混沌密码学

——应用密码学课程项目报告

小组成员：

谢成淋 1901210540
陈夏润 1901210620
李成扬 1901210420

目录

混沌密码学.....1
1. 混沌密码学简介.....3
1.1 混沌理论发展.....3
1.2 混沌加密技术的研究现状.....3
2. 混沌的基本原理和特征.....4
2.1 混沌的基本定义.....4
2.2 混沌运动的特征.....6
1）非周期性.....6
2）遍历性.....6
3）随机性和确定性.....6
4）非常复杂的有序涵盖于无序当中.....6
5）不可以预测长时间的行为.....6
3. 基于混沌的加密算法.....7
4. 基于混沌加密的图像加密.....9
5. 混沌系统与传统密码的差别.....9
6. 混沌加密的不足.....10
6.1 短周期响应.....10
6.2 限精度效应.....10
6.3 实现精度与保密性的矛盾.....10
7. 混沌密码的安全性和研究价值思考.....11
8. 参考文献.....12

1.混沌密码学简介

1.1 混沌理论发展

混沌是客观存在于自然界中的一种不规则的、有界的奇异运动形态。是一种具备确定性但又表现出随机特性的非线性动力系统，从某种意义上来看，混沌理论是继量子力学和相对论之后，20 世纪人类在物理学上的又一项重大发现。

混沌理论的各研究者表示，对这一理论进行研究的目的旨在揭示混沌的本质、刻画它的基本特征、了解它的运动状态并力求对它加以控制，将其运用在一些实际场合中。

在混沌理论的研究初期，其研究主要包括混沌系统的设计、分析和仿真，随后结合其理论特性将各种实际应用相结合，在现有的混沌理论研究中，研究重点是如何有效对其进行控制和合理利用。

对于混沌的研究发展迅速，尤其是在 21 世纪，对于混沌理论的研究已经逐步从最开始的混沌特性描述发展到现在的理论与实际结合，其研究为混沌的实际应用打下了扎实的基础。而在混沌理论的应用中，又不断得提出对混沌理论新的挑战。在近几年中，混沌理论在各种场景下有了应用，和其他学科相互渗透，发展出很多交叉学科，其应用主要包括混沌保密通讯、混沌图形加密压缩、模式识别等，而随着对混沌理论研究的不断深入，其应用也将更加广泛。

1.2 混沌加密技术的研究现状

回顾密码学的发展历史，我们可以看到，首先，其他学科研究成果的不断应用推进着密码学的发展：计算机的使用极大地增加密码算法的强度，数学难题的应用很大程度上改变了密码学的面貌等。其次，密码学还是一门很年轻的学科，从其飞速发展到如今也不过三十多年的时间，虽然目前已有大量的设计和算法出现，但其基本的设计原则和思想并没有本质的改变。当前网络信息传输产生出各种各样的需求，迫切的需要设计更多有效的算法。因而，不断借鉴各学科最新的研究成果，探索更多有效的信息安全传输手段，是密码学中不断需要着力研究和解决的问题。混沌密码就是适应这种需求而发展起来的一类新颖的信息加密手段。混沌理论自 20 世纪 60 年代从数学、物理、生物等领域发展起来，并最终在 70 年代得到基本的确立。由于混沌系统和安全系统有着诸如参数敏感性、类随机等诸多相似特性，人们很早就开始进行混沌安全系统的研究。

混乱和扩散是密码学当中指导密码设计需要坚持的基本原则。其中，扩散是在密文当中分散开明文冗余度，进而对明文的统计构造进行隐藏，而确保明文的所有位数对密文重点的多位的值产生影响是实现手段。混乱指的是对秘钥、密文、明文间的关系进行掩盖，确保尽量复杂的秘钥密文间的统计联系，让攻击密码的人员难以由密文当中获取秘钥。混沌的轨道混合特性跟传统加密系统的扩散特性相对应，混沌信号对系统参数的敏感性与类随机特性跟传统加密系统的混乱特性相对应。鉴于此，有着优异混合特性的混沌能够确保混沌加密器的混乱以及扩散的功能能够跟传统的加密算法相媲美。

1989 年，R.Matthews 定义了一个广义的 Logistic 映射，并用它产生的伪随机序列进行数据加密，自此混沌系统开始与数据加密结合起来产生了混沌密码学的定义。大量基于混沌的加密方法被相继提出，开创了使用混沌伪随机序列进行数据加密的新思路。

至此之后，大量各类不同的混沌加密算法陆续提出。时至今日，对于混沌密码系统的设计已经有了较为明确的思路，其思路主要包括以下几个方面：

1）基于混沌的序列密码（流密码）：直接用混沌伪随机实值序列作为密钥流去加密明文信息。混沌系统迭代产生的状态值是浮点数，不能直接作为密码算法的密钥。因此，此类密码算法设计的关键问题是混沌伪随机数的生成和离散化。

2）基于混沌的分组密码：S 盒（Substitution box）是构造分组密码系统的主要元件之一，也是其中仅有的非线性组成部分。因此，混沌应用于分组密码算法中研究较多的是使用混沌系统设计分组密码中的 S 盒。基于混沌系统生成动态 S 盒应用于分组加密的算法，由于对每个分组进行加密时使用的是动态变化的 S 盒，可以有效的抵御一些针对 S 盒攻击的密码学分析方法。

3）基于混沌的公开密钥密码：利用混沌理论与公钥密码相结合的思想，提出常规密码系统和混沌密码系统相结合的系统方法，提高整个加密算法的抗攻击能力。

与传统密码相同，混沌密码算法会在相应的密码攻击的推动下逐渐发展和完善。将混沌理论应用于密码学中，很大程度上促进了基于混沌的加密技术的进步。但由于密码体系自身结构和数字计算机能够处理的数据都是限精度的，势必会引起混沌系统的非线性动力特性产生退化现象，严重影响了基于混沌的密码体制的各种性能。目前已提出的混沌加密方案大多应用数值仿真给出实验结果，真正的硬件实现较少，并且混沌加密算法没有特定的算法设计基本原则和安全性能评估准则，极大的阻碍了混沌密码的发展，建立一套混沌密码系统安全性评估标准成为一个迫切需要。然而，混沌加密应从理论分析与设计的阶段走向实际应用。因此，混沌加密的研究正逐步从理论分析与设计转变到硬件实现和应用。

2.混沌的基本原理和特征

应用混沌理论属于一个学术热门话题，有着广阔的发展前景，且逐步地变成一种新型的领域，具备非常大的优势和经济效益。当前形势下，人们能够清晰地认知混沌理论以及在各种行业 当中的应用。在发展混沌理论与非线性科学的影响下，混沌课程 被普遍地应用于图像处理、信息科学、电子学等一系列的方面。其中之一就是混沌密码学。混沌密码理论借助混沌序列的伪随机特点与非周期性特点，把混沌序列充当原始明文序列以及密钥流而获取加密密文或者是进行诸位异。

2.1 混沌的基本定义

混沌是自然界中客观存在的一种基本运动形态，是普遍存在于宇宙间的各种各样的复杂性表现。混沌的发现彻底改变了人们的自然观和思维方式，并从根本上回答了自然界是确定性的还是随机性的重要问题。混沌现象隶属于确定性系统

但表现出复杂的随机行为。随着混沌现象研究的不断深化，人们对它的认识越来越具体。过去人们曾经尝试用各种不同的方式，试图找到一个合适的可以被普遍接受的混沌定义，但是混沌表现出的各种复杂特征到现在仍然没有被全部通晓，因此目前混沌在国际上还没有一个确定规范的定义。

Lorenz 曾经通俗的概括了混沌定义：对于一个确切的系统，在除去其它随机因素的作用之后，还能表现出类似随机的行为，那么就认为它是混沌的。下面介绍几种能定性描述混沌现象的定义，这几种常见的不同意义下的定义都有各自规范的数学理论和特定的分析方法，从不同的角度刻画了混沌的基本特性。

对于混沌的定义，现在在理论上还无法给出严格而广泛的定义，大部分研究人员认为将混沌准确界定不是一件十分容易的事，其原因是：

1）不利用很多专业术语无法给混沌下定义。

2）效力各种学科范畴的人，根据各自不同的专 业和研究领域，对混沌的定义及运用也是仁者见仁，智者见智。

在众多混沌的定义中，Li.Yorke 定理是被当今学者普遍认可的，其界定的出发点是区间映射，这一定义为 1975 年提出的一种在闭区间上连续自映射混沌的定义。

Li-Yorke 定义：设 F 在区间 J 上，$F:J\to J$，若 F 在区间 J 上有 3 周期点，则对于每一个正整数 k，在 J 中有 F 的周期 k 的周期点。

设有一个不包括周期点的不可数集合 $S\subset J$ 且符合下面三个条件，则认为它是混沌的：

1）对集合 S 中有两个不相等的点 p,q 满足

$$\limsup_{n\to\infty}|F^n(p)-F^n(q)|>0$$

2）对集合 S 中任意两点 p,q 满足

$$\liminf_{n\to\infty}|F(p)^n-F(q)^n|=0$$

3）对任意 $p\in S$ 的和周期点 $\mathrm{q}\in J$ 满足

$$\limsup_{\mathrm{n}\to\infty}|F^n(p)-F^n(q)|>0$$

另一个定义是 Devaney 提出，其描述为如下。

在集合中 V，如果映射 f 具备下面的前提就称该映射是混沌的：

1）f 有对初始条件的敏感依赖性；

2）f 是拓扑传递的；

3）状态点在集合 V 中是稠密的。

在上面 Devaney 的定义中，反映了混沌的难以预测性、难分解性和规律性，这三个条件又被看作是混沌运动的三要素，其中，条件 1）意味着在初始条件发生极小改变后，通过较长时间变化就难以预测出混沌的运动状态。条件 2）使系

统不可分为两个在同一映射下不彼此影响的子系统。条件 3）说明系统规律性的运动存在在看似杂乱无章的形态中。

2.2 混沌运动的特征

通常来讲，混沌是在确定性力学系统当中存在的一种和随机运动相似的运动。系统自身的非线性是形成混沌现象的根本所在，其不受到外部的影响。然而，当前形势下，严格的公认的关于混沌的概念缺少，实践证实，需要立足于混沌现象的本质特点定义混沌的概念，以及兼顾物理与数学的层次，这样才可以获得正确、系统、完善的结论。为了跟其它的复杂情况进行区分，通常都认为混沌的基本特点是：

1）非周期性

作为一种非线性动态系统的一种可能定态的混沌来讲，相空间的轨道并非一味改变的，也并非周期性的，属于非周期性起伏、曲折地改变，而判定系统的非单调行为是周期运动或者是瞬间运动的看法都是不对的。

2）遍历性

一种混沌吸引域（确定的区域）是混沌运动轨道的限制，且混沌区域之内的所有状态点都被混沌轨道所经过。

3）随机性和确定性

确定性指的是对力学系统微分方程当中的系数的描述是确定的，不具备概率性的要素。针对初始值的确定，确定性方程将确定的解给出，对系统确定的行为进行描述。然而，在一部分非线性系统当中，如此的过程会由于扰动非常小的初始值而出现比较大的改变。因为系统的初值敏感性，以物理作为视角，如此的过程好像是随机性的，然而确定性系统内部本来就具备的就是如此的随机性，因此又被叫做内存随机性。

4）非常复杂的有序涵盖于无序当中

从表面上而言，混沌运动的随机现状是无序混乱的，然而，如此的随机现状属于内在的随机现状，有序涵盖于随机当中，由混沌的相空间对一部分任意地取出，且进行放大，依旧跟整体相似，具备一定的自相似性和无穷尽的精细构造。

5）不可以预测长时间的行为

因为对初始的条件比较敏感，和随机运动相同，难以有效地预测混沌系统的长时间行为。然而，不可以一味地认为不能够预见混沌运动。为此，混沌系统的演化方程式是确定性的，混沌吸引子具备确定的相空间位置，能够预测短时间的行为。吸引子的运动跟一定的概率规律相服从，有着统计作用的可预见性，发现混沌可以使人的预见性提升。

3.基于混沌的加密算法

混沌轨道的发散特性和对初值的敏感性正好对应着 Shannon 提出的密码系统设计的扩散原则。混沌吸引子的内随机性和对系统参数的敏感性正好对应于混淆原则。混淆是指要尽可能复杂化密文与明文之间的统计性和相关性，使得密码分析者无法利用。扩散使明文每一位的影响尽可能作用到较多的密文位中，同时使密钥每一位的影响尽可能扩展到较多的密文位中，以此达到隐藏明文统计特性的目的。混沌系统具有良好的伪随机性，可以满足许多流密码的要求，能够很好地通过各项标准的统计检验，能够增强密码算法的混淆和扩散特性。在混沌算法中，Logistc 映射是一种较为常见的混沌算法。

Logistic 映射：是一类简单但被广泛运用的动力系统，可以用来模拟生物种群数量的生长行为，所以又称“虫口模型”。

假设有一种昆虫，每年夏季成虫产卵后全部死亡，第二年春天每个虫卵孵化为一个成虫。设第 n 年的虫子数目为x_n，每只成虫平均产卵 a 个。这样的过程年复一年的重复下去，一般规律可以写成 $x_{n+1} = ax_n$，进一步推导可得：

$$x_{n+1} = a^n x_0$$ ，其中 x_0 是起始年度的虫子数量

但考虑到种群数量上升后的内部竞争和资源的有限性，一定会存在对于种群数量的负相关的作用。 因为 x_n 只虫子配对的事件总数是 $\frac{1}{2}x_n(x_n-1)$。当 x_n >> 1 时，基本上是 x_n的平方。因而虫口模型可以用公式表达为：

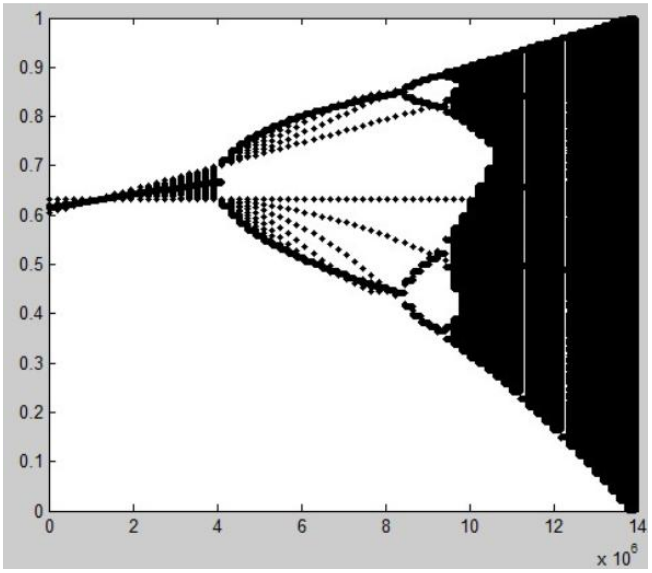
$$x_{n+1} = ax_n - bx_n^2$$

进一步简化，

1. 设环境能承受的最大虫口数为 M，第 n 代虫口数为 n，我们用x_n表示第 n 代相对虫口数，于是有 x_n=n/ M，相对虫口数不会大于 1, 即 $x_n \in [0, 1]$
2. 令 a = b = μ，为了满足x_n 的取值要求，μ ∈（0，4）
3. 可得公式为：

$$x_{n+1} = ux_n(1-x_n), \quad x_n \in [0, 1], \quad \mu \in (0, 4)$$

从这里可以看出，初始状态x_0与参数μ可作为为种子密钥，研究发现，当参数 μ 在[3.57，4.00]之间时，产生的混沌序列的随机性比较好即混沌效果最佳，仿真对比结果如图所示



除 Logistic 映射的混沌加密外，还有一些其他场景离散混沌系统：

Arnold 映射，

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod 1$$

3D-Lorenz 系统，

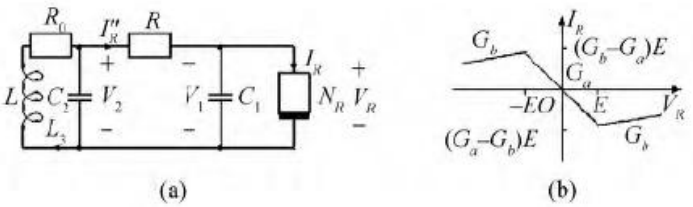
$$\begin{cases} x_{n+1} = x_n y_n - z_n \\ y_{n+1} = x_n \\ z_{n+1} = y_n \end{cases}$$

连续的混沌系统：

Lorenz 系统，基于大气环流，

$$\begin{cases} \dot{x} = -a(x-y) \\ \dot{y} = bx - y - xz \\ \dot{z} = xy - cz \end{cases}$$

Chua 电路，



4.基于混沌加密的图像加密

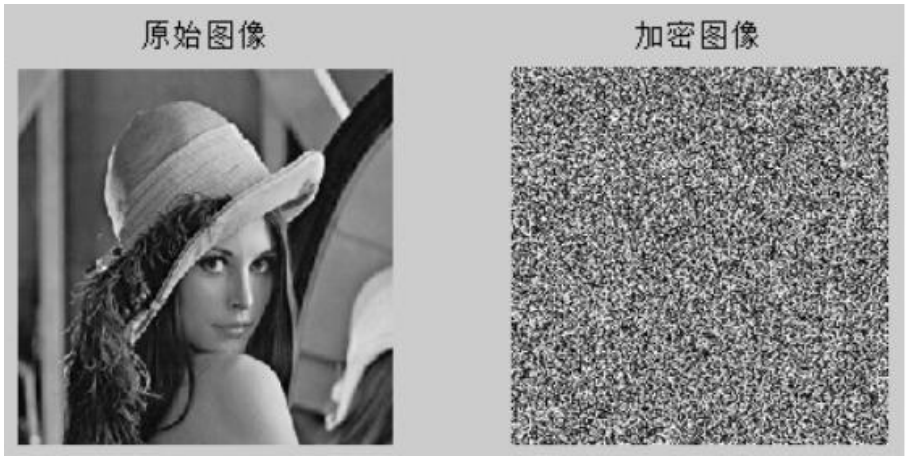
对于图像数据来说，相邻像素之间存在强相关性，同时图像的数据量比较大，诸如 AES，DES，IDEA 之类的传统加密算法不适合有效加密。基于混沌系统的随机性和敏感性特征，我们可以用它来生成伪随机序列，这可用于流密码或者或分组密码中。

许多学者提出了许多基于混沌的图像加密算法，可以对像素位置进行干扰。但是许多数算法被证明是不安全的，并且容易遭受密码分析等经典攻击。低维度的混沌密码简单，易于实现，但是系统的密钥空间较小。此外，在数字计算机中，混沌系统的周期性可能会以有限的精度降级。多维超混沌系统可以为加密过程提供多个混沌序列，以扩大密钥空间并消除动态降级。同时，可以使用多维超混沌系统提供伪随机混沌序列，结合普通图像用分组密码来计算其初始值用于代替或置换，或者基于流密码体系，利用混沌序列作为密钥进行加密。

因为上述的 logistic 映射方程是针对一维数据的，换言之，要生成 n 位的字符流需要处理 n 此，由x_0，x_1，，，χ_n 构成。图像的 RGB 范围为【0，255】，因为χ_n的范围是【0，1】因为容易映射。
加密的密钥是 x_0 和 μ

加密流程如下：
1） 对于 M*N 的图片 p, 使用 logistic 映射方程生成 M*N 的序列流
2） 将序列流与图片进行异或，即完成加密

下图为通过混沌序列作为伪随机序列进行加密的结果，分别是加密前和加密后的图。



解密过程，仅需将图片再次与基于 x_0 和 μ 生成的序列流进行异或即可。

5.混沌系统与传统密码的差别

常见的混沌系统是基于实数域的，但传统的密码学是基于离散的整数域的。这就导致当前混沌理论运用于密码学时，必须进行离散化处理，而这又会导致混

沌系统本身的安全性得不到保证，以及难于分析。

6.混沌加密的不足

6.1 短周期响应

现有的混沌序列的研究对于所生成序列的周期性、伪随机性、复杂性、互相关性等的估计是建立在统计分析上，或是通过实验测试给出的，这难以保证其每个实现序列的周期足够大，复杂性足够高，因而不能使人放心地采用它来加密。例如,在自治状态下，输入信号为零时，加密器表现为有限周期响应。不同的初始状态对应于不同的周期,其周期长度可能很短。这一缺点在某种程度上降低了混沌加密系统的保密性。

6.2 限精度效应

混沌序列的生成总是要用有限精度器件来实现的，从而混沌序列生成器可归结为有限自动机来描述，这样，混沌生成器否能超越已有的用有限自动机和布尔逻辑理论所给出的大量研究成果，是一个很值得研究的课题。大多数在有限精度下实现的混沌系统，其性质会与其理论结果大相径庭,从而使许多基于混沌系统的应用无法实现。甚至有学者认为，有限精度效应是目前混沌理论走向应用中出现的一大难题。

6.3 实现精度与保密性的矛盾

对于分段线性的混沌映射加密系统，相邻的两个状态可能落在同一条直线段上，这样，在数字实现精度很高的情况下，解密者就可利用此特点，在知道少量的明文-密文对照的情况下轻易地恢复出具有足够精度的密钥。也就是说，它对于选择明文攻击的抵抗力很差，从而在这一意义上不具有保密性。任何特定混沌序列的实现都是由其非线性方程和相应的初始条件完全确定了的，有人在研究跟踪混沌序列进行破译的工作。

解决了上述三个问题，混沌序列才可能在密码设计中得到广泛应用。且人们已发现，用由低维动力学系统产生的混沌可短期预测，所以用它来构造保密通讯系统的保密性是脆弱的，这是由于低维系统的混沌序列只有一个正的 Lyapunov 指数(LE)，正的 LE 值反映混沌系统对初值的敏感性，因而人们就想到利用高维动力系统产生超混沌，使正的 Lyapunov 指数个数大于 1，得到超混沌信号，以提高保密性能，但高维动力学系统的维数毕竟还是有限的，系统的自由度要受到维数的限制。近年来,出现了具有时延的动力学系统用于保密通讯的研究，一个典型的例子是 Mackey-Glass 系统。时延动力学混沌系统是无穷维的系统，它不仅对初始时刻的初值极其敏感，而且对时延时间段[τ ,0]上的初值函数 ϕ (y)极端敏感，利用这些性质可构造出密级高的混沌码序列。

为了在密码学中有效地使用混沌理论，应该实现混沌映射，以使映射生成的熵可以产生所需的混淆和扩散。混沌系统和密码基元中的属性共享独特的特征，这些特征允许将混沌系统应用于密码学。如果可以对称地映射混沌参数以及加密密钥，或者可以映射混沌参数以生成可接受的功能输出，那么对手几乎不可能在不了解初始值的情况下找到输出。由于现实生活中的混沌图需要一组有限的数字，因此，如果可以预测混沌行为，则它们实际上在密码系统中可能没有任何实际用途。对于任何密码原语而言，最重要的问题之一是系统的安全性。但是，在许多情况下，事实证明基于混沌的加密算法是不安全的。在许多经过密码分析的算法中，主要问题是系统中实现的混沌映射的不足。

7.混沌密码的安全性和研究价值思考

由于离散化的混沌系统缺乏合适的理论分析工具，因而当前的分析主要是利用计算机仿真，且结果为统计平均的反映，这页是主要的缺点之一，因为没有办法保证单独某次的安全性。但我们没办法质疑混沌系统高强度的非线性，虽然因此也致使系统本身很难具有合适的数学结构，但本身数学结构的混乱性，如果得以合理的运用，在对抗攻击方面又会转变为另一种优势。 且当前的密码学发展，迫切需要我们提出更为有效的算法，与其他学科的有效结合是发展的一种必然尝试的思路。诚然，我们看到当前混沌系统发展与使用的局限性，但是如果离散化技术上、安全分析方法能够得到较多突破的话，可能会迎来第三次的发展高潮。

8.参考文献

1. Chai X, Fu X, Gan Z, et al. A color image cryptosystem based on dynamic DNA encryption and chaos[J]. Signal Processing, 2019: 44-62.
2. Liu Q, Li P, Zhang M, et al. A novel image encryption algorithm based on chaos maps with Markov properties[J]. Communications in Nonlinear Science and Numerical Simulation, 2015, 20(2): 506-515.
3. Çavuşoğlu, Ünal, Kaçar, Sezgin. A novel parallel image encryption algorithm based on chaos[J]. Cluster Computing, 2019.
4. Mosola N N, Dlamini M T, Blackledge J, et al. Chaos-based encryption keys and neural key-store for cloud-hosted data confidentiality[J]. 2017.
5. Mareca P, Bordel B. A Robust Implementation of a Chaotic Cryptosystem for Streaming Communications in Wireless Sensor Networks[C]. world conference on information systems and technologies, 2017: 95-104.
6. 赵耿, 田玉露, 殷岁. 混沌密码算法及相关进展(一)[J]. 北京电子科技学院学报, 2016(4).
7. 廖春龙. 基于混沌理论的图像加密算法的分析与设计[D]. 中南大学, 2013.
8. 混沌运动的特征及其在密码学中的应用研究_杨柳
9. 杨柳. 混沌运动的特征及其在密码学中的应用研究[J]. 电子测试, 2016, No.344(09):14+44.
10. 王悦. 超混沌系统的研究及其在图像加密中的应用[D]. 哈尔滨理工大学, 2015.
11. 尹汝明, 袁坚. 关于混沌密码及其关键问题的思考[J]. 中国电子科学研究院学报, 2008(06):27-33.
12. 郑丽华. 混沌中的哲学[J]. 广东社会科学, 1998(1):71-74.
13. 郝伯林. 从抛物线谈起——混沌动力学引论[M]. 上海科技教育出版社, 1993.