基于Rossler系统、PRNG S-Box和Recaman序列的图像加密

Mohamed ElBeltagy,

Wassim Alexan

*SMIEEE*

*及埃及开罗德国大学IET学院*

[wassim.alexan@ieee.org](mailto:wassim.alexan@ieee.org)

[mohamed.elbeltagy@ieee.org](mailto:mohamed.elbeltagy@ieee.org)

Mohamed Moustafa

*埃及开罗德国国际大学信息学和计算机科学行政资本学院*[mohamed.dawood@student.giu-uni.de](mailto:mohamed.dawood@student.giu-uni.de)

Hisham H. Hussein

*埃及开罗加拿大行政首都大学科学与创新学院*

[hisham.hussein@uofcanada.edu.eg](mailto:hisham.hussein@uofcanada.edu.eg)

***摘要***

**本文提出了一种仅基于3个步骤的轻量级图像加密方案。第一步是使用Rossler吸引子用于Rossler系统，第二步骤使用S-Box作为PRNG(伪随机数发生器)，而第三步骤使用Recaman序列。使用多个度量来评估所提出的加密方案的性能。度量的计算值表明，在处理时间成本非常低的情况下，与文献中的对应方案相比，性能相当。这种特性表明，所提出的图像加密方案具有实时图像安全应用的潜力。**

***关键词***

**密码学、图像加密、Rossler系统、Recaman序列、s-Box。**

1. 引言

数字图像处理和网络通信的重大发展促进了人们在互联网和无线网络上对于实时安全图像传输的巨大需求[1]。因此，基于密码学和隐写术[2]–[7]的数据加密手段确保了数以百万计的在线应用程序得以安全可靠的运行 [8]。加密技术在信息安全中有着至关重要的作用，吸引了无数科学家和工程师的关注和研究，经过数十年，加密技术得以快速发展并取得了累累硕果 [9]-[11]。近期，全球的研究员正专注于改进图像传输的安全性，在此基础上提出了新的密码系统，包括细胞自动机、DNA编码和混沌理论[12]-[14]。

混沌系统具有伪随机性、遍历性和对初始条件和对初始参数的高度敏感性。因此，它被广泛用于图像加密范畴。在加密领域中，混沌系统常常用于一次或反复多次的PRNG(伪随机数发生器)以及真正的RNG(真随机数发生器)的一部分。关于PRNG的文献结合了混沌理论[15]、[16]、数学序列[17]、电路[18]、量子物理学[19]以及许多其他方面的实例。

Rossler系统是一个具有单个二次交叉项的三阶连续时间微分方程系统，并以奥托·罗斯勒于20世纪70年代引入的3个值作为参数[20]。这些微分方程创建了一个连续的时间动力学系统，构建了与吸引子分形特性相关的混沌动力学[21]。计算的特征通常涉及在极限环的倍周期级联之后产生单瓣混沌吸引子（简称为螺旋型），有时涉及由于同宿轨道的存在而产生更复杂的混沌吸引子（简称为螺杆型）[22]。Rossler系统的一些性质可以通过线性方法（如特征向量）得出，但该系统的主要特征需要非线性方法（如庞加莱映射和分叉图）获得。最初的Rossler研究论文指出，Rossler吸引子以Lorenz吸引子为蓝本进行设计，故二者有较为相似的性质，同时它也同Lorenz吸引子具有更容易进行定性分析的优点[21]。

Recaman序列是一个有趣且易于实现的整数序列，但由此序列产生的强复杂性在密码分析上的强大之处d。[23]的作者将基于Recaman的序列图像隐写术用于2D图像，此方案展现了优异的性能和强大抗隐写分析的能力。

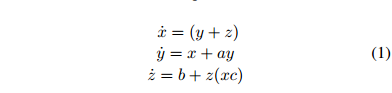
在密码学中，S-Box（替换盒）是执行替换的对称密钥算法的基本组件。在分组密码中，它们通常用于模糊密钥和密文之间的关系，从而确保Shannon的混淆特性。第一个S盒用于对称密钥算法，如高级加密标准（AES）和数据加密标准（DES），但此类S盒的主要问题是弱于统计分析攻击。因此，为了产生动态低耦合度的密钥，PRNG和混沌系统被用于构造S盒，如[24]和[25]所示。[26]的作者介绍了一种基于Rossler系统构建S盒的新方法，其中所提出的S盒在抵抗攻击方面有很好的表现。[27]中提出了另一个构造S盒的不错范例。[27]的作者使用了一种新的变换、模逆和置换来构造他们的S盒。通过基于文献中设定的标准的比较和性能评估，其加密强度得以验证。

在本文中，我们提出了一种基于三个步骤的图像加密方案。第一步骤使用Rossler系统，第二步骤使用S-Box，第三步骤使用Recaman序列。本文按照如下的顺序进行讲解：第二节简要介绍了Rossler系统，然后是基于S-Box的PRNG和用于目标图像加密方案的Recaman序列。第三节概述了计算和测试的数值结果，并对其进行了适当的评论。第四节最后得出了论文的结论，并提出了可以进一步开展的未来工作。

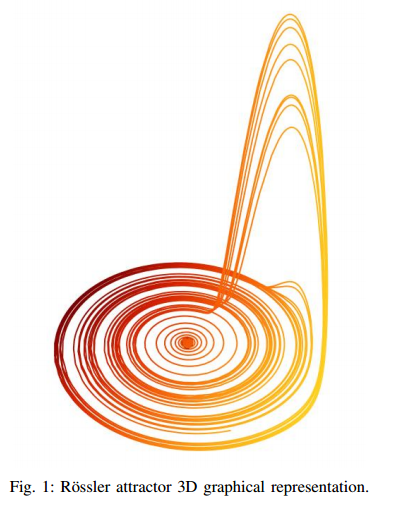
1. 提出的图像加密方案

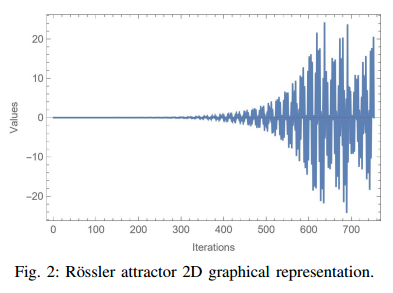
提出的图像编码方案由三个步骤组成。第一步骤使用Rossler系统，第二步骤使用PRNG S-Box，第三步骤使用Recaman序列。接下来的几节将分别介绍这三个概念。

A、 Rossler吸引子

Rossler系统是一个很牛逼(原文infamous，但是非正式用法)的连续动力系统原型，由以下3个非线性微分方程组定义：

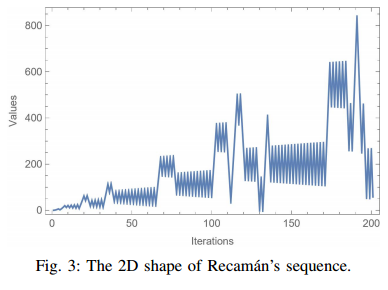
其中a、b和c是非负参数。这一众所周知的系统通过倍周期分岔路径的原理逼近达到混沌效果。在本文所提出的加密方案中，采用的参数值为a=0.1、b=0.01和c=14，如图1所示。依次于坐标系中列出计算出的x、y和z值构成的三维坐标，并将其与迭代次数进行比较，得出Rossler吸引子点集的图，如图2所示。





B、 S盒

替换盒是现代分组密码的关键组成部分，有助于为指定的明文生成混乱的密文。通过合并S-box的方法，算法建立了输入和输出数据之间的非线性映射，借此过程产生混淆[28]。数据的安全与否依赖于替换过程是否安全。替换是一种执行位混淆的非线性变换。它为密码系统提供了香农[29]所描述的混淆性质。

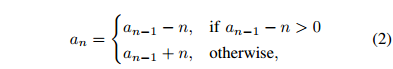


通常，S盒接受m个输入位并将其转换为n个输出位。这被称为mnS-box，通常以查找表的形式实现。这些S盒经过精心挑选以抵抗和防止线性和差分密码分析。通过合并S盒，建立了输入和输出数据之间的非线性映射，以产生混淆[30]，[31]。

对于所提出的加密方案，我们使用Wolfram Mathematica®随机生成一个16×16维的S盒。表四显示了其值。

C、 Recaman序列

为了生成Recaman序列，可以让a1＝1并遵循（2）中所示的数学表达式来生成其元素an。



其中n是元素在序列中的位置。这提供了前几个元素，如1、3、6、2、7、13、20、12、21、11、22、10、23、9, ...

图3是我们提出的加密方案中用于生成随机比特密钥的前200次迭代的2D图形表示。

D、 图像加密和解密过程

所提出的图像加密方案实现如下。

首先，选择适当尺寸的图像，然后将图像的像素转换为一维字节流。最后，这些字节被转换成比特流d。

其次，计算图像像素的平均强度。结果值是一个相当小的数字，我们将其乘以放大因子fM。乘法的结果值用µ表示。

接下来，我们将d循环右移µ位，生成的比特流（现在表示为dµ）然后与kCA进行异或运算。kCA是第一个密钥，一个与d和dµ长度相同的比特流，由R–ossler吸引子中前250个Rossler数的二进制表示所产生的第一个NCA比特的重复组成。让我们将生成的比特流表示为C1。这结束了加密的第一步。

接下来，随机生成的S-Box用于如表IV所示从第一步骤之后获取的比特流中替换每8位的十进制表示，为了满足此条件，使用了Wolfram Mathematica®的RandomSample函数。接下来，我们将这些得到的十进制表示更改为位流C2。此时，我们获取Recaman序列方程中每个点的x和y坐标，并将其展平为单个1D阵列。接下来，我们将这些值绘制成2D，如图3所示。

检查图3中的图表，我们将这些整数值更改为位表示。这个新获得的长度为NL的比特流将构成我们Recaman基于序列的密钥的种子。我们重复这些NL位，直到它们与d和C1的长度相同，从而形成第二个密钥。让我们将其表示为kL。

接下来，我们将kL与C2进行异或，得到C3。这就是加密的第三步。

最后，C3被重新整形为与普通图像相同尺寸的图像，从而获得加密图像。

解密过程以与加密过程相反的方式实现。

1. 数值结果和性能评估

本节概述了所提出的图像加密方案的指标和性能评估，并与文献中发现的对应算法进行比较。所提出的评估方案是在运行Windows 10 Enterprise的计算机上使用计算机代数系统Wolfram Mathematica®测试实现的。PC在配置方面使用了2.3 GHz 8核Intel®CoreTM i7处理器和32 GB 2400 MHz DDR4内存。所使用的密钥分配了以下值：NCA=250、NL=200和fM=106。本节使用了图像处理应用/实验中常用的四幅图像。

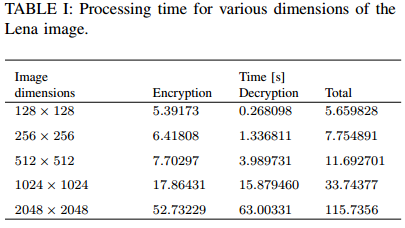
这些是Lena、Mandrill、Peppers和House，尺寸均为256×256。

表II所示的图形表示是表示样本图像的像素分布特征的直方图。可以观察到，普通图像（加密之前）和解密获得图像的像素在直方图上不均匀分布。加密图像的直方图像素分布则不同，该直方图像素分布与直方图一起显示出相当均匀的分布图案。此处注意到，与对非均匀分布的原始图像进行的统计分析相比，统计分析、破坏尝试和攻击不会产生任何密码分析结果。因此，这一观察结果表明，无法从加密图像的任何特征中区分或确定任何信息。

图4显示了普通和加密Lena图像的相关系数图。可以清楚地看到，普通图像的相邻像素的水平、垂直和对角线相关系数是线性的。然而，在检查加密图像生成的关系数图时，图中数据是均匀的，并且以散点状分布。这意味着拟议方案对统计分析或攻击的抵抗力。

使用时间大小复杂度度量来评估所提出的图像加密方案的效率，以便识别该方案是否适合实时应用。表I显示了加密、解密所需的处理时间，以及某些不同标准化正方形图像维度（例如{128，256，512，1024，2048}）所需时间的总和。此外，表I显示，对于128×128的图像尺寸，小于1秒的解密时间足以成功解密图像。反过来，这意味着所提出的图像加密方案适用于移动设备之间的实时图像交换。这对于设备上的图像处理期间消耗的功率具有更好的资源管理和优化。此外，表I显示了加密-解密过程所需的时间随着图像尺寸的增加而增加。这种行为以一定的速率表现出来，该速率于超过1024×1024图像尺寸时开始收敛到较慢的速率。

表III列出了我们提出的方案的MSE和PSNR的计算值，以及文献中2个对应方案的计算值（特别是[32]和[33]）。MSE值越大表示安全级别越高。我们提出的方案被证明优于[33]的MSE值，但其性能低于[32]中的性能。由于作为度量的PSNR与MSE成反比，因此这三种方案在PSNR方面的比较仍然具有与前述相同的意义。

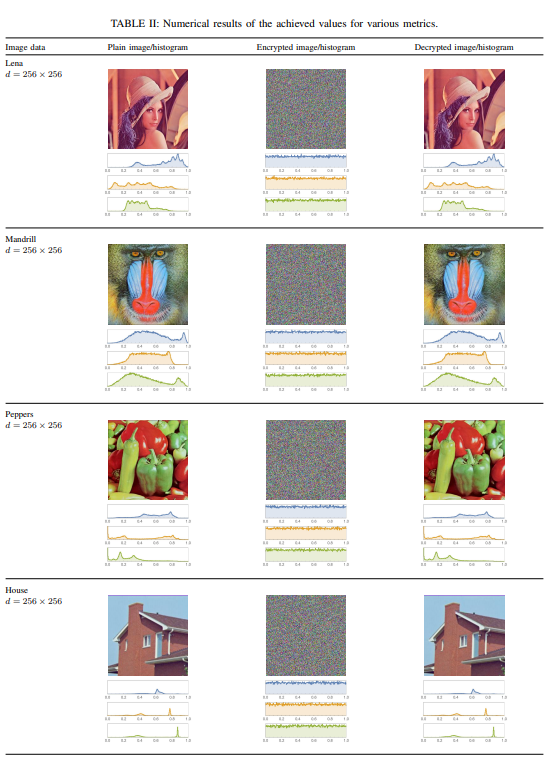


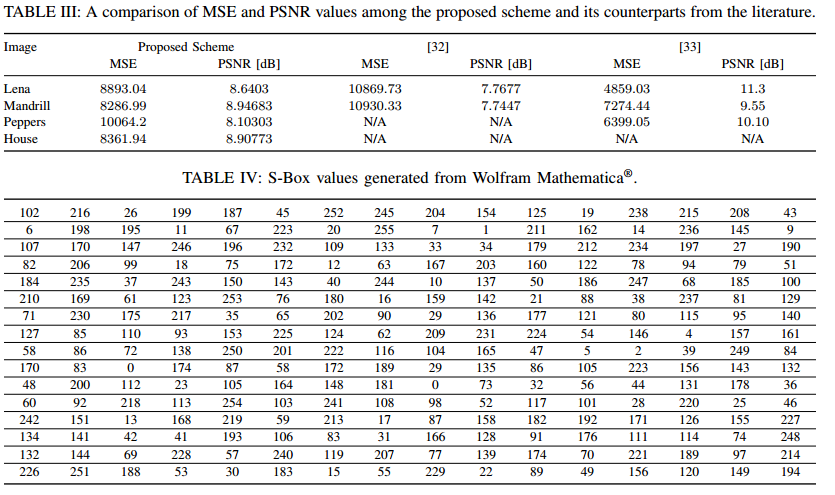
信息熵用于测量加密图像的灰度像素值分布的随机性。理论上，随机加密图像的熵值是8，因为灰度图像每个像素具有256个可能的取值，像素的数据具有2的8次方可能的组合。表V中显示了各种加密图像的熵值。可以看出，每个值略高于7.999，这表明所提出的加密方案随机化了普通图像的像素分布，使得攻击者不可能获得关于普通图像的任何信息。此外，表V提供了所获得的信息熵值与文献[32]–[34]中对应方案所获得的值之间的比较。

国家标准与技术研究所(NIST)提供的测试方法，可以检验某个PRNG的随机性程度。一个好的PRNG应该通过一系列包含NIST分析套件的测试来满足其随机性标准。具体地说，对于任何被视为随机的比特流，每个测试的概率或p值都应该大于0.1。表VI显示了在加密的Lena图像上运行的NIST分析结果。很明显，所有测试的值都大于0.1，假设我们提出的图像加密方案成功地通过了NIST分析。

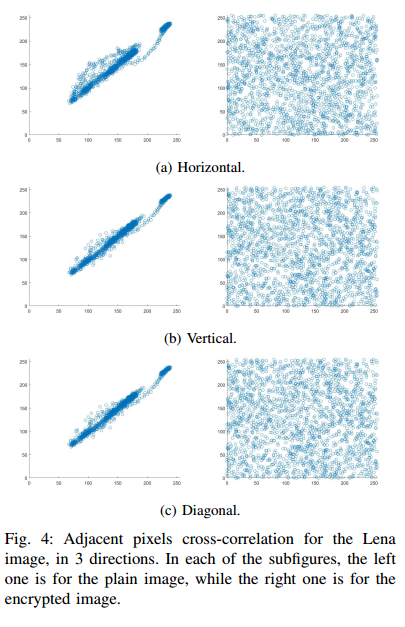
四、结论与未来工作

本文提出了一种基于3个步骤的图像加密方案。第一步骤使用Rossler系统，第二步骤使用PRNG S-Box，最后步骤使用Recaman的序列。算法构建完毕后使用了一些适当的指标和分析对本方案进行了绩效评估。其中包括对普通图像和加密图像的目视检查、直方图分析、互相关分析、熵值、MSE和PSNR值分析。与文献中相应的方案进行了比较，所提出的方案显示了相当的安全性能。





最后，对处理时间进行了计算记录，结果显示处理时间为较低水准，表现出了所提出方案在移动设别之间进行安全图像交换的适用性。将来，可以着手于构建一个更安全的S-box，而不是依赖通过Wolfram Mathematica®生成的PRNG S-box。



*参考文献*

本文共参考33篇文献，此处略去