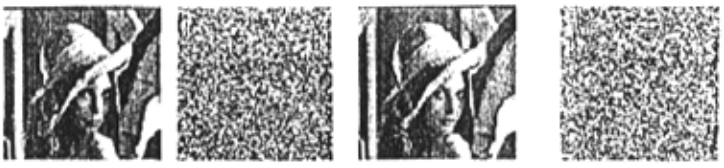


图 5.3 图像多级混合混沌加密和解密结果

Fig.5.3 The result of multistage image encryption and decryption

5.4 本章小结

本章对混沌在图像加密中的应用进行了初步探讨,提出一种基于混合混沌序列的多级图像加密方法，该算法不仅改变图像象素点的灰度值而且对图像进行空间域置乱，并用实例说明了该算法的有效性和安全性。当然，这些工作只是简单的尝试。

6 总结及展望

当前，随着网络的发展和普及，信息技术与信息产业日益受到重视。在信息的传输及处理过程中，有关如何保护信息使之不被非法窃取或窜改，亦即信息的认证与保密问题，自然成为人们关注的问题。因此密码学的理论与技术成为信息科学与技术中的一个重要研究领域。

本文主要研究混沌理论在序列密码中的应用，论文的主要工作和内容有：

① 综述了现代密码学基本原理、序列密码（流密码）和混沌理论。总结了线性反馈移位寄存器序列性质特点；阐述了混沌的起源、应用前景、定义、特征和刻画混沌吸引子的特征量。

② 从理论上对 Logistic-map 混沌序列性能进行了详细分析，在充分研究基于混沌系统的序列密码的基础上，对传统密码学和混沌密码的原理进行了分析与比较，并指出混沌序列存在的问题。利用混沌对参数敏感和 m-序列的良好随机性，提出混合混沌序列，可以克服有限精度对混沌系统的影响，对这类混合混沌序列的周期、平衡、相关性以及线性复杂性等特性进行了系统的分析。给出具体的混合混沌系统设计与实现，并进行相应的仿真实验，包括混合混沌序列的随机性、平衡性、游程特性、自相关和互相关函数及线性复杂度等多项指标，同时对该系统的安全性能进行了深入分析，如扩散扰乱特性、密钥空间、弱密钥问题和抗密码学分析等。

③ 研究了如何利用混合混沌序列进行图像加密，提出了一种基于混合混沌序列的多级图像加密算法，并对该算法进行详细的设计和分析。该算法在置乱之前，利用混沌序列的随机性扰动象素点的灰度值，然后在空间域图像进行置乱，以进一步提高系统的抗攻击能力。

混沌密码技术目前正处在发展时期，还有一系列理论问题和关键技术有待进一步深入研究，而国内的研究正处于起步阶段，根据作者的研究体会，认为以下方向、技术或内容需要深入研究和开发：

①针对混合混沌序列，需要作进一步的理论分析，确定其理论的安全性。

②由于混沌系统可以提供具有良好随机性、相关性和复杂性的拟随机序列，因此特别适合于信息加密领域。如何将混沌理论与传统分组密码学结合起来，探讨新的混沌密码加密体制，是目前混沌加密领域中的又一前沿性课题。要想使混沌密码能够象传统密码那样被广泛接受、认可和使用，有一个关键问题需要解决，就是混沌密码安全性评价标准的建立。目前还没有形成一致的观点，整体上缺乏系统的理论分析。

③ 多媒体技术的广泛应用是目前网络社会的一个普遍现象，而其中图像信息占了 70%左右。因此研究基于混合混沌序列的 Internet 数字图像加密技术具有十分广阔的应用前景。选用何种混沌系统和图像加密策略，以及为了减少传输带宽而需要数据压缩技术的集成应用等诸多问题应仔细研究与解决。

以上几个方面只是作者的体会，不能涵盖该领域的所有研究内容。总之，混沌密码学已经取得了一些研究成果，但要获得实质性的重大进展，仍然需要广大研究者的继续努力。本文的研究工作只是很少的一部分，对有些问题还只是进行了一些有意义的尝试。因此今后将在现有研究基础上继续作深入的研究。

由于作者水平有限，本论文中存在错误或不足，敬请各位专家和学者批评指正。

致 谢

首先，我诚挚地感谢我的导师廖晓峰教授。在整个研究生学习期间，廖老师在学习、生活上都给予我热情关怀和支持。廖老师在学业上给予的悉心指导，谆谆教诲，使我受益终身。他严谨、求实、认真的治学态度和科研作风，是我学习的楷模。他自始至终地关心和支持本论文的全部过程，提供了许多有价值的宝贵意见。廖老师无微不至的教导和关怀，我将永远铭记在心。

特别感谢我的师兄李传东博士，感谢他在学术上给予我的精心指导，并提供了大量的有关混沌密码领域的研究资料，这使得本论文能够按期顺利完成。

感谢廖老师举办的混沌密码课题小组的各位老师和师兄弟们，他们每周的学术报告和专题讲座使我开拓了视野，活跃了思维，并对我的研究工作提出了许多宝贵的建议。在此对他们表示感谢。

在日常的学习和研究中，我得到了杨德刚、蔡罡等同学热心的帮助和支持，在此，我向他们表示由衷的谢意！

同时，我还要感谢我的父母和亲人，没有他们的支持，我不可能取得任何成绩，尤其是他们在我漫长求学过程中对我的关系、鼓励与教诲，更是让我感激不尽。谨以此论文表达我深深的敬意和谢意。

最后，衷心地感谢在百忙之中评阅论文和参加答辩的各位专家、教授！

韦鹏程

2004 年 4 月于重庆

参考文献

[1] W.F. Friedman. The Index of Coincidence and Its Application In Cryptography. Riverbank publication No.22,Riverbank Labs,1920.Reprinted by Aegean Park Press,1987.

[2] C.E.Shannon. Communication Theory of Secrecy Systems. Bell System Technology Jounal ,Vol.28, pp.656-715, 1949.

[3] National Bureau of Standards, NBS FLPS PUB46. Data Encryption Standard. National Bureau of Standards, U.S. Department of Commerce, Jan 1977.

[4] W.Diffe and M.E. Hellman. New Direction in cryptography. IEEE Transaction on Information Theory, Vol.IT22, No.6, pp.644-654, 1976.

[5] 王衍波，薛通. 应用密码学. 北京：机械工业出版社，2003.

[6] Matthews, R. On the derivation of a chaotic encryption algorithm. Cryptologia, 1989, XIII(1):pp.29-42.

[7] Pecora M, Carroll L. Synchronization in chaotic systems. Phys. Rev. Lett., 1990, 64(8): pp.821-823.

[8] Habutsu, T., Nishio, Y., Sasase, I., and Mori, S. A secret cryptosystem by iterating a chaotic map. Advance in cryptology – EUROCRYPT'91, ed. D. W. Davies, LNCS 547 (Springer – Verlag, Berlin), 1991, pp.127-140.

[9] Biham, E. Cryptanalysis of the chaotic-map cryptosystem suggested as EUROCRYPT'91, Advance in cryptology – EUROCRYPT'91. ed. D. W. Davies, LNCS 547 (Springer – Verlag, Berlin), 1991, pp.532-534.

[10] L.Kocarev, G.Jakimoski. Logistic map as a block encryption algorithm. Phys. Lett. A, 2001, 289 (4-5): pp.199-206.

[11] J.Fridrich. Symmetric ciphers based on two-dimensional chaotic maps. Int. J. Bifurcation and Chaos, 1998, 8(6): pp.1259-1284.

[12] K.W.Wong. A fast chaotic cryptographic scheme with dynamic look-up table. Phys. Lett. A, 2002, 298(4): pp.238-242.

[13] 易开祥，孙鑫，石教英. 一种基于混沌序列的图像加密算法. 计算机辅助设计与图形学学报, 2000, 12(9): pp.672-676.

[14] 倪皖荪, 华一满, 邓浩等. 混沌通信". 物理学进展， 1996, 16(3,4):pp. 645-655.

[15] k.. M.Short. Steps toward unmasking secure communications. Int, J, Bifurcation and

Chaos,1994, Vo.4, No.4, pp.959-977

[16] 冯登国, 裘定一. 密码学导引. 北京: 科学技术出版社, 1999.

[17] 杨义先, 林须端. 编码密码学. 北京: 人民邮电出版社, 1992

[18] R.L.Lifster, A. Shamir, and L.M.Adleman. A Method for Obtaining Digital Signature and Public Key Cryptosystems. Communications of the ACM, Feb 1978, V.21, No,2, pp.120-126.

[19] B. Schneier [美], 吴世忠、祝世雄、张文政等译. 应用密码学—协议、算法与 C 源程序. 北京: 机械工业出版社, 2000.

[20] 卢开澄. 计算机密码学——计算机网络中的数据安全与保密. 北京: 清华大学出版社, 1998.

[21] 王育明,刘建伟著. 通信网的安全——理论与技术. 西安: 西安电子科技大学出版社, 1999.

[22] 肖国镇著. 伪随机序列及其应用. 北京: 国防工业出版社, 1996.

[23] R.A.RUEPPEL. Linear complexity and random sequences, Advances in Cryptology. EURO CRYPT'85 (LNCS 219), pp.167-188,1986.

[24] Janson, Boekee. The shortest feedback shift register, that can generate a given sequence, Advances in Cryptology. EURO CRYPTO'89 (LNCS 435), pp.90-99, 1990.

[25] Massey J L. Shift-register synthesis and BCH decoding. IEEE Trans. on IT, 1969, IT-15(1):pp.122-127.

[26] Jinzhong xu, Lexington, Kentuchy,. Stream Cipher Analysis Based on FCSRS. Eurocrypto2000.

[27] 吴详兴, 陈忠等.混沌学导论.上海: 上海科学技术文献出版社.1996

[28] Li T Y and Youke J A . Period three implies chaos . Am.Mathe.Monthly.1975,82,pp.985-99

[29] 唐 巍等. 混沌理论及其应用研究. 北京: 电力系统自动化. 2000.

[30] 周作领. 符号动力系统. 上海: 上海科技教育出版社, 1997.

[31] 刘延柱, 陈立群. 非线性动力学. 上海: 上海交通大学出版, 2000.

[32] 盛昭翰, 马军海. 非线性动力系统分析引论. 北京: 科学出版社, 2001.

[33] Steven M.Prinncus. Approximate entropy as a measure of system complexity. Proc Nat1.acd.sci.USA 1991,88(3):pp.2297-2301.

[34] 彭军. 混沌在网络信息安全中的应用研究[博士学位论文]. 重庆大学, 2003.

[35] L.M.pocro,T.L.Carrol. Synchronizing chaotic circuits. IEEE Trans,On Circuits and System,38(4):pp.453-456,1991.

[36] D.R.Frey. Chaotic digital encoding an approach to secure communication. IEEE Trans,On circuits and systems(II),40(10):pp.660-666,1993.

[37] K.M.Cuomo, A.V.Oppenheim. Chaotic signals and system for communication. IEEE Proc. Of ICASSP'1993,3:pp.137-140.1993.

[38] Kohda Tohur,Tsuneda Akio. Pseudonoise sequence by chaotic nonlinear and their correlation properties. IEICE Trans commun,1993,E97-B(8):pp.855-862.

[39] 凌 聪. 孙松庚.Logistic 映射跳频序列. 电子学报, 1997,25(10):pp.107－110

[40] 王 彦, 胡建栋. 改进型 Logistic Map 混沌扩频序列. 通信学报,1997(8):pp.71-77

[41] 冯登国. 密码分析学.清华大学出版社,南宁: 广西科学技术出版社,2000.

[42] 邹恩,李详飞等. 混沌及混沌应用. 计算机工程与应用,2002(11)

[43] C.E.Shannon. Communication theory of secrecy system. The Bell System Technical Journal, 1949, 28(4): pp.656-715.

[44] L.Kocarev. Chaos-based cryptography: A brief overview, IEEE Trans. on CAS-I, 2001, 1(3): pp.6-21.

[45] 丘水生, 陈艳峰, 吴敏等,混沌加密的若干问题与新的加密系统方案.2002 中国非线性电路与系统学术会议论文集, 2002.11, pp.174-179, 中国深圳.

[46] 韦鹏程, 廖晓峰, 李传东等.基于符号动力学的 0－1 序列发生器.计算机工程与应用.已录用

[47] 王毅. 基于混度序列的图象加密研究. 计算机工程与应用, 2002.20.

[48] 唐秋玲,覃团发,陈光旨. 混沌图象加密. 广西大学学报（自然科学版）,1999;24(1).

[49] 王光瑞, 陈光旨.非线性常微分方程的混沌运动.南宁: 广西科学技术出版社, 1995.

[50] 王育民. 混沌密码序列使用化问题. 西安电子科技大学学报, 1997,24(4):560-562.

[51] Robert Mathew. On the derivation of a "chaotic" Encryption Algorithm,Cryptologial,1989, (13):pp.29-42.

[52] Coppersmith, D.Kawczys,H.and Mansour Y. The Shrinking Generator. Advancesin Cryptology -Crypto'93, Springer-Verlag,1994,pp.22-39.

[53] Meler,W.and Staffetbach,O. The Self-Shrinking Generator . Advances in Cryptology Eruocrypt'94,Spring-Verlag,1995,pp.205-214.

[54] 张道法, 陈伟东. 关于对 Shrinking Generator 及 Self-shrinking Generator 的熵漏分析.通信学报, 1996,17(4):pp15-20.

[55] Golic,J. Intrinsic Statistical Weakness of Key-stream Generator. Advances in Cryptology Eurocrypt'94,Spronger-Verlag,1995,pp.91-103.

[56] J.Gernak. Digital generators of chaos. Phys.Lett.A, 1996,214:pp.151-160.

[57] 周红, 凌燮亭. 有限精度混沌系统的 m-序列扰动实现.电子学报,1997,25(7):pp.95-97

[58] E. Alvarez, A. Fernández, P. García, J. Jiménez and A. Marcano.New approach to chaotic encryption.Phys. Lett. A, 1999, 263 (4-6): pp.373-375.

[59] M.sushchik, L.S.Tsimring and A.R.Volkovskii. Performance analysis of correlation-based communication schemes utilizing chaos. IEEE Trans. on CAS-I FTAA, Vol. 47, No.12, 2001.12, 1684-1691.

[60] Z.Jako, G.Kis. Application of noise reduction to chaotic communication systems. IEEE Trans. on CAS-I FTAA, Vol. 47, No.12, 2001.12, 1720-1725.

[61]张小华，刘芳等.一种基于混沌序列的图象加密技术.中国图象图形学报,2003 年(4):374-378

[62] 吴昊升,王介生，刘慎权.图象的排列变换.计算机学报,1998,21(6):514－519

[63] Voyatzis G, Pitas I Application of toral automorphisms in image watermarking,IEEE Int conf on Image Processing,1996,2:237~240

[64]丁玮，齐东旭.数字图象变换及信息隐藏与伪装技术,计算机学报，1998,21(9):838～843

[65]王毅.基于混沌序列的图象加密研究.计算机工程与应用,2002.99～102

[66] Abidi M A , Gonzalez R C.data Fusion .san Diego.Academic Press, 1992

附录 发表的论文及参加的科研项目

1 发表的论文

[1] 韦鹏程,廖晓峰,李传东,杨德刚等. 基于动力系统的0－1序列发生器.计算机工程与应用,2005,1.

[2] 韦鹏程,杨德刚. 基于 VPN 技术的网络安全. 重庆工业高等专科学校学报,2003,18(4):25-28.

[3] 杨德刚,韦鹏程.基于整合防火墙与入侵检测技术的网络安全技术.重庆大学学报，已录用。

2 参加的科研项目

[1] 《计算机网络与信息系统安全》教材部分章节的编写.

[2] 加密系统的设计与开发.

[3] 重庆市科委应用基础研究资助项目（编号 6801）.

[4] 重庆市科委应用基础研究资助项目（编号 7370）

[5] 国家自然科学基金资助项目（编号 60271019）

独 创 性 声 明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作及取得的研究成果。据我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得重庆大学或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

学位论文作者签名：[illegible]　　签字日期：2014年 4月25日

学位论文版权使用授权书

本学位论文作者完全了解 重庆大学 有关保留、使用学位论文的规定，有权保留并向国家有关部门或机构送交论文的复印件和磁盘，允许论文被查阅和借阅。本人授权 重庆大学 可以将学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。

保密（　　），在____年解密后适用本授权书。

本学位论文属于

不保密（√）。

（请只在上述一个括号内打“√”）

学位论文作者签名：[illegible]　　导师签名：[illegible]

签字日期：2014年 6月25日　　签字日期：2014年 6月25日