附件 2

江苏省高等学校
大学生创新创业训练计划项目申报表
（创新训练项目）

推 荐 学 校：	（盖章）
项 目 名 称：	基于新型分段线性函数实现的多翅膀混沌流调控及其在图像加密中的应用
推荐项目级别：	□ 国家级 ✓ 省级
所属一级学科名称：	工学
所属重点领域：	
项目负责人：	姜子怡
联 系 电 话：	13280907830
指 导 教 师：	李春彪
联 系 电 话：	13912993098
申 报 日 期：	2024.4

江苏省教育厅 制

二〇二四年三月

填 表 说 明

一、申报表要按照要求逐项认真填写，填写内容必须实事求是表述准确严谨。空缺项要填“无”。

二、格式要求：表格中的字体采用小四号宋体，单倍行距；需签字部分由相关人员以黑色钢笔或签字笔签名。

三、项目推荐类型为国家级项目、省级项目等。

四、项目来源：1. “A”为学生自主选题，来源于自己对课题的长期积累与兴趣；“B”为学生来源于教师科研项目选题；“C”为学生承担社会、企业委托项目选题。2. “B”和“C”需填写“来源项目名称”和“来源项目类别”栏；“来源项目类别”栏填写“863 项目”、“973 项目”、“国家自然科学基金项目”、“省级自然科学基金项目”、“教师横向科研项目”、“企业委托项目”、“社会委托项目”以及其他项目标识。

五、所属重点领域：**国家级项目选填**，如果属于重点领域的则填报。具体包括 10 类：泛终端芯片及操作系统应用开发；云计算人、工智能和无人驾驶；新材料及制造技术；新能源与储能技术；生物技术与生物育种；绿色环保与固废资源化；新一代通信技术、千兆光网技术和新一代 IP 网络通信技术；生物医学工程与精准医学、脑科学和类脑计算；城乡治理与乡村振兴；社会事业与文化传承。

六、表格栏高不够可增加。

七、填报者须注意页面的排版。

<table>
<tr><td colspan="2">项目名称</td><td colspan="7">基于新型分段线性函数实现的多翅膀混沌流调控及其在图像加密中的应用</td></tr>
<tr><td colspan="2">项目所属
一级学科</td><td colspan="3">工学</td><td>项目所属
二级学科</td><td colspan="2">电子信息类</td></tr>
<tr><td colspan="2">所属重点领域</td><td colspan="6">（国家级项目选填）</td></tr>
<tr><td colspan="2" rowspan="2">项目来源</td><td>A</td><td>B</td><td>C</td><td colspan="2">来源项目名称</td><td>来源项目类别</td></tr>
<tr><td></td><td>✓</td><td></td><td colspan="2">忆阻神经元的非分岔振荡调控与多吸引子动力学编辑</td><td>国家自然科学基金面上项目</td></tr>
<tr><td colspan="2">项目实施时间</td><td colspan="6">起始时间： 2024 年 4 月 完成时间： 2025 年 4 月</td></tr>
<tr><td colspan="2">项
目
简
介
(限 200 字)</td><td colspan="6">该项目的主要目标是通过研究基于新型分段线性函数实现的多翅膀混沌流调控及其在图像加密中的应用，通过数字化模拟实现高可靠、高稳定性加密通信。为此，该项目将基于非线性动力学的基本理论，利用科学计算工具进行分析和计算，以研究和开发一个新的混沌加密系统。该项目旨在提供低成本、高可靠的保密通信模块，以降低在数据传输过程中的安全风险。</td></tr>
<tr><td rowspan="7">申请人或申请团队</td><td></td><td>姓名</td><td>年级</td><td>学号</td><td>所在院系/专业</td><td>联系电话</td><td colspan="2">QQ 邮箱</td></tr>
<tr><td>主持人</td><td>姜子怡</td><td>2022</td><td>2022833
20022</td><td>长望学院</td><td>13280907830</td><td colspan="2">3097733614@qq.com</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td rowspan="4">成员</td><td>高佳丽</td><td>2022</td><td>2022833
20119</td><td>长望学院</td><td>18260592180</td><td colspan="2">2936708764@qq.com</td></tr>
<tr><td>胡锦秀</td><td>2022</td><td>2022833
10056</td><td>长望学院</td><td>13611081052</td><td colspan="2">3069315419@qq.com</td></tr>
<tr><td>周栩佳</td><td>2022</td><td>2022833
30014</td><td>长望学院</td><td>18861598368</td><td colspan="2">256155763@qq.com</td></tr>
<tr><td>毛颖</td><td>2022</td><td>2022833
20059</td><td>长望学院</td><td>13915965121</td><td colspan="2">2156280256@qq.com</td></tr>
<tr><td rowspan="4">指导教师</td><td rowspan="2">第一指导教师</td><td>姓名</td><td colspan="2">李春彪</td><td>单位</td><td colspan="2">南京信息工程大学人工智能学院</td></tr>
<tr><td>年龄</td><td colspan="2">53</td><td>专业技术职务</td><td colspan="2">教授</td></tr>
<tr><td colspan="2">主要成果</td><td colspan="5">[2019]Li, C., Lu,T., Chen,G. and Xing, H. Doubling the coexisting attractors. Chaos, 29, 051102 (2019);doi: 10.1063/1.5097998
[2019]Li, C., Xu, Y., Chen, G., Liu Y., Zheng J. Conditional symmetry: bond for attractor growing. Nonlinear Dyn (2019). 95, 1245-1256</td></tr>
<tr><td>第二指</td><td>姓名</td><td colspan="2"></td><td>单位</td><td colspan="2"></td></tr>
</table>

	导教师	年龄		专业技术职务	
	主要成果				

一、申请理由（包括自身具备的知识条件、自己的特长、兴趣、已有的实践创新成果等）

负责人：姜子怡

已系统学习模电、数电等相关知识，并绘制拼接成功收音机等设备，较为了解 Matlab 、 pyCharm 、 LTspice、FPGA 等软件的使用方法与编程原理，对于器件组成以及电路设计感兴趣。

成员：高佳丽

已学过电路分析基础、工程制图、模拟电子技术和数字电子技术的基础专业课，目前还在学习各种硬件语言。对于电路设计和搭建比较感兴趣。

成员：胡锦秀

系统地学习了多项电子类专业课程，包括电路分析、模电、数电等。通过相关的练习和实验，我掌握了电路元件的特性、电路分析、设计与计算方法。我能够熟练运用 multisim、quartus 等软件进行电路绘制和仿真。学习 C 语言，有一定的创新思维，有团队意识和一起解决问题的能力。

成员：周栩佳

曾获得江苏省高数竞赛三等奖，参加过数模培训并自学了 matlab，有一定的编程基础。对混沌电路有一定的了解并有极大的兴趣，目前已经掌握 multisim，能够对混沌电路进行仿真实验，并且愿意钻研，责任心强，擅长各类图表制作。

成员：毛颖

在 FPGA 和单片机方面有较为深入的专业知识和研究经验。接受过相关的电赛培训课程和高数培训，参加过高数竞赛并取得国奖成绩。具备较强的实验技能和数据分析能力，可独立开展研究工作并承担项目管理任务。同时，具有团队合作精神和较强的沟通表达能力，能够有效与组内成员、导师和合作单位进行协作和交流。

二、项目方案

1、项目研究背景

（1）国内外的研究现状及研究意义

混沌（chaos）是指确定性动力学系统因对初值敏感而表现出的不可预测的、类似随机性的运动，又称为浑沌。运动的可预测性是一种物理概念，即使一个运动是确定性的，但是仍为不可预测的。20 世纪 70 年代后的大量研究表明，大量非线性动力学系统中尽管系统是确定性的，却普遍存在着对运动状态初始值极为敏感、貌似随机的不可预测的运动状态，即为我们小组所研究的主体对象——混沌运动，在统计特性上类似于随机过程，被认为是确定性系统中的一种内禀随机性。混沌系统所对应的系统方程，简化了系统，但是将运动形式复杂化，起始值的细微变化，会使得轨道全然改观，将数值计算在三维空间中绘制出来，会呈现出一条在三维空间的一条看似无序的光滑曲线。系统轨道的同一归宿，则形成所谓的奇异吸引子，在其上，任取两个接近的数值为初始值，对应运动轨迹以指数形式迅速分离，表现为敏感性。

混沌密码学是混沌理论中的一个重要应用领域，依据混沌的基本特性，即随机性、遍历性、确定性和对初始条件的敏感性，将混淆（confhainn）和扩散（diffusion）联系在一起，形成了混沌密码学。混沌是由非线性系统所产生的复杂的动力学行为，由于其对初值条件具有极端的敏感性，因此可以产生大量的、不相关的、具有伪随机性的混沌序列，将这些作为密钥序列，利用该序列对所需要加密的对象进行加密，加密后的内容经信道传输，接收方设定相同系统参数和初始条件、基于非线性系统的方程和参数对混沌进行重构，因此实现同步和解密过程。而目前混沌加密技术还存在的缺点是：每个实现序列的周期长度不确定，保密性不足；有限精度的限制；实现精度和保密性的矛盾，有人专门对混沌进行破译。因此，我们还需要继续学习和研究，争取早日解决这些问题。

混沌现象的发现和混沌理论的建立，是对牛顿确定性经典理论的重大突破，目前已经对混沌系统有了较为系统且全面的认识。混沌密码学于 1989 年英国学者 Robert A.J.Matthews 首次明确提出并获得广泛关注，给出了一种基于变形 Logistic 映射的混沌序列密码方案，在密码学领域掀起了一阵关于混沌密码学的热潮而后沉寂。1997 年以后，混沌系统又开始了新一轮的研究热潮，最近十年也有了相关综述性文献。针对混沌加密方法的研究，我们新一代青年应该努力进取，对该方向进行深入学习，提高混沌加密的保密性，可以为我国信息安全做出一定的帮助。

（2）研究积累与已取得的成绩

① 项目已有的基础与研究积累

项目申请人所在小组从事非线性电路与系统及其应用研究，研究内容涉及混沌动力学理论、混沌电路（包含模拟电路以及基于 ARM、FPGA 和 FPAA 等技术的电路实现）、忆阻混沌电路、隐藏混沌振荡、多稳态理论、混沌同步技术等，并进一步延伸到混沌吸引子与排斥子、混沌雷达和混沌保密通信等混沌信号处理领域。

②参与成员已有的基础与研究积累

小组成员在高数竞赛上取得优异成绩,都初步了解了混沌电路产生的原理以及相关软件的应用，例如 Matlab 、 pyCharm 、 LTspice、单片机等，对于产生混沌电路的方程以及电路连接具有一定的基础，小组成员均已掌握基础电路分析相关的知识，能够运用模拟电路、数字电路等相关知识解析电路，能够熟练运用 Multisim 等软件模拟电路，对 C 语言具有一定基础。

（3）已具备的条件

① 研究小组情况

申请人所在小组导师长期进行非线性理论基础和电路实现研究，对混沌系统的幅度、偏置与频率开展调控，多稳态，隐藏振荡等不同复杂振荡行为有深入理解，是 IEEE Transactions on Circuits and Systems，Physics Letter A， Nonlinear Dynamics，International Journal of Bifurcation and Chaos， Chinese Physics 等期刊审稿人，IJBC 期刊编委，中国密码学会混沌保密通信专业委员会委员，中国电子学会电路与系统分会混沌与非线性电路专业委员会副主任委员，全国材料与器件科学家智库电子信息材料与器件专家委员会委员，中国密码学会物联网密码专委会委员。主持并参与国家自然基金、省自然基金、省高校基金、省“333 人才”项目、国家博士后面上基金和特别资助等项目 10 余项，发表核心及 SCI 论文百余篇。系统性地展开忆阻混沌信息系统的调幅、调频、调偏置研究和动力学系统的多稳态分布调控研究，以第一作者发表 Top 1% ESI 数据库高被引论文（HCP）和热点论文共十余篇，获国内授权发明和实用新型专利二十多项。获 2023 年度江苏省工程师学会科学技术奖提名奖，获 2022 年度江苏省通信学会科学技术奖一等奖，2022 年度江苏省科技咨询协会科学技术奖二等奖，第八届“春晖杯”创新创业大赛优胜奖，2018 年江苏省教育教学与研究成果奖（研究类）三等奖，获得国家教学成果奖二等奖一项，江苏省教学成果奖一等奖一项和全国高校电子信息类专业课程实验教学案例设计竞赛二等奖一项。

本小组国际交流频繁，与（意大利）Ludovico Minati（电子科技大学），（瑞士）Tomasz Kapitaniak，（伊朗）Sajad Jafari 等多位海外优秀学者合作。我们在混沌和非线性动力学领域的前沿研究中扮演着重要角色，通过与海外专家的交流合作，我们不仅深入研究混沌通信系统的设计和安全性分析，还拓展了研究领域，涵盖了机械系统稳定性、磁计算、系统网络优化等方面。我们的团队成员不仅是优秀的研究者，更是国际间的桥梁和连接器，将不同地域、不同文化背景下的智慧和创新融合在一起。这种多元化的合作不仅丰富了我们的研究项目，也促进了我们对混沌和非线性动力学应用的深刻理解，从而推动了该领域的发展。

②设备情况

申请人所在单位南京信息工程大学电子与信息工程学院拥有电工电子实验室、高频与通信原理实验室、电子工艺实验室、数字信号处理实验室、嵌入式系统设计实验室、综合电子系统设计开放实验室、电子系统仿真开放实验室、集成电路试验室和传感器实验室等。实验室中配备了计算机、TDS 数字存储示波器、Agilent 频谱分析仪、Agilent 逻辑分析仪、多功能函数信号发生器、矢量信号发生器、电路板在线分析仪以及各种仿真软件等，本项目组拥有 FPGA，ARM 等科研相关的实验开发板以及深度学习 GPU，这些设施的存在为项目的开展实施提供了强有力的保障。

（4）尚缺少的条件及方法

① 实现多翅膀混沌映射所需的分段电路，将会通过数字模拟探索出合适的电路实现方法。

② 具有复杂动力学行为的混沌映射以及基于此加密的具体方法，这也是本项目的加密处理的关键方法。

2、项目研究目标及主要内容

项目的研究内容主要包括通过分段线性方程的构造与分析以及通过分段线性实现多翅膀混沌在通信信息加密中的应用。本项目在前期研究的基础上，从混沌电路的基础出发，通过系统模拟与分析，借助 Multisim 模拟平台研究电路的持续反馈对混沌涡卷的影响，进而产生具体分段电路，实现电路突破。以神经元系统以及 VB5 系统为载体，将分段电路转化为多翅膀混沌，观察其演变过程及现象。

具体而言，研究目标包括以下三个方面：

（1）分段线路的建立：通过合理的数学模型及模拟电路，构建一个能够产生多翅膀混沌的分段电路。对其进行实际的实验模拟，评估其输出序列的随机性与不可预测性。

（2） 多翅膀混沌的模拟与处理：以神经元系统以及 VB5 系统为载体，对线性方程进行加工处理，并将其与已有研究进行比较，分析多翅膀混沌的创新点。

（3）基于多翅膀混沌的加密算法研究：对多翅膀混沌产生的随机序列进行处理，探究加密算法，使所得结果能够实现对通信信息的加密处理。

3、项目创新特色概述

（1）引入分段电路模型的混沌系统设计：本项目通过特有的分段电路非线性反馈提供多翅膀混沌映射自身的复杂度，从而输出具有不同极性与幅值的超混沌序列。本项目还将着力于建立一套系统化的混沌映射理论框架，为其在混沌加密领域中的应用提供理论支持和指导。

（2）基于多翅膀混沌系统的加密方式：本项目通过对分段函数的非线性函数构造的混沌序列进行特殊数据处理，进而通过 NIST 测试检验加密序列的强随机性，最终将随机序列用于数据加密，实现信息的机密性、完整性等安全性要求。

（3）低成本、高稳定性、高加密性的通讯设备设计：分段电路设计时尽量减少元器件的使用，多翅膀涡卷具有更强的稳定性，也更加具有低成本的特点。从混沌系统产生涡卷数量多少来看，多翅膀混沌系统产生的涡卷数量多，具有更多的涡卷密钥参数，具有更复杂的混沌动力学行为，能够实现高加密性通讯设备要求。

4、项目研究技术路线

（1）多翅膀混沌映射的建模与分析

多涡卷混沌系统的建模关键在于找到合适的非线性函数，一些具有奇对称性的非线性函数能够产生多涡卷吸引子，这些具有奇对称性的非线性函数主要包括分段函数、三角波、锯齿波、三角函数、指数函数、符号函数等，基于连续混沌系统离散化和数字化处理技术实现混沌算法，将实验结果与仿真结果相对比，调整出非线性混沌映射在保密通信中的应用。实验方案流程图如图 1 所示，实验方案原理如图 2 所示。

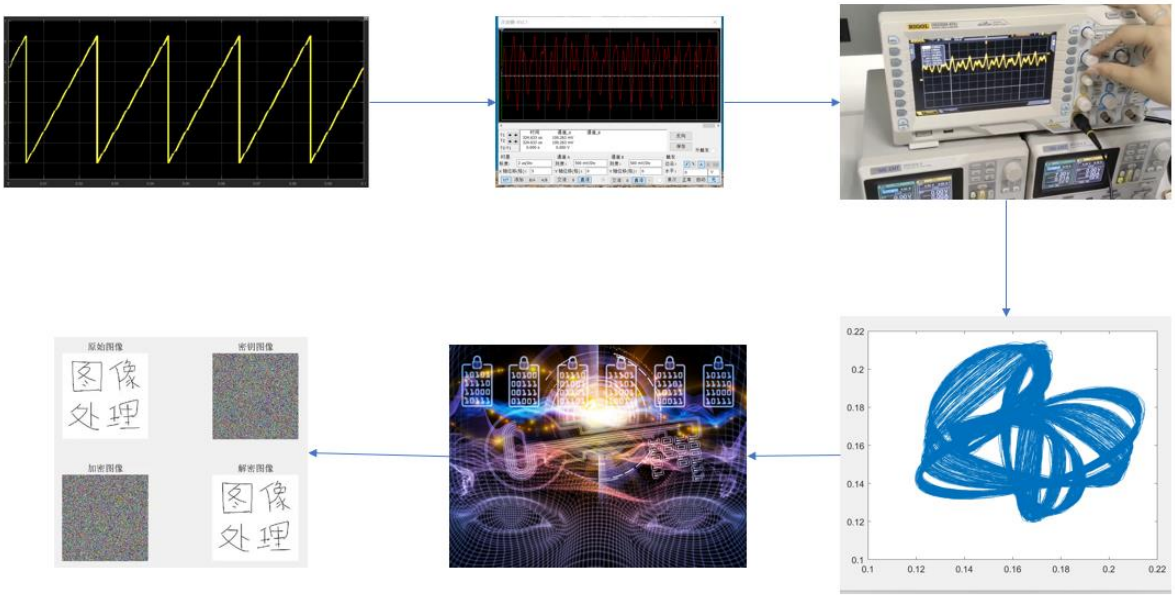

图 1 实验方案流程图

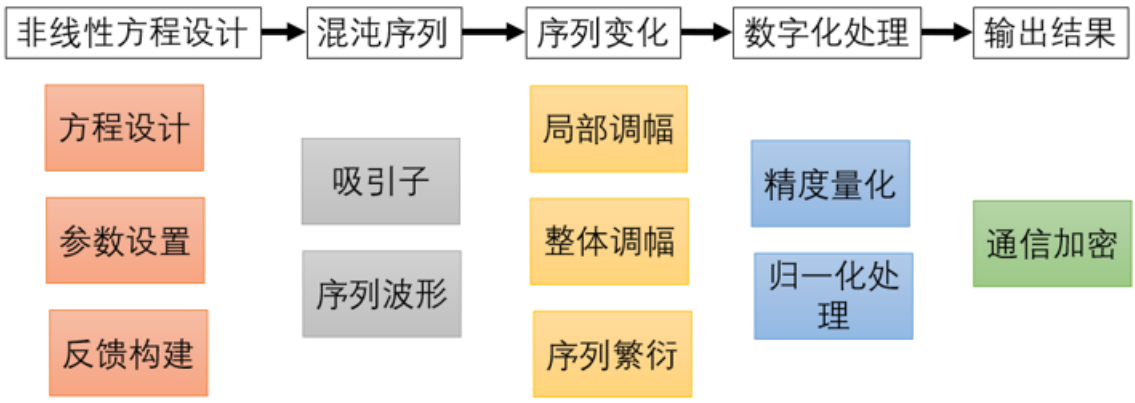

图 2 实验方案原理

（2）伪随机数生成及加密

通过非线性离散混沌映射，得到的混沌序列，设为$X=\{x_1,\ x_2,\ldots,x_n\}$，通过如下的函数取模得到随机 0-1 序列

$$P_i=(X_i+|X_{min}|.K)modN \tag{3}$$

其中 K 为正整数，X_{min} 为 X 的最小值，mod 表示将括号内的数据取模转变成不大于 N 的 最小整数。我们选择 k 为 10 的 7 次方，N 为 256，得到的 P_i 序列即为随机 0-1 序列。

对离散混沌映射输出序列进行取余处理得到随机 0-1 序列后，将序列与文件序列进行异或加密，以图片文件为例：对于图片文件的加密过程，首先使用 Arnold 变换对图像进行置乱操作，然后将置乱后的二维数组转换为一维数组。接着，将获取的随机 0-1 序列与该一维数组进行异或加密，从而得到加密后的密文。解密为类似的相反过程，伪随机数的生成及加密流程如图 3 所示。

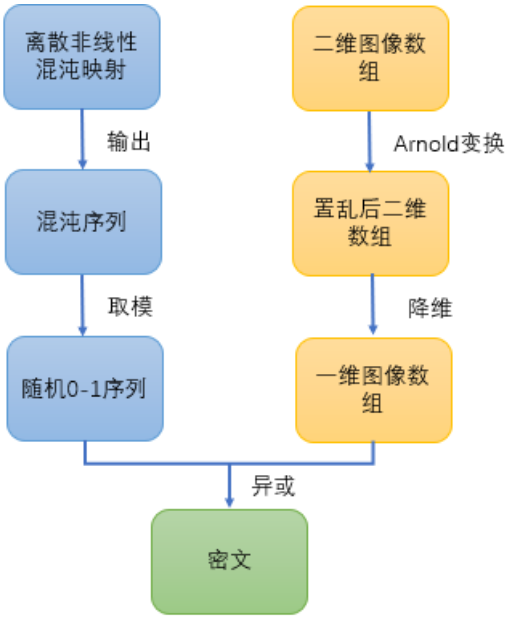

图 3 伪随机数生成及加密流程

（3）混沌加密算法在嵌入式设备上的部署

使用 C 语言对设计出的非线性系统离散混沌映射进行描述，在数字电路上进行映射计算，并根据图三所示的流程得到密文。将其操作到具体仪器设备当中进行验收，在发射端，通过无线串口进行密文的发送。在接收端，通过无线串口接收到密文并使用解密操作得到解密信息。保密通信流程如图 4 所示。

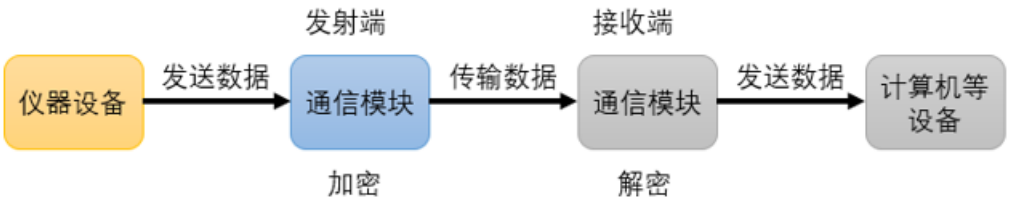

图 4 保密通信流程

5、研究进度安排

第一阶段：理论学习与成员分工　2024.4-2024.6

阅读相关文献，收集和整合资料，学习混沌动力学、混沌电路产生原理以及多翅膀混沌和通信信息加密的核心，为后续研究工作提供理论支撑。项目成员根据自己所负责的部分，熟练掌握 Mulitisim、matlab、python 等。

第二阶段：分段线路的建立与实验模拟　2024.6-2024.9

根据前期研究，设计合理的数学模型和模拟电路，构建能够产生多翅膀混沌的分段电路。利用 Multisim 模拟平台进行电路仿真，观察分段电路的混沌行为，并进行参数调整和优化。评估输出序列的随机性与不可预测性。撰写分段线路建立与实验模拟报告，记录实验数据和结果。

第三阶段：多翅膀混沌的模拟与处理　2024.9-2025.1

以神经元系统以及 VB5 系统为载体，将分段电路转化为多翅膀混沌，并进行模拟实验。对线性方程进行加工处理，分析多翅膀混沌的演变过程及现象。将多翅膀混沌的研究结果与已有研究进行比较，分析创新点和应用前景。撰写多翅膀混沌模拟与处理报告，总结研究成果和发现。

第四阶段：基于多翅膀混沌的加密算法研究与论文撰写　2025.1-2025.4

根据多翅膀混沌产生的随机序列，设计加密算法框架和流程。进行仿真测试，并对算法进行优化和改进，评估其加密效果和安全性。撰写加密算法研究报告，详细阐述算法原理、实现过程及实验结果。对整个项目进行总结，梳理研究成果，撰写相关软著专利。

6、项目组成员分工

• 姜子怡（负责人）

构建混沌加密的模型，负责在研究过程中的方向引导，对于所有仿真软件能熟练使用，与每一阶段的成员进行配合研究，将混沌与加密较好联结在一起。同时负责相关软著、专利的撰写。

• 高佳丽（小组成员）

负责研究三角波的形成原因和相应电路图，较为熟练的掌握 multisim、matlab 等仿真软件，对于电路和所形成的现象进行仿真研究；掌握论文的排版和撰写。

• 胡锦秀（小组成员）

负责研究由三角波形成相应复杂混沌系统的过程，使用 matlab、python 等进行仿真实验，得到相应的产生混沌的电路图和混沌相轨图；掌握论文的排版和撰写。

•周栩佳（小组成员）

负责研究基于已有的混沌电路图如何进行进一步加密操作，掌握对 matlab、python 的使用，实现将图像实现加密操作；掌握论文的排版和撰写。

•毛颖（小组成员）

负责相关实际电路的搭建和仿真，熟练使用函数发生器、示波器等实验室设备，对于 matlab、python 等软件也能熟练使用，配合各阶段成员进行电路搭建和相关软件使用。

三、学校提供条件（包括项目开展所需的实验实训情况、配套经费、相关扶持政策等）

（1）学校配置有专业实验室和实验器材，可以提供本项目组所需的硬件设施。

（2）学校图书馆拥有极其丰富的相关文献、书籍等资源，为本项目组提供了大量的可参考文献。指导老师指导成员研究，保障项目研究计划稳步开展。

（3）本研究团队配备有笔记本电脑，能够提供进行离散忆阻超混沌映射设计的平台以及 MCU 的集成开发环境。

四、预期成果

（1）第一、二阶段：2024.4-2024.9 起步阶段

构建一个能够产生多翅膀混沌的分段电路，完成参数评估和优化。

（2）第三阶段：2024.9-2025.1 实践阶段

成功将分段电路转化为多翅膀混沌，设计加密算法，并使其达到在保密通信中的指标。

（3）第四阶段： 2025.1-2025.4 结项阶段

实现保密通信的功能，申请软著一篇或专利一篇，发表核心期刊论文。

（4）预期最终成果

① 设计一个能够产生多翅膀混沌的分段电路。

② 拟撰写一篇基于多翅膀混沌和通信信息加密方法的论文，并撰写相关软著和专利。

五、经费预算

总经费（元）	**6000**	**财政拨款/企业资助（元）**	**0**	**学校拨款（元）**	**6000**

注：总经费、财政拨款、学校拨款按照规定金额填写。

具体包括：

1、购置项目研发的元器件、软硬件测试、小型硬件，预计经费 3000 元；

2、资料购置、打印、复印、印刷、文献检索等费用，预计 1000 元；

3、撰写与项目有关的论文版面费、申请专利费等，预计 2000。

六、导师推荐意见

同意推荐。

签名：李春彪

2024 年　6 月　　4 日

七、院系推荐意见

该项目研究目标明确，研究思路清晰，研究方案可行，人员结构合理，是一个较好的培养大学生创新能力的训练项目。

指导教师科研能力较强、指导经验丰富，能够指导学生团队顺利完成项目。

同意推荐申报。

院系负责人签名：吉琨　　学院盖章：

2024 年　6 月　　4 日

八、学校推荐意见：

同意推荐申报，学校将提供经费及各方面支持！

学校负责人签名：　　学校公章

2024 年　　6 月　　4 日