基于超混沌的像素级和比特级图像加密算法

由于图像数据本身具有大数据量，高冗余和相邻数据有强相关性的特点，使用AES等传统加密算法并不适合用于图像加密。
本文所提出的混沌系统具有遍历性，非周期性，对初始条件和控制参数具有高灵敏度和类随机行为等优良的内在特性。基于混沌映射的典型加密过程可以分为两个部分：置换和融合。在图像加密这一研究领域，之前的主流方式是在像素级排列的图像加密，像素级加密本质上就是对于图片以非线性形式进行重组排列，难以抵御选择明文和选择密文攻击。
如基于混沌切比雪夫发生器的图像加密算法，使用非线性切比雪夫函数生成密钥，相较于先前的其他系统的设计优势在于，整体降低了计算复杂度并维护安全性，主要流程简单来说就是，先生成两个伪随机序列，再将随机序列用于二维混沌切比雪夫函数，并同时添加参数用以扩大密钥空间。系统保证了足够大的密钥空间，且对初始条件足够敏感。

Image encryption algorithm using chaotic Chebyshev generator

还有一篇基于简单表查找和交换技术的有效扩散方案作为图像混沌映射的轻量级替代，并且基于混沌理论的思想和拉丁方模式，使其在程序层面性能高于浮点运算。拉丁方的构成有点类似于数独，定义上是一种为了减少实验顺序对于实验的影响而采取的一种平衡实验方式，从0开始，构成一个n个不同整数的集合，集合的n阶拉丁方是一个n行n列的数组，并且每一项都是集合内元素，使得数组的每一行每一列都只出现一次相同的元素。
在这篇文章设计的系统中，对于N*N的图像进行总共2N次混沌迭代以构建LUT，不仅将LUT用于像素排列，也用于图像扩散。他的优势在于，在另一篇文献中提到的传统的使用混沌系统针对图像的加密系统中，需要使用两个混沌状态变量加密一个像素以保证安全性，这篇文中提出的方案是平均2/N个混沌状态变量就可以，相应的好处就是提升了速度，同时维持了鲁棒性。

An efficient image encryption scheme using lookup table-based confusion and diffusion

在对于图片进行比特级加密运算方面，提出了一种基于循环移位、交换和PWLCM分段线性混沌映射(Piecewise)混沌映射的比特级图像加密方案。PWLCM是一种混沌映射方式，使用

NPCR（像素数变化率）和UACI（均匀平均变化强度）评估加密算法的防御差分攻击性能。
首先使用BBD二进制位平面分解将普通图像分解为八个位平面，接着将位平面任意分为两组，将两个组转换为两个二进制序列A1和A2，位平面的元素从上到下，从左到右从高到低顺序排列。在扩散阶段，采用混沌、循环移位和XOR运算来改变A1和A2中的位值，然后产生B1和B2。在混淆阶段，通过使用来自混沌映射的控制来交换B1和B2中的二进制元素，然后我们获得C1和C2。
最后，通过将C1和C2转换为位平面并组合所有位平面，获得密码图像。第n轮用于进一步提高所提出系统的安全性。混沌映射的初始参数和条件作为密钥。

A novel bit-level image encryption algorithm based on chaotic maps

除此之外，人们发现DNA计算具有大规模并行、巨大存储和低功耗的特点，提出了很多基于DNA规则的图像加密相同的特点，然而却同样具有像素级图像加密算法的弱点。每个DNA序列包含四个碱基对，分别是A(腺嘌呤),C(胞嘧啶),G(鸟嘌呤),T(胸腺嘧啶)其中A和T、C和T是互补对，也就是说能组成24中编码，其中8种满足互补规则，现在我们使用四个核酸碱基C、T、A和G分别表示二进制值00、01、10和11，灰度图像的每个8位像素值可以编码为核苷酸串，这就完成了编码部分的设计。
这我阅读的这篇文章中，首先通过PWLCM生成分别排列行与列，通过DNA编码将每个像素编码为四个核苷酸，然后使用互补规则将每个核苷酸转换成其对应的碱基对，这些碱基对使用切比雪夫混沌映射生成,能够保证密钥在不改变公钥的情况下为每次加密而改变，并获得较大的密钥空间。

Image encryption using DNA complementary rule and chaotic maps

相较于低位混沌系统和高位混沌系统，超混沌系统由其所不具备的优势，即更大的密钥空间，更好的灵敏度、更加复杂的动态特性和随机性。直到这篇文章提出的算法之前，还未有同时使用像素级和比特级排列的算法，此外并采用超混沌系统来抵御破译低维混沌映射的一般方法。这是一篇目前引用次数342的文章。

对于基于混沌图像密码系统，时间消耗主要来源于混沌映射迭代和量化操作，在满足安全要求的前提下，对于这几方面的优化可以有效提升性能。

混沌系统

这里的混沌并非指的是无序，而是当一个简单确定的系统不仅可以产生简单确定的行为，还可以

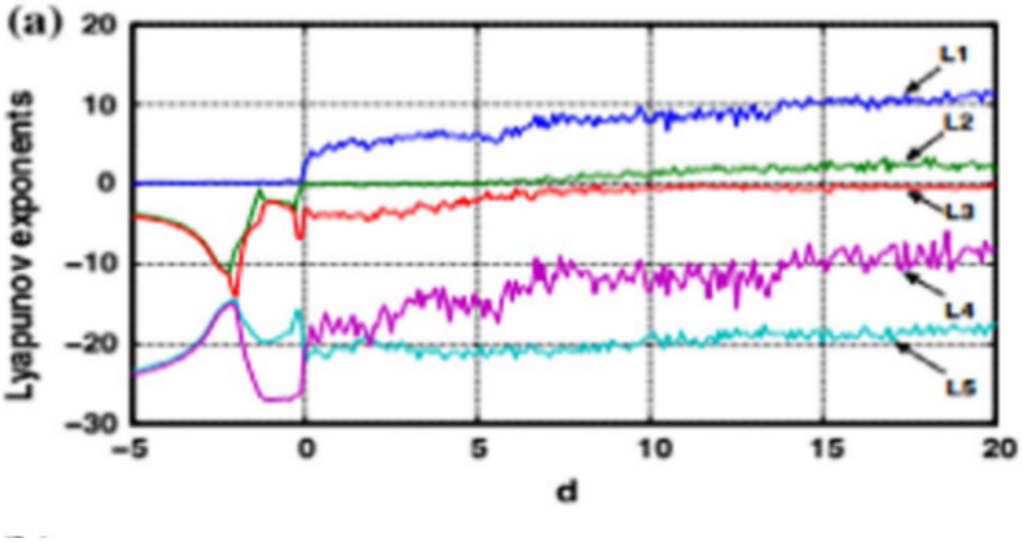
产生貌似随机的不可确定行为。对于混沌的定义是指确定的宏观非线性系统在一定条件下所呈现的不确定的或不可预测的随机现象；是确定性与不确定性，规则性与非规则性；有序性与无序性融为一体的现象。这也和香农提出的密码学扩散混淆理论有一定相似之处。我们对于混沌定义以下几个特征:

- 首先是对于初始条件的灵敏依赖性，通俗来说就是蝴蝶效应，“失之毫厘差之千里”，局部或足够微小的扰动都会对于系统最后的结果产生较大的改变。
- 长期不可预测性，混沌的非线性动力学特性决定了混沌是不可预测的，一方面混沌对于数值的高敏感决定了对于算法的预测存在相当的难度。另一方面当尝试预测时，每次都会丢失部分信息，预测的次数越多，最后丢失的信息便越多，难以保证长期预测，因而不可预测。
- 分形性，分形性指混沌的运动轨线在相空间中的行为特征，表示混沌运动状态具有多叶，多层结构，且叶层越分越细，表现为无限层次的自相似结构。
- 有界性，混沌运动轨线始终局限于一个确定区域，混沌吸引子是混沌有界性的最好体现。
- 遍历性，混沌运动在其混沌吸引域内是各态历经的，在有限时间内混沌轨道不重复地经历吸引子内每一个状态点的邻域。
- 混沌的运动限于有限区域且轨道永不重复，且具有丰富的层次和自相似结构。

如图所示，这里是一个5-D多翼超混沌系统,我们称其为系统(1)。其中包含三个非线性元素，五个状态变量x1~5和8个参数abcdefgh。实验中我们选择a=10，b=60，c=20，d=15，e=40，f=1，g=50，h=10，初始条件为（1，1，1，1，1）。结果显示五个参数中L1-3大于零，系统是超混沌的。

$$\begin{cases} \dot{x}_1 = -ax_1 + x_2x_3 \\ \dot{x}_2 = -bx_2 + fx_5 \\ \dot{x}_3 = -cx_3 + gx_4 + x_1x_2 \\ \dot{x}_4 = dx_4 - hx_1 \\ \dot{x}_5 = ex_5 - x_2x_1^2 \end{cases}$$

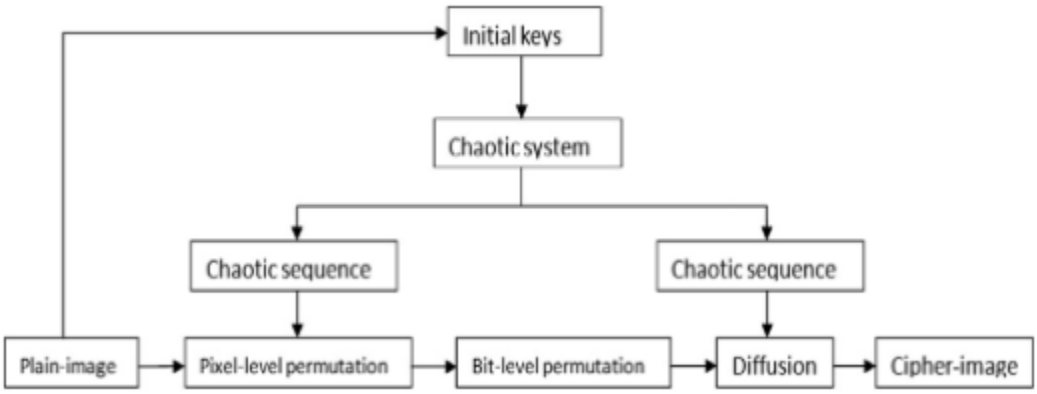
下面首先引出一个概念：又称李雅普诺夫特征指数，是用于识别混沌运动的一个特征
。常常被用来判定一个系统的混沌性，通过图像可以直观地看出某个系统或者映射是否是混沌系统或映射。
判定依据是当其大于0时，说明系统会进入混沌态，对应的映射也具备被称为混沌映射的资格。小于零时说明会趋于稳定且此时对系统的初始状态不敏感，等于零时说明系统稳定。



首先文中给定实验参数从图中实验可以看出，当d<0时，系统是稳定的，此时没有出现正李雅普诺夫指数，当d在8.8和20之间时，系统被证明是混沌的，而d大于20后，系统是超混沌的。

图像加密算法详情

算法共分为四个部分：首先根据处理图像的特征生成对应的混沌序列，采用像素级排列以混淆图像，接着利用位级置换来增强秘密系统的安全性，最后通过扩散得到密文。



- 像素级排列过程

像素级排列的本质是为了破坏像素的相关性，在文中的设计为：
首先将数字图像矩阵转为一维向量，比如一个`m*n`形式的像素，对其作扁平化处理，得到一个一维向量，长度为`m*n`。
计算所有像素的总和，根据以下公式计算出混沌系统的初始密钥x1~x5。这里的s是图片的面积。

$$\begin{cases} x_1 = \frac{sum + S}{2^{23} + S} \\ x_i = \mod(x_{i-1} \times 10^6, 1) \quad i = 2, 3, 4, 5 \end{cases}$$

接着我们使用前文所提出的混沌系统(1)，进行N0+m*n次迭代，之后丢弃前N0个值以避免有害的影响，产生的混沌序列有`m*n`个元素，记为L。
在这部分的最后一步，我们将使用混沌序列对图片向量进行处理，将混沌序列按升序排列，得到一个序列L'，对图像像素序列P进行像素位置的置换，得到处理后的最终序列Q。

- 比特级置换过程

在这个过程中，对序列使用比特级排列来改变像素的位，位置换过程将重新创建四个新字节，通过组合四个字节的方式改变每个字节的位。从数学角度来看，这部分的操作本质上相当于一个向量乘以一个常数矩阵。
将上一部分最后得到的混洗序列Q分解成4*4的矩阵，接着将一个常数矩阵和分割出的子矩阵相乘，得到一个新的矩阵，常数矩阵和逆矩阵如下图所示。

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \quad \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$$

重复计算直到所有子矩阵都完成了一轮比特级置换操作，然后组合子矩阵获得矩阵D，其尺寸为m*n

- 扩散阶段

扩散过程可以大大增强对统计攻击和差分攻击的抵抗力，保证密文图像的直方图相当均匀，并且要与普通图像的直方图显著不同。
为了实现良好的扩散过程，应使用与普通图像密切相关的关键流。当对不同的平面图像进行加密时，我们可以在加密算法中得到完全不同的混沌序列。

根据下述公式获得密钥流，其中的L是混沌序列。

$$K_i = \mod((abs(L_i) - floor(abs(L_i))) \times 10^{14}, 256)$$

并通过下公式加密图像矩阵D的像素值:

$$C_1 = \mathrm{mod}(D_1 + C_0, 256) \oplus \mathrm{mod}(Q_1 + K_1, 256)$$

$$C_i = \mathrm{mod}(D_i + C_{i-1}, 256) \oplus \mathrm{mod}(Q_i + K_i, 256) \quad i = 2, 3, \ldots, m \times n$$

其中C0是一个定义的常数，也可以用作加密密钥。

然后重复步骤2，直到i=m*n,得出最终的密码图像C。

- 解密阶段

解密过程与加密过程相反，首先得到混沌系统产生的混沌序列之后，并通过以下公式执行扩散的逆运算以获得加扰图像D',然后执行类似的矩阵切割操作，利用上面给出的逆矩阵进行相应的逆运算，对于加密过程中的像素级排列我们已经知道排列过程，在这里执行反转操作便可以得到原来的图像。

$$D'_i = \mathrm{mod}((C_i \oplus \mathrm{mod}(Q_i + K'_i, 256) + 256) - C_{i-1}, 256) \ i = 2, 3, \ldots, m \times n$$

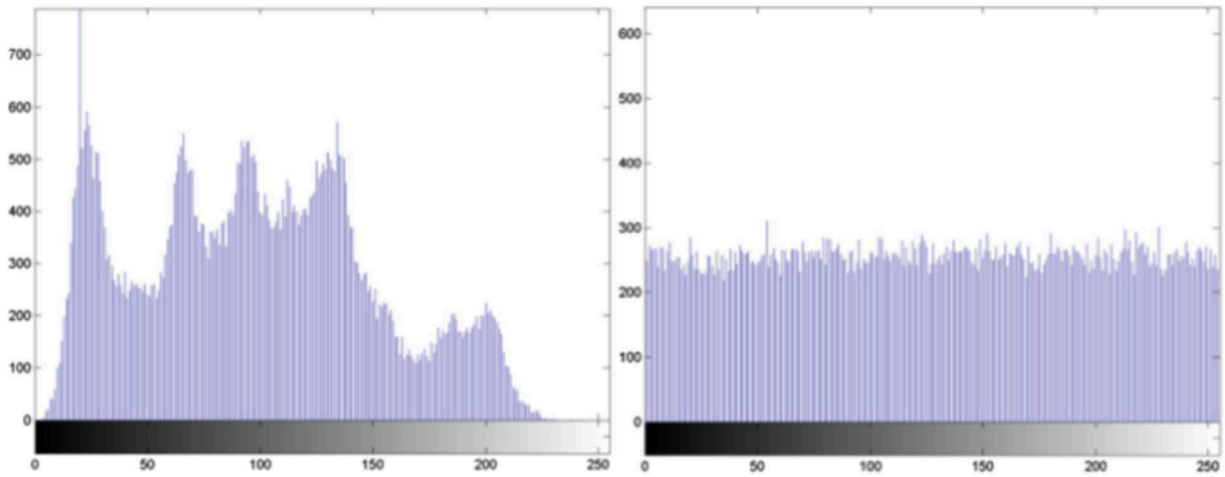
安全性分析

- 密钥空间

在该算法中，密钥包括混沌系统的初始值，迭代次数N0和常数C0，取常数C0 = 28，初始值的精度为`10^16`，总密钥空间大约为`2^273`。而对于嵌入式密码系统，密钥空间的大小应该不低于2^100，本算法是完全符合要求的。

- 直方图分析

其次是直方图分析，对于原始图像的加密算法要求产生的加密图像与原图片相似度差且像素分布均匀，对于每个密钥的数量分析，我们计算直方图的方差以评估加密图像分布的均匀性，方差值越低，表示加密图像的均匀性越高。



实验中对于明文图像的直方图值为33860.0547因而表明所提出的算法可以抵御任何形式的攻击。

- 相关性分析

原始图像的响铃像素在水平、垂直和对角线方向上具有高相关性。理想的加密算法应当保证加密图像的像素有相当低的相关性以抵抗统计攻击。实验中为了分析和比较加密前后的相关性，随机选择了每个方向上的一万组相邻像素对，相对于原始图像中相关性接近于1，加密后图像在三个方向上的相关性都能保证尽可能接近0，说明算法的混淆性和不确定特性都相当良好。

- 差异性分析

为了抵御不同的攻击，一个好的密码系统应该确保普通图像中的任何微小修改都会导致密码图像中的显著差异。NPCR和UACI理想值分别为99.61%和33.46%，通过对于500个明文只有不同像素的密码图像，证实该算法能够有效抵御差分攻击。

- 信息熵分析

信息熵是用以考量随机性的重要度量，假设信息源发送256个字符，我们计算理论信息熵值时，越接近8说明越具有良好的信息熵特性，实验中给出的明文图像计算后得到的信息熵是7.9972，说明信息熵特性良好。