基于无人机 MAVLink 协议遥测类消息的隐蔽通信方法

黄冬艳[1,2]，黄珉[1,2]
（1. 桂林电子科技大学信息与通信学院,广西 桂林 541000；2. 认知无线电与信息处理省部共建教育部重点实验室,广西 桂林 541000）

摘要：针对无人机在受监管环境中隐蔽通信的需求，本文提出了一种基于微型飞行器链路（Micro Air Vehicle Link，MAVLink）协议遥测类消息的隐写方案。该方案在不修改协议标准的前提下，利用浮点数尾数的最低 2 个二进制位嵌入信息，在常规遥测数据流中实现密文的可靠传输。考虑到 ATTITUDE、ATTITUDE_QUATERNION 与 HIGHRES_IMU 这三类消息具有持续高频更新、低扰动以及浮点字段天然容错的特点，本文选择它们作为核心载体，并设计了一种物理约束保持的预测-修正嵌入算法，在无人机动力学模型的引导下实时求解最佳嵌入位置。仿真实验证明，在静态悬停场景下平均容量达 1.38 kbit/s，为理论容量的 96.5%；在动态机动场景下容量仍可维持在 0.95 kbit/s 左右，能够满足大多数隐蔽通信任务的实时性要求。

关键词：无人机协议；隐蔽通信；物理约束；LSB 隐写；预测-修正嵌入算法
中图分类号：TP393.0
文献标志码：A
doi：10.11959/j.issn.1000–436x

Covert Communication Method for UAVs Based on Telemetry-Type Messages of the MAVLink Protocol

Huang Dongyan[1,2], Huang Min[1,2]
1. School of Information and Communication Technology, Guilin University of Electronic Technology, Guilin 541000, China
2. Ministry of Education Key Lab. of Cognitive Radio and Information Processing, Guilin 541000, China

Abstract: To address the demand for covert communication of unmanned aerial vehicles (UAVs) in regulated environments, this paper proposes a steganographic scheme based on Micro Air Vehicle Link (MAVLink) telemetry messages. Without modifying the protocol standard, the scheme embeds information into the least two significant bits of the mantissa of floating-point numbers, enabling reliable transmission of ciphertext within conventional telemetry data streams. Considering that ATTITUDE, ATTITUDE_QUATERNION, and HIGHRES_IMU messages feature continuous high-frequency updates, low perturbation, and inherent error tolerance of floating-point fields, we select them as the core carriers and design a prediction–correction embedding algorithm with physical constraint preservation. Guided by a UAV dynamics model, the algorithm solves for optimal embedding positions in real time. Simulation results demonstrate that the scheme achieves an average capacity of 1.38 kbit/s in a static hovering scenario, corresponding to 96.5% of the theoretical capacity; in a dynamic maneuvering scenario, the capacity remains around 0.95 kbit/s, which can meet the real-time requirements of most covert communication tasks.

Key words: UAV protocol, covert communication, physical constraints, LSB steganography, prediction-correction embedding algorithm

收稿日期：XXXX–XX–XX；修回日期：XXXX–XX–XX
通信作者：黄冬艳，huangdongyan-gua@163.com
基金项目：广西自然科学基金面上项目（2025GXNSFAA069685）
Foundation Items：Guangxi Natural Science Foundation General Project (Grant 2025GXNSFAA069685).

1 引言

1.1 研究背景与意义

无人机凭借其高效性与灵活性，可替代人类执行困难或危险的任务，极大拓展了作业能力边界。随着无人机应用场景的不断拓展，其面临的安全挑战也日益严峻。一方面，通信链路易遭受窃听或干扰，可能导致任务失败；另一方面，在受监管环境等特定应用场景下，无人机之间或无人机与地面节点之间存在建立隐蔽通信信道的迫切需求。

以微小型无人机广泛采用的微型飞行器链路（Micro Air Vehicle Link，MAVLink）协议为例，该协议作为实现自主飞行与远程操控的关键基础，定义了无人机与地面站之间状态、控制与任务数据的交换格式。隐蔽通信的目标，是在公开合法的MAVLink数据流掩护下，以难以被第三方察觉的方式秘密传递信息。传统的加密通信虽然能保证内容的机密性，但其流量特征易暴露通信意图与身份。相比之下，隐蔽通信将秘密通信本身一并隐藏，可实现更高级别的操作安全。因此，在MAVLink协议中构建隐蔽通信信道，在保持飞行控制稳定与外部流量特征不变的前提下实现高容量、高隐蔽性的信息传输，不仅具有重要的理论价值，也在无人机安全应用、协同组网与特定任务支持等方面展现出广阔前景。

1.2 本文研究内容与主要贡献

本文提出一种面向MAVLink协议的容量稳定型隐写方案。该方案在不修改协议标准的前提下，利用协议字段末两位容错空间，实现隐蔽信息在常规遥测数据的嵌入与可靠传输。主要研究内容与贡献如下：

1)构建了基于消息载体的隐写评估框架，涵盖扰动性、容量潜力、检测风险与场景适配性四个维度。分析了HIGHRES_IMU（高分辨率惯性测量单元消息）、ATTITUDE（姿态消息）、ATTITUDE_QUATERNION（四元数姿态消息）三类高频遥测类消息作为隐写载体的优势，为方案奠定了安全可靠的基础。

2)提出了一套完整的隐蔽信息嵌入与提取算法。采用自适应最低有效位修改策略，提出约束满足嵌入空间的概念，将隐蔽信息的编码严格限制在同时满足所有物理与安全约束的可行解集合内。根据字段实时数值动态调整嵌入深度，确保物理量波动远低于飞控系统的噪声容限与异常检测阈值。设计了包含同步标识、帧序号、校验位的固定帧结构，并结合“粗-细”双阶段同步机制，保障了在连续数据流中的可靠帧定位与数据恢复。

3)针对不同飞行阶段对传感器数据波动特性，设计了基于字段安全触发概率的动态容量适配机制。通过加权轮询分配算法与数据缓存池，在波动环境中维持稳定有效带宽，并平滑输出流量，使统计特征与正常通信无异。

4)基于PX4飞控软件在环与Gazebo高保真仿真环境，实现了隐写方案的端到端仿真测试。设计了静态悬停、稳定平飞、动态机动三种典型飞行场景，从有效隐蔽容量、功能扰动度、协议兼容率、检测规避性四个维度对方案进行了定量验证。结果表明，该方案在保证飞行控制功能零干扰、协议100%兼容的前提下，可实现kbps级隐蔽带宽，并能有效抵抗基于流量统计与协议分析的常规检测。

2 国内外研究现状

无人机平台凭借其高机动性及独特的空地信道特性，近年来已成为隐蔽通信研究的前沿热点。围绕无人机辅助的隐蔽通信，国内外学者已开展了大量研究工作，从物理层传输、轨迹优化、资源分配等层面提供了丰富的理论框架与技术方案[1-12]。

无人机系统的通信高度依赖于具体的协议栈，其中MAVLink作为最广泛采用的无人机通信协议，其自身的安全性与隐蔽性同样值得深入探索。基于此，另一类研究聚焦于MAVLink协议本身，从协议安全增强与信息隐藏两个维度展开。在协议安全方向，现有工作致力于加固MAVLink以抵御外部攻击，在保护密钥，认证加密和MAVLink协议本身隐患排查等多个方面提供的多种高可行性的技术方案[13-17]。在信息隐藏方向，M Veksler等人[18]探讨了利用MAVLink协议在无人机通信中建立隐蔽通道以对抗泄露敏感信息的攻击。该论文设计了四种隐蔽通道，初步验证了在流量分布和熵检测下利用MAVLink协议可实现强隐蔽性的隐写。但该方案所选隐写载体既未考虑无人机动力学敏感量，欠缺物理一致性约束，又未定义量化安全边界，因此无法保证嵌入操作不会影响飞行安全。在抗检测方面，该方案的安全假设过于理想，仅假定检测方只具备流量分布和单字段熵等基础分析能力，却忽

视了协议行为异常、多特征联合统计等更强的检测模型；此外，该方案依赖字段独立拼接，缺乏帧同步与差错校验，在非理想信道下可靠性不足。

最低有效位（Least Significant Bit, LSB）隐写是信息隐藏领域中经典的空间域隐写方法之一，其核心思想是利用数字媒体中存在的感知冗余，通过替换载体数据的最低若干比特位来嵌入秘密信息。目前，LSB隐写的研究集中于针对图像的算法研究，包括最优替换算法，动态嵌入算法和统计特性优化算法等多种方案[19-23]，针对有强约束性的协议字段的文献相对较少。将传统LSB隐写直接应用于MAVLink协议的遥测字段存在三方面局限。

1)物理一致性约束缺失。传统LSB隐写的样本之间相互独立，修改某一像素或采样点不会影响其他样本的语义。但MAVLink遥测字段之间存在严格的物理关联，例如三轴加速度的模长应与重力加速度和机体线加速度满足运动学关系。独立篡改某一字段的尾数可能破坏这种一致性。

2)控制回路扰动放大。地面站可能基于被修改的数据决策，嵌入操作引起的数值扰动可能被控制回路放大，违背功能安全原则。例如，对加速度计值的微小修改可能导致姿态解算的微小偏差，这一偏差经过PID积分放大后可能产生可观测的漂移。传统LSB未考虑此动态效应。

3)破坏四元数单位范数约束。独立修改四元数尾数会破坏单位范数约束，产生无效姿态，传统LSB缺乏对四元数几何结构的保持能力，无法将嵌入操作约束在可接受扰动范围内。

因此，MAVLink隐蔽通信不能照搬传统LSB隐写，需设计物理约束保持、安全优先且具自适应的新方案。本研究首次系统性地将网络隐写术理论与无人系统主流通信协议MAVLink深度结合，聚焦于多重约束条件下的信息隐藏模型与方法，提出了一套完整的基于MAVLink协议的信息隐写方案。该工作丰富了MAVLink协议隐写术的研究内容，可为后续攻防两端的技战术探索提供参考，并为构建更安全的无人系统通信体系提供一定的理论与技术支撑。

3　隐蔽通信方案设计

3.1　MAVLink协议中隐蔽通信载体选择

MAVLink协议由消息定义层、协议格式层和代码实现层构成。其中，消息定义层通过XML文件规定了所有消息类型，包括消息的唯一ID、名称，以及消息内部字段的类型、顺序和含义。每条消息类型对应唯一的ID，携带确定的语义和数据格式。MAVLink消息的循环校验（CRC）由字段的结构、顺序和类型唯一确定，因此标准消息一经发布便不可修改。依靠这些严格定义的消息类型，MAVLink在不同系统之间建立一套稳定且高度互操作的通信机制。目前，MAVLink协议有1.0和2.0两个主要版本，本文所有设计与实验均基于MAVLink 1.0协议。相较于2.0版本，1.0协议的报文头更短，无消息签名与扩展字段。但值得一提的是，其遥测类消息的结构在后续版本中保持了向后兼容，因此本文提出的浮点字段LSB隐写方法经适当适配后亦可推广至MAVLink 2.0环境。为简化阐述并聚焦于物理约束保持的核心机制，下文不再区分版本，默认采用1.0协议规范。MAVLink的主要消息类型和功能如表1所示。

本文的隐蔽通信系统主要建立在消息定义层。隐蔽通信旨在不被第三方察觉的前提下传输秘密数据，其载体选择需要满足以下四项准则：

1）低扰动性：字段修改不影响设备功能；

2）高容量潜力：消息更新频率高、可修改字段多，足以承载秘密数据；

3）低检测风险：消息属于高频正常流量，修改不改变帧结构，且避免触碰协议敏感字段；

4）场景适配性：消息使用场景符合隐蔽通信长期和稳定的需求，信息嵌入不引发流量特征异常。

基于上述四项准则，本文系统评估并筛选出适合作为隐蔽通信载体的MAVLink消息类型。如表2所示，MAVLink协议中，遥测类消息在多个维度上适配性最佳。

控制指令类消息存在高功能风险和低容量两类问题。首先，控制指令类消息字段修改易引发功能异常（如SET_MODE（设置模式消息）的custom_mode被篡改可能触发飞控模式误切换）；其次，控制指令类消息的可修改字段极少（如COMMAND_LONG（长命令消息）仅param1–param7），且修改字段需要与ACK回执匹配，任何改动都可能导致指令执行失败并产生异常日志。

任务类消息存在频率低、交互性强和字段敏感

表 1 MAVLink 的主要消息类型和功能

类别	典型消息（ID）	主要功能说明
1. 心跳与系统状态类	HEARTBEAT (0)、SYS_STATUS (1)、SYSTEM_TIME (2)、STATUSTEXT (253)	提供系统识别、状态上报与心跳广播功能。
2. 全局导航类	GPS_RAW_INT (24)、GPS_STATUS (25)、GLOBAL_POSITION_INT (33)、GLOBAL_POSITION_INT_COV (63)	提供 GPS 定位、速度及全局位置估计信息。
3. 姿态传感器类	HIGHRES_IMU (105)、ATTITUDE (30)、ATTITUDE_QUATERNION (31)	输出 IMU、磁力计及姿态角等传感器数据。
4. 本地位置类	LOCAL_POSITION_NED (32)、LOCAL_POSITION_NED_COV (64)、ODOMETRY (331)、	提供本地坐标系下的位置、速度及外部位姿信息。
5. 控制指令类	SET_MODE (11)、COMMAND_LONG (76)、COMMAND_INT (75)	发送飞行模式切换、动作控制等飞行指令。
6. 任务管理类	MISSION_ITEM (39)、MISSION_ITEM_INT (73)、MISSION_REQUEST (40)、	处理航点上传、计数与任务状态管理。
7. 文件参数传输类	PARAM_REQUEST_LIST (21)、PARAM_VALUE (22)、PARAM_SET (23)	读取与修改飞控系统参数。
8. 电源类	BATTERY_STATUS (147)、POWER_STATUS (125)	报告电池电压、电流及剩余容量等电源状态。

表 2 适配隐蔽通信系统的消息类型评估

消息类型	扰动性	容量潜力	检测风险	场景适配
控制指令类	高	低	高	不适配
任务类消息	高	低	高	可在更新频率低的场景下传输，容量小
文件传输类	高	高	高	一般不适配
系统基础类	高	低	高	不适配
遥测类消息	低	高	低	遥测类消息在无人机飞行全程持续传输，覆盖隐蔽通信长期稳定传输的需求

三类问题。首先，任务类消息属于按需发送（如航点任务仅发送对应次数的 MISSION_ITEM（任务项消息）），更新频率低；其次，若修改关键字段（如 seq、command）易引发任务执行失败；第三，任务类消息字段多为整型，若进行修改则数值变化直观。

文件传输类消息存在帧结构敏感和流量特征异常两类问题。其 data 字段为文件字节流，修改需严格保持长度与校验和匹配，若产生偏移或长度错误将导致传输中断；同时，该类消息呈现流量突发特征（如 LOG_DATA（日志数据消息）批量传输），与遥测类持续小流量差异明显。

系统基础类消息存在低频率且字段无修改空间两类问题。例如，HEARTBEAT（心跳消息）频率仅 1Hz，SYSTEM_TIME 频率仅 0.1Hz；其次，系统基础类消息可修改字段极少，如 system_status、autopilot 等枚举字段取值固定，修改后会导致地面站误判设备类型。

与上述消息字段类型形成鲜明对比，遥测类消息为飞控导航和地面监控提供实时物理状态，有低扰动性、字段物理意义适配、无功能关联性、持续高频更新等优势，天然符合对隐蔽通信的载体需求。具体而言，一定程度上修改字段不影响飞控功能，因此具有低扰动性；核心字段是物理状态的量化反馈，数值本身就存在微小波动，因此只要修改 LSB 引起的数值变化控制在传感器噪声范围内，可被飞控视为正常波动；遥测类消息仅为状态反馈，不触发设备操作，修改无功能风险；遥测类消息的更新频率远高于其他类型的消息，且在无人机飞行全程持续传输，因此满足隐蔽通信长期稳定的需求。

基于上述分析，本文最终选择 ATTITUDE、ATTITUDE_QUATERNION 与 HIGHRES_IMU 三类消息作为本方案的隐写载体。这三类消息同时具

备低扰动性、高容量潜力与场景适配性三大核心优势。理论分析与实验统计表明，通过对上述消息中特定浮点字段进行自适应 LSB 修改，在绝大多数飞行状态下，所引起的数值扰动远低于飞控系统设定的异常检测阈值，可被飞控系统的状态估计与控制系统视为传感器本底噪声。在容量方面，HIGHRES_IMU（200Hz）含 9 个可嵌入字段，单条消息最大贡献 3600 bit/s 物理带宽（9×200×2），占总隐蔽容量的 83.7%；ATTITUDE（50 Hz，3 字段）、ATTITUDE_QUATERNION（50 Hz，4 字段）最大补充 700 bit/s 物理带宽，三类消息合计物理上限达 4.3 kbit/s。经后续实验证明，即使在动态飞行场景中，本方案依旧能保持可观的容量。

4　物理约束保持的自适应隐蔽通信系统设计

4.1　威胁模型与检测者能力假设

为明确本方案在 MAVLink 协议环境下的隐蔽性目标，并使后续检测规避性实验具备可验证的理论基准，本节定义了检测者的能力模型与隐蔽性成功标准。模型假设检测者能够长期被动监听无人机与地面站之间的 MAVLink 通信链路，并即时获取完整的报文流。此时，检测者能获取以下三类信息：

首先是 MAVLink 的所有消息 ID、字段类型与顺序、CRC-16-CCITT（16 位循环冗余校验）校验算法结果以及消息的固定长度与可变长度规则；其次是任意飞行场景下所有字段的统计特性，包括数值范围、均值、方差和 LSB 的 0/1 分布熵值；第三是无人机的传感器噪声特性与无人机飞行异常日志。

由此，我们假设检测者可能采用以下四类典型检测手段。这些方法覆盖了从单字段统计到物理模型一致性的不同层次，能够较全面地评估本方案的抗检测能力。第一，单字段统计检测。检测者针对每个可嵌入字段，检测其浮点数尾数 LSB 序列是否偏离正常分布。这类检测旨在发现因 LSB 替换导致的 0/1 概率不均匀。第二，多字段联合统计检测。检测者可以分析同一消息中多个字段之间，或同一字段在时间窗口内的联合统计特性。本文使用 RS 分析、样本对分析和广义卡方检验作为代表。这些方法能够发现 LSB 替换引入的高阶统计异常，例如字段间的协方差结构改变。第三，协议行为异常检测。检测者可分析 MAVLink 的固定模式是否存在异常，例如 CRC 校验成功率是否为 100%；修改后的数值是否超出传感器手册规定的物理范围；消息发送频率是否存在突变等。第四，物理一致性检测。检测者利用无人机动力学模型检验传感器测量值是否与运动状态估计相符，包括检测四元数范数是否超出数值容限，传感器安全边界通过率是否为 100% 等。

4.2　系统设计原则与安全边界

4.2.1　安全优先的设计原则

无人机隐蔽通信面临隐蔽性、安全性与兼容性的三元悖论。飞行控制系统对数据完整性和实时性极为敏感，微小扰动可能被控制回路放大，引发不可预知的飞行风险。因此，本文采用安全优先的设计原则，遵循以下原则：第一，功能安全绝对性，即嵌入操作不干扰无人机的正常飞行控制；第二，物理约束严格性，即所有修改必须符合无人机动力学规律；第三，协议兼容性，确保修改后的消息能够通过 MAVLink 协议栈的完整性校验，包括 CRC 验证和签名验证；第四，统计隐蔽性，在满足前三项约束的前提下，最大化隐蔽通信容量和抗检测能力。

4.2.2　多维安全边界定义

传感器安全边界：根据 PX4 源码和传感器手册数据定义了三层递进的安全边界，确保系统的绝对安全性。对于任意可嵌入字段，其嵌入扰动 $\delta_i(t)$ 必须满足：

$$\left|\delta_i(t)\right| < \varepsilon_i = \min\left(\tau^i_{\mathrm{det}\,ect},\tau^i_{control},\tau^i_{stability}\right) \tag{1}$$

其中，ε_i 为系统安全边界阈值，$\tau^i_{\mathrm{det}\,ect}$ 为飞控系统对该字段的异常检测阈值；$\tau^i_{control}$ 为保证控制性能不下降的最大允许扰动；$\tau^i_{stability}$ 为保持控制系统稳定裕度的扰动上限。

物理一致性边界：嵌入后，传感器测量值应与无人机运动状态保持一致。设 $h(\cdot)$ 为系统观测模型，$x(t)$ 为状态估计值，物理一致性残差 $r(t)$ 需满足：

$$\left|r(t)\right| = \left|y_{embedded}(t) - h\left(x(t)\right)\right| < \beta \tag{2}$$

其中，β 为基于传感器噪声特性与状态估计精度确定的物理一致性阈值。

统计隐蔽边界：含密流量与正常流量在统计特

征上应不可区分。设$P_{embedded}$和P_{normal}分别为含密流量和正常流量的概率分布，其 Kullback-Leibler 散度需满足：

$$D_{KL}\left(P_{embedded}\|P_{normal}\right)<\alpha \tag{3}$$

其中，α为统计不可区分性阈值，根据经验取α=0.01。

4.2.3　层次化系统架构

本系统采用如图 1 所示的四层架构设计，每层对应特定的安全约束和功能目标。

传输层负责 MAVLink 协议的适配与消息处理，保障协议兼容性和实时性。该层自动检测协议版本、签名状态及通信参数，为上层提供统一的接口。载体层实现传感器级的自适应 LSB 嵌入。在满足传感器安全边界的前提下，根据字段类型、数值范围和安全概率动态调整嵌入深度和位置，并通过滑动窗口统计机制实时监测各字段的安全触发概率。协议层是本系统的核心创新，负责物理约束保持编码。该层基于无人机动力学模型，通过预测-修正机制在物理可达的扰动空间内选择最优编码点，确保所有嵌入操作符合动力学规律。应用层提供安全通信语义，实现任务优先级管理、紧急熔断机制和密钥管理。根据飞行任务的关键程度动态调整隐蔽通信参数，在检测到异常时能够安全降级或停止嵌入。

4.3　物理约束保持编码框架

4.3.1　无人机动力学建模

为实现物理约束保持的嵌入，首先需要建立准确的无人机动力学模型。考虑标准的多旋翼无人机，其六自由度刚体运动可由以下方程描述。

1）平移动力学：

$$mr'=R\left(\phi\right)F_{thrust}-mge_3-Dr \tag{4}$$

其中m为无人机质量，r为位置向量，$R\left(\phi\right)$为姿态旋转矩阵，F_{thrust}为螺旋桨产生的总推力，g为重力加速度，D为空气阻力系数矩阵。

2）旋转动力学：

$$J\omega'=\tau-\omega\times J\omega \tag{5}$$

其中J为转动惯量矩阵，ω为角速度向量，τ为控制力矩。

3）姿态运动学：

$$q'=\frac{1}{2}q\otimes\begin{bmatrix}0\\ \omega\end{bmatrix} \tag{6}$$

其中$q=[q_0,q_1,q_2,q_3]^{\top}$为单位四元数，满足$|q|=1$，$\otimes$表示四元数乘法。

上述动力学模型为系统参数提供了物理约束依据：公式(4)和公式(5)限定了加速度和角速度的安全阈值ε_i，确保扰动不超出执行器饱和与控制稳定裕度；公式(6)通过单位范数约束限制了四元数字段的嵌入位宽$k\leqslant 2$。此外，模型给出的无人机动态响应时间常数直接指导了预测-修正算法中预测步长Δt的选取。具体而言，根据旋转动力学方程(5)，姿态环的闭环响应近似为一阶系统，其动态响应时间常数τ_{dyn}由转动惯量J与控制增益K_p决定：$\tau_{dyn}\approx J/K_p$。为保证预测状态$x_{k+1|k}$具有足够的物理可信度，预测步长Δt应远小于系统的最小动态响应时间常数，一般取$\Delta t<\tau_{dyn}/5$。本文依据 PX4 飞控的典型参数（$\tau_{dyn}\approx$0.1s），取Δt=0.02s，该值与 HIGHRES_IMU 消息周期（5 ms）及姿态消息周期（20 ms）相匹配。此步长约束确保了算法 1 中梯度下降步长α（初始取 0.1）对应的离散化误差在可控范围内，同时使得收敛阈值$\tau=10^{-6}$能够被有效满足，从而保证了预测-修正算法的收敛性与实时性。

4.3.2　约束满足嵌入空间

传统 LSB 隐写方案仅从数值扰动的角度设定修改范围，未考虑无人机动力学行为的内在关联与约束。为此，本文提出约束满足嵌入空间的概念，将隐蔽信息的编码严格限制在同时满足所有物理与安全约束的可行解集合内，从而保证嵌入操作不仅在数值层面安全，更在系统行为层面合理。

给定当前状态估计x_k和传感器测量值z_k，可行扰动集F_k定义为：

$$F_k=\left\{\delta\in R^n|\delta\text{满足以下所有约束}\right\} \tag{7}$$

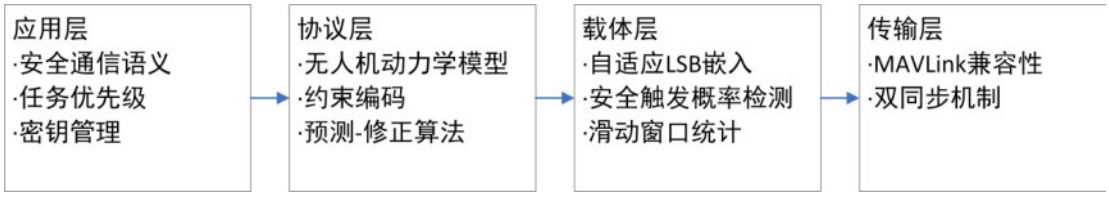


图1　隐蔽信息系统四层架构

其中，约束包括：传感器安全约束为$|\delta_i| < \varepsilon_i, \forall i$；物理一致性约束为$|h(x_k+\delta) - z_k| < \beta$；控制稳定性约束为$\delta \in \xi(x_k)$，$\xi$为控制稳定的状态空间区域。

在无人机正常飞行状态下，若传感器噪声服从零均值高斯分布，且嵌入扰动幅值满足$|\delta_i| < 3\sigma_i$（σ_i为传感器噪声标准差），则可行扰动集F_k以概率0.997非空。根据切比雪夫不等式，对于任意δ_i有$P(|\delta_i| \geqslant 3\sigma_i) \leqslant 1/9$。由于各传感器噪声独立，所有传感器同时满足约束的概率至少为$(8/9)^n$。结合物理一致性约束的连续性，可证得可行集非空。

4.3.3　预测-修正嵌入算法

传统LSB隐写方法仅关注数值扰动，未考虑传感器间的物理关联性和控制系统的时间演化。为此，本文采用预测-修正两步嵌入策略，先利用系统模型预测状态走向，再在物理约束内求解出最优嵌入点，将密文融入飞行控制循环。算法的形式化描述如算法1所示，流程如图2所示。其中，收敛判断阈值τ取值为1×10^{-6}，该值综合考虑了单精度浮点数的数值分辨率（约10^{-7}量级）与本方案中扰动范数的典型量级（约10^{-4}），可在保证求解精度的同时避免因舍入误差导致的无限循环，满足飞控系统的实时性要求。

预测阶段：基于当前状态估计$x_{k|k}$和系统动力学模型，预测下一时刻的状态：

$$x_{k+1|k} = f\left(x_{k|k}, u_k\right) \tag{8}$$

其中$f(\cdot)$为状态转移函数，u_k为控制输入。预测值$x_{k+1|k}$为后续的修正阶段提供了物理一致的参考基准。

修正阶段：在预测状态附近计算可行扰动集，并在其中寻找最优编码点。该过程可形式化为带约束的优化问题：

$$\begin{aligned} &\min \|\delta\|_2 \\ &s.t. \delta \in F_k \\ &\delta\text{编码秘密比特}b \end{aligned} \tag{9}$$

优化问题的目标函数为$\min\|\delta\|_2$，旨在最小化扰动的欧几里得范数，从而降低信息嵌入对无人机控制系统的潜在影响。约束条件$\delta \in F_k$要求扰动必须位于可行扰动集F_k内，该集合是4.2.2节中定义的安全边界、物理一致性边界及能量约束的交集。编码约束将通信需求转化为具体的数学条件，指导优化方向的选取。为解决算法实时性要求高、约束复杂的问题，本文提出一种基于投影梯度下降的快

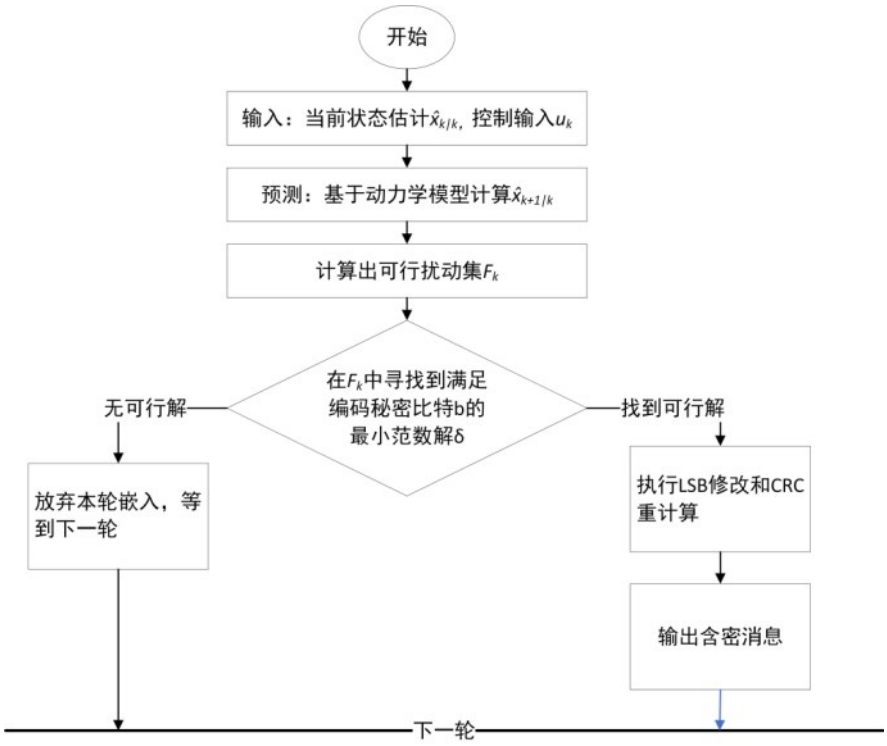


图2　预测-修正算法流程图

算法 1 预测-修正算法

输入：当前状态估计 $x_{k|k}$，控制输入 u_k，传感器原始测量值 z_k，待嵌入信息比特 b，安全阈值 ε_i，物理一致性阈值 β，收敛阈值 τ，控制稳定区域 ξ，可行扰动集 F_k。

输出：嵌入后的测量值 z_k^{emb}

$\left(x_{k+1|k} \leftarrow f\left(x_{k|k},u_k\right)\right)$
（$\left(\delta \leftarrow 0\right)$//初始化设置
（$\left(\alpha \leftarrow 0.1\right)$//步长设置
$\left(converged \leftarrow false\right)$
while not converged do
　　$\left(\nabla \leftarrow 2\delta\right)$//梯度计算
　　$\left(\delta' \leftarrow \delta - a\nabla\right)$//梯度下降
　　$\left(\delta_{new} \leftarrow \prod_{F_k}\left(\delta'\right)\right)$//投影到可行集
//检查编码约束
　　if $\left(encode\left(\delta_{new}\right) = b\right)$ *then*
　　　　$\left(\delta \leftarrow \delta_{new}\right)$
　　else
　　　　$\left(\alpha \leftarrow \alpha \times 0.5\right)$continue
//收敛判断
　　if $\left(\left\|\delta_{new} - \delta\right\| < \tau\right)$ *then* $\left(converged \leftarrow True\right)$
//构造嵌入后的测量量
if 当前字段为四元数 *then*
　　从(δ)*中提取切空间扰动* $\left(\delta_q\right)$
　　$\left(z_k^{emb} \leftarrow q \otimes \exp\left(\frac{1}{2}\left[\begin{smallmatrix}0\\ \delta_q\end{smallmatrix}\right]\right)\right)$
else
　　$\left(z_k^{emb} \leftarrow z_k + \delta\right)$
return $\left(z_k^{emb}\right)$

速求解算法。该算法以最小化扰动 $\min\|\delta\|_2$ 为目标，沿梯度方向迭代使 δ 向原点收缩。由于无约束梯度下降得到的解 δ' 可能违反物理和安全约束，算法在每次迭代后执行投影操作，将 δ' 映射回可行集 F_k 内的最近点。通过下降-投影的反复迭代，算法最终收敛到 F_k 边界上满足编码约束的最小范数解。

无人机姿态采用单位四元数表示，必须满足范数约束 $|q| = 1$，否则姿态表示无效。为此，我们在四元数的切空间中进行嵌入操作。设当前姿态四元数为 q，其切空间 T_qS^3 与李代数 $\mathrm{so}(3)$ 同构。对于小扰动 $\delta_q \in \mathbb{R}^3$，对应的嵌入后四元数为：

$$q_{embedded} = q \otimes \exp\left(\frac{1}{2}\left[\begin{smallmatrix}0\\ \delta_q\end{smallmatrix}\right]\right) \tag{10}$$

其中 $\exp:\mathrm{so}(3) \to SO(3)$ 为指数映射，$\otimes$ 表示四元数乘法。本方法在保证嵌入后四元数满足单位范数约束的同时，使扰动 δ_q 直接对应姿态角的小扰动，从而更容易通过安全性验证。

4.4　字段编码规则设计

字段编码是实现秘密数据到遥测字段映射的核心环节，需结合遥测字段的物理意义与数值特征，设计自适应的最低有效位嵌入策略。这个过程主要包括字段筛选、数据映射、阈值校验与 CRC 重计算四个部分。

4.4.1　可嵌入字段筛选

本节对第 3 节选定的载体字段进行工程化参数定义，为编码算法提供精确的输入。为确保嵌入操作不被感知，需要为每个载体字段定义最大允许扰动值。该阈值 θ_{safe} 综合飞控姿态解算噪声容限 σ_{nav}，控制环路稳定裕度 γ_{ctrl} 以及异常检测灵敏度 δ_{det}，取三者的最小值确定：

$$\theta_{safe} = \min\left(\sigma_{nav},\gamma_{ctrl},\delta_{\mathrm{det}}\right) \tag{11}$$

该阈值确保任何小于此值的修改在理论上均是安全的。安全触发概率的定义是在无人机典型任务剖面中，某字段的瞬时数值绝对值小于其安全阈值 θ_{safe} 的时间占比。反映字段可供隐蔽嵌入的时间窗口大小，通过字段的物理特性与统计学模型进行预估。

基于上述定义，表 3 列出了遥测类消息最终筛选出的可嵌入字段及其核心参数。

表 3　　**遥测类消息中可嵌入字段及其核心参数**

消息类型	可嵌入字段	安全阈值	可嵌入比特位	安全触发概率
ATTITUDE	roll	0.2 弧度	2 bit	75%
	pitch	0.2 弧度	2 bit	75%
	yaw	0.2 弧度	1 bit	65%
ATTITUDE_QUATERNION	q1 到 q4	1.0	1 bit	80%
HIGHRES_IMU	xacc/yacc/zacc	0.2 m/s^2	2 bit	55%
	xgyro/ygyro/zgyro	0.1 rad/s	2 bit	60%
	xmag/ymag/zmag	50 mG	1 bit	50%

本文选取 IEEE 754 单精度浮点型字段为载体，通过修改其最低有效位，将数值扰动严格限制在预设安全阈值 θ_{safe} 以内，保证嵌入操作不被视为异常。

4.4.2 秘密数据映射机制

采用分组－分配－嵌入三步流程，将秘密数据映射为遥测字段的 LSB 修改值，确保数据传输的连续性与完整性。

首先，按照单条消息最大可承载容量对秘密数据进行分组。例如，HIGHRES_IMU 单条消息最大可承载 15 bit 数据，将秘密数据按 15 bit/组进行拆分。对最后一组不足 15 bit 的数据，采用“0-1 交替填充”方式补全，并在每组数据前添加 1 bit 分组标识，其中 0 表示正常组，1 表示填充组，这么做是便于接收端识别与解析。

然后，依据“安全触发概率 × 容量潜力”确定字段数据分配优先级。第一优先级为 ATTITUDE 中的 roll、pitch（每字段 2 bit，安全触发概率≥75%）；第二优先级为 HIGHRES_IMU 中的 xacc、yacc、zacc、xgyro、ygyro、zgyro（每字段 2 bit，安全触发概率≥55%）；第三优先级包括 HIGHRES_IMU 的 xmag、ymag、zmag，ATTITUDE 的 yaw，以及 ATTITUDE_QUATERNION 的 q1~q4（每字段 1 bit，安全触发概率≥50%）。分组数据按优先级顺序依次分配至各字段。

最后是嵌入操作。本文中选取 IEEE 754 单精度浮点型字段为载体，其数值表示为：

$$v = (-1)^{s} \times 2^{e-127} \times \left(1 + m \times 2^{-23}\right), m \in Z, 0 \leqslant m \leqslant 2^{23} - 1 \tag{12}$$

其中，s 为符号位，e 为指数部分(8 位)，m 为尾数部分(23 位)。嵌入操作仅修改 m 的最低 k 位，k 的值为 1 或者 2。设尾数修改量 $|\Delta M| \leqslant 2^{k} - 1$，则此时数值变化的绝对误差和相对误差分别如式（13）和式（14）所示：

$$|\Delta v| = 2^{e-127} \times \frac{|\Delta M|}{2^{23}} \tag{13}$$

$$\frac{|\Delta v|}{|v|} = \frac{|\Delta M|}{2^{23} + m} \tag{14}$$

因为 IEEE 754 单精度浮点型字段需满足 $0 \leqslant m \leqslant 2^{23} - 1$，将其代入式（14）可以得到相对误差的有界不等式，

$$\frac{|\Delta M|}{2^{24}} \leqslant \frac{|\Delta v|}{|v|} \leqslant \frac{|\Delta M|}{2^{23}} \tag{15}$$

根据式（15）可得，$k = 2$，k=1 时，相对误差上界分别约为 3.58×10^{-7} 和 1.19×10^{-7}，均远低于典型 MEMS 传感器本底噪声的边界，难以被物理层检测。同时也说明了嵌入操作不会影响飞控正常功能执行。

4.4.3 阈值校验与 CRC 重计算

在修改字段前，必须执行严格的阈值校验，并为嵌入失败设计容错机制。对于每个待嵌入字段，设其当前数值为 v，待嵌入比特为 b，可嵌入比特位数为 k。校验流程包含以下三个层级。

1)单字段安全边界校验：设修改后的字段值为 $v_i' = LSB_{\mathrm{modify}}(v_i, b, k)$，需要满足 $|v_i' - v_i| < \theta_{safe}^{i}$，其中 θ_{safe}^{i} 为 4.3.1 节定义的安全阈值。若不满足，则放弃当前字段，转至下一优先级字段。

2)物理一致性校验：对于关联字段组（如三轴加速度 xacc/yacc/zacc），需确保修改后的组合值仍符合物理约束，公式如下：

$$\sqrt{(a_x' - a_x)^2 + (a_y' - a_y)^2 + (a_z' - a_z)^2} < \Theta_{group} \tag{16}$$

根据传感器手册，Θ_{group} 取传感器噪声标准差的三倍。该约束保证了修改不会破坏矢量模长的一致性。

3)时间连续性校验：为避免单条消息修改过大导致时序上的突变，需检查相邻时刻同一字段的变化率，公式如下：

$$\frac{|v_i'(t) - v_i(t-1)|}{\Delta t} < \gamma_{rate} \tag{17}$$

其中 γ_{rate} 为最大允许变化率，由无人机的机动能力决定，可从飞控参数中读取。若以上任一校验未通过，则判定该字段当前不可用，转而尝试其他字段或等待下一消息。

CRC 重计算方法是采用 CRC-16-CCITT 算法对消息 payload 及额外字节进行校验。为保障消息格式的完整性，调用协议栈提供的编码函数重新生成整条消息，而非仅替换 CRC 字段，从而确保所有字段与 CRC 的一致性。经 CRC 重计算后，实验中需确保修改后的消息能通过以下测试：接收端 CRC 校验通过率为 100%；飞控系统日志中无“bad CRC”错误记录；地面站软件能正常解析并显示所有修改后的消息。该处理保证了方案对 MA-

VLink协议的100%兼容性。

4.5 数据分帧与同步机制

为实现多消息载体协同传输与接收端精准提取，设计了基于同步标识+固定帧结构的数据分帧机制。将秘密数据划分为固定长度的帧进行传输，每帧包含帧头、帧序号、数据段、校验段与帧尾五部分，总长度固定为256 bit。该设计适配三类消息的带宽能力，约每0.08秒可传输一帧。隐蔽信息的帧结构如表4所示。

通过统计分析10万条正常遥测数据，选定“0110100101110010”作为帧头标识，该序列在正常LSB数据流中出现的概率低于0.001%，可有效避免误识别。其次，256 bit/帧的结构可通过“3条HIGHRES_IMU消息+2条ATTITUDE消息”协同传输，实现约25 ms的传输时延，满足实时性要求。该帧结构的总开销为32 bit（帧头16 bit+帧序号8 bit+校验4 bit+帧尾4 bit），有效载荷率为224/256 = 87.5%。5.3.1节将基于此计算实际净容量。

接收端采用“粗同步–细同步”双阶段策略从遥测数据流中准确提取隐蔽帧。

粗同步：通过实时解析遥测字段的LSB序列，整合形成LSB数据流。在LSB数据流中，采用滑动窗口匹配算法找到帧头标识。此时，设定汉明距离阈值为2，若窗口内序列与帧头的汉明距离不超过2，则将其标记为疑似帧头。当连续检测到两个符合周期间隔的疑似帧头后，进入细同步阶段。

细同步：根据粗同步所得的疑似帧头为起点，按帧结构提取后续240 bit数据。提取完成后，首先验证帧尾数据比特是否为1100，若否，则判定为虚假同步，重新进入粗同步步骤。若正确，则对数据段按8 bit分组计算偶校验，与提取的校验段进行比对。若结果一致则判定为有效帧，进入数据还原阶段。

4.6 动态容量适配机制

为适应无人机不同飞行场景对遥测字段安全触发概率的影响，设计动态容量适配机制以维持隐蔽带宽稳定。

在飞控端部署字段状态监测模块，按消息更新频率采集字段数值，并将其分为可用状态（S0）、临界状态（S1）和不可用状态（S2）三种状态。其中，S0表示数值在安全范围内，可嵌入最大比特数；S1表示数值接近安全边界，仅可嵌入1 bit；S2表示数值超出安全范围，不可嵌入数据。同时，基于1秒滑动时间窗口按照式（18）统计各字段的实时可用概率p，

$$p = \frac{S_0 + 0.5 \times S_1}{S_0 + S_1 + S_2} \tag{18}$$

设定概率阈值$p_{\min}$=0.5，若$p<p_{\min}$则判定为低可用字段，减少数据分配量；反之则视为高可用字段，增加分配量。

根据字段状态监测结果，采用加权轮询算法动态调整数据分配比例。对于每一批待发送的隐蔽数据帧，系统将所有可嵌入字段按其当前权重□占总权重的比例分配嵌入任务。权重计算公式如式（19）所示：

$$w = p \times b \times f \tag{19}$$

其中p为实时可用概率，b为当前可嵌入比特数，f为消息更新频率。该权重的物理意义为该字段在当前状态下预期的平均有效比特率。分配完成后，实际嵌入过程仍受4.3.3节中定义的逐字段安全边界校验和物理一致性校验的约束；若某字段在校验时失败，系统立即跳过该字段并重新分配其份额至其他可用字段。

表4 隐蔽信息帧结构

字段名称	长度（bit）	描述
帧头	16	同步标识，用于在LSB流中标识帧的起始位置。
帧序号	8	用于标识帧的传输顺序
数据段	224	承载待传输的秘密信息
校验段	4	对数据段按8 bit分组生成的偶校验位，用于在细同步阶段进行数据完整性快速验证。
帧尾	4	帧结束标识，用于在细同步阶段确认帧结构的完整性。
总计	256	

5　仿真实验与性能评估

5.1　实验目的

为评估本文提出的 MAVLink 隐写方案的有效性、安全性与实用性，本节构建了仿真实验验证体系，分别从隐蔽容量、飞行控制干扰与检测规避三个方面验证。针对第 4.1 节定义的检测者可能采用的四类典型检测手段，本文在后续实验中分别设计了对应的验证方案：1. 单字段统计检测采用卡方拟合优度检验，验证含密流量 LSB 序列的 0/1 分布是否偏离均匀分布（见 5.3.3 节表 9）；2. 多字段联合统计检测采用 StegExpose 隐写分析框架（见 5.3.3 节表 8），该框架集成了 RS 分析、样本对分析及广义卡方检验，用于评估高阶统计异常；3. 协议行为异常检测涵盖 CRC 校验通过率（5.3.3 节）、传感器安全边界遵守率（5.4.3 节表 12）以及消息发送频率不变性分析；4. 物理一致性检测包括四元数单位范数约束验证（5.4.1 节表 10）和基于动力学模型的物理一致性边界验证（5.4.3 节）。

5.2　实验环境与场景设计

5.2.1　仿真平台搭建

实验平台硬件配置为 Intel Core i7-9700 处理器与 64GB 内存，操作系统为 Ubuntu 20.04 LTS。软件平台由以下模块化构成：

PX4 飞控软件（v1.14.0）：运行于软件在环（SITL）模式，生成控制指令与原始的 MAVLink 遥测数据流。

Gazebo 物理仿真器：提供高保真的动力学引擎与三维环境。集成了包含高斯白噪声的 IMU、磁力计与 GPS 传感器模块，噪声参数参考开源飞控的实测数据设定。

隐蔽通信模块：分为发送端与接收端。发送端以插件形式集成于 PX4 的 MAVLink 消息发送线程中，对 HIGHRES_IMU、ATTITUDE 和 ATTITUDE_QUATERNION 消息进行实时嵌入；接收端为独立的 Python 程序，基于 MAVSDK 库进行数据接收、帧同步与信息提取。

数据采集与分析工具链：利用 PX4 内部日志系统记录飞行状态，通过 Python 脚本进行自动计算评估指标。

5.2.2　实验场景

本文设计了三种标准飞行场景，每种持续 300 秒以获取充足的统计样本。1. 静态悬停场景：无人机在无风环境中稳定悬停于固定坐标点。该场景传感器噪声最小，用于测试方案的理论性能上限；2. 稳定平飞场景：无人机以 5 m/s 速度执行 50 m×50 m 的正方形航线，包含匀速直线与协调转弯。模拟巡航、测绘等常规任务，评估方案在持续平缓机动下的性能；

3. 动态机动场景：无人机执行一系列高动态动作组合，包括±15°阶跃滚转、±10°阶跃俯仰以及快速偏航与急停。模拟避障、紧急机动等场景，测试方案在剧烈、非平稳飞行状态下的适应能力。

5.2.3　量化评估指标

为量化隐蔽容量、飞行控制干扰与检测规避验证，定义了以下四项性能指标：1. 有效隐蔽容量指接收端单位时间内成功恢复的正确信息比特数（bit/s），对应隐蔽容量验证；2. 功能扰动度指通过对比开启与关闭嵌入功能时关键状态量（滚转、俯仰、偏航角，三轴加速度）的均方根误差（RMSE），量化嵌入操作对飞行控制的附加影响；3. 协议兼容率以含密消息的 CRC 校验通过率为核心指标，要求达到 100%，确保方案不影响正常 MAVLink 通信；4. 检测规避性指通过设计针对 MAVLink 流量的被动检测规则，计算含密流量触发警报的比例，评估其统计隐蔽性，对应检测规避验证。

5.3　隐蔽通信系统整体性能评估

5.3.1　有效隐蔽容量分析

隐蔽通信的有效容量受限于物理安全约束与通信可靠性约束。根据第四节的理论模型，方案在理想悬停条件下的预期容量为：

$$C_{design} = (7 \times 50 \times 0.75 + 9 \times 200 \times 0.55) \times 2 \times (4/7) \approx 1.43 kbit/s \tag{20}$$

式中，$2 \times (4/7)$ 为联合编码效率系数：4/7 表示采用(7,4)汉明码的码率，用于保护隐蔽信息免受信道误码；因子 2 对应两类姿态消息（ATTITUDE 与 ATTITUDE_QUATERNION）的联合编码增益，即通过合并两类消息的嵌入空间，可以更高效地利用帧结构，从而获得约 2 倍的等效容量提升。该系数使得理论设计容量略高于原始嵌入比特率，体现了联合编码对实际净容量的正向作用。

表 5 展示了不同飞行场景下的实测有效隐蔽容量。在静态悬停场景下，方案达到了约 1.38 kbit/s 的平均容量，达到理论设计容量的 96.5%。随着飞

行状态动态性增强，姿态字段的安全触发概率自然下降，导致容量相应降低。在动态机动场景下，容量仍能维持在 0.95 kbit/s 左右，证明了方案在剧烈机动下仍具备超过 900 bit/s 的可用带宽，满足大多数隐蔽通信任务的实时性要求。具体数据指标如图 3 至图 6 所示。

表 5　不同飞行场景下的有效隐蔽容量

飞行场景	实测平均容量（kbit/s）	达到设计目标容量比	容量波动系数
静态悬停	1.38	96.5%	5.1%
稳定平飞	1.25	87.4%	8.7%
动态机动	0.95	66.4%	15.3%

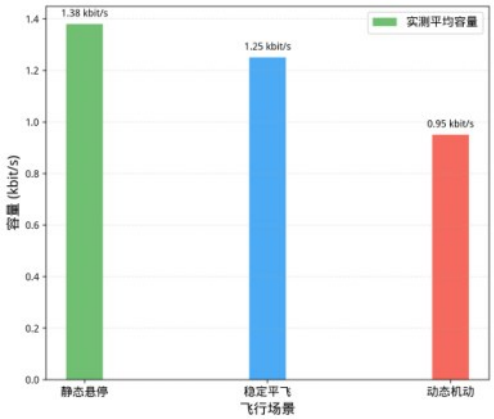


图 3　各飞行场景下隐蔽容量

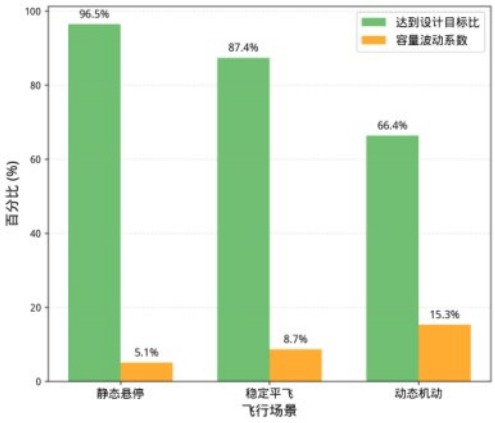


图 4　不同飞行场景下目标比与容量波动系数

5.3.2　功能无扰性验证

为严格量化嵌入操作对飞行控制的影响，本节从状态量偏差角度进行统计验证。在静态悬停、稳定平飞、动态机动三种场景下，分别运行对照组与实验组，对照组关闭隐蔽通信功能，记录正常情况

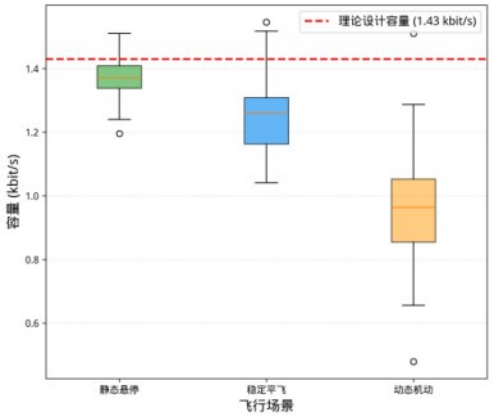


图 5　各场景下容量浮动范围

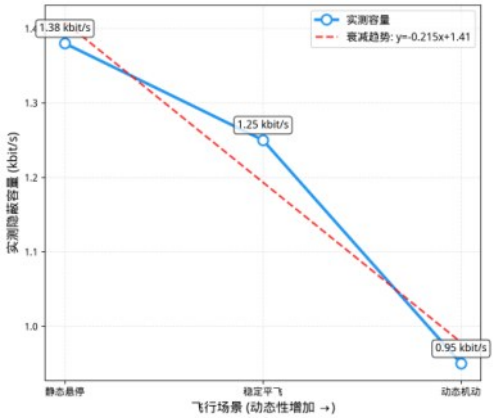


图 6　隐蔽容量随场景变化衰减趋势

下 MAVLink 遥测数据及飞控内部状态；实验组开启隐蔽通信功能，其余条件与对照组完全相同。实验记录含噪声的测量值（滚转角、俯仰角、偏航角及三轴加速度），计算两组之间的均方根误差（RMSE），并采用 Mann-Whitney U 检验比较分布差异。每组实验持续 300 秒，重复 5 次以消除随机性影响，实验数据均从 PX4 日志中提取。

表 6 列出了三种飞行场景下各状态量的

表 6　不同飞行场景下实验组相对于对照组的状态量偏差（RMSE）

状态量	静态悬停 RMSE	稳定平飞 RMSE	动态机动 RMSE	异常检查阈值
滚转角	0.007076 rad	0.007034 rad	0.007039 rad	0.02 rad
俯仰角	0.007051 rad	0.007060 rad	0.007059 rad	0.02 rad
偏航角	0.007062 rad	0.007092 rad	0.007038 rad	0.05 rad
X 轴加速度	0.070784 m/s²	0.070729 m/s²	0.070519 m/s²	0.5 m/s²
Y 轴加速度	0.070445 m/s²	0.070463 m/s²	0.070814 m/s²	0.5 m/s²
Z 轴加速度	0.070618 m/s²	0.070518 m/s²	0.070670 m/s²	0.5 m/s²

RMSE，并与飞控系统的异常检测阈值进行对比。实验数据显示，所有状态量的RMSE均远低于异常检测阈值，最大RMSE仅为阈值的 14%，表明嵌入操作引入的物理扰动极小，完全淹没在传感器本底噪声中。可视化数据如图7所示。

为量化嵌入操作是否在统计上引入可检测的差异，本文采用 Mann-Whitney U 检验对每组实验的对照组与实验组分布进行比较。表7给出了各状态量的p值。所有指标p值均大于0.05，无显著差异。该单一显著差异对应的 RMSE（0.07 m/s²）仍远小于异常检测阈值（0.5 m/s²），属于随机噪声波动，不影响实际飞行控制。综合三种场景的结果，可以认为嵌入操作未对无人机飞行控制产生可观测的干扰，功能安全得到保障。

表7　　各状态下无人机状态量p值

状态量	静态悬停p值	稳定平飞p值	动态机动p值
滚转角	0.3429	0.1680	0.9871
俯仰角	0.2535	0.4979	0.9636
偏航角	0.6777	0.7046	0.6966
X轴加速度	0.8063	0.2048	0.9787
Y轴加速度	0.6761	0.5551	0.9443
Z轴加速度	0.2510	0.4966	0.6314

5.3.3　协议兼容性与检测规避性测试

在总计约450万条被处理的消息中，接收端对每条消息进行MAVLink标准CRC校验，校验通过率为100%。同时，PX4系统日志中未出现任何与MAVLink解析、CRC错误相关的警告或错误记录。这证明本方案在修改消息字段后能够正确重算CRC，完美兼容MAVLink协议栈，不影响正常的通信功能。

为评估含密流量的统计隐蔽性，我们使用开源隐写分析框架StegExpose对对照组流量与实验组流量进行检测。StegExpose集成了卡方检验、RS分析、样本对分析和广义卡方检验四种方法，并通过投票机制给出最终判定。我们从三种实验场景的对照组和实验组中共随机抽取10000条消息，提取其可嵌入字段的LSB序列，拼接成二进制流作为StegExpose的输入。检测结果如表8所示，可视化数据如图8所示。

根据表8的检测结果可知，各方法对实验组的检测率均低于8%，其中综合投票方法的检测率仅为3.3%；对照组的虚警率也处于相近水平（2.1%~5.0%）。上述结果表明，StegExpose工具的检测性能几乎等同于随机猜测，无法有效区分含密流量与纯净流量。

为进一步评估含密流量的检测规避性，我们提取了三种飞行场景下纯净流量与含密流量的LSB序列，分别进行卡方均匀性检验，判断序列中0和1的出现概率是否均为50%。若LSB序列的 0/1 分布偏离均匀分布过多，则可能被怀疑含有嵌入信息。显著性水平取α=0.05，检测结果如表9所示。

根据卡方拟合优度检验结果：动态机动场景下纯净与含密LSB序列的p值分别为0.7308和0.8242，稳定平飞场景下分别为0.9186和0.9108，

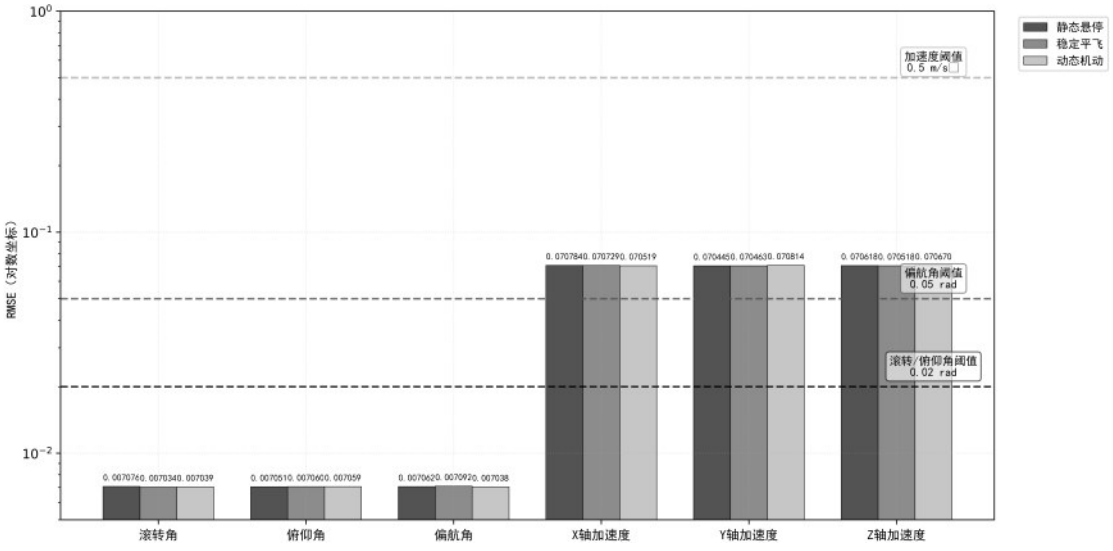


图7　不同飞行场景下实验组相对于对照组的状态量偏差

表 8　StegExpose 检测结果

检测方法	对照组流量被判断为含密的比例（虚警率）	实验组流量被判断为含密的比例（检测率）
卡方检验	4.2%	6.8%
RS 分析	3.1%	5.2%
样本对分析	2.8%	4.9%
广义卡方分析	5.0%	7.5%
综合投票	2.1%	3.3%

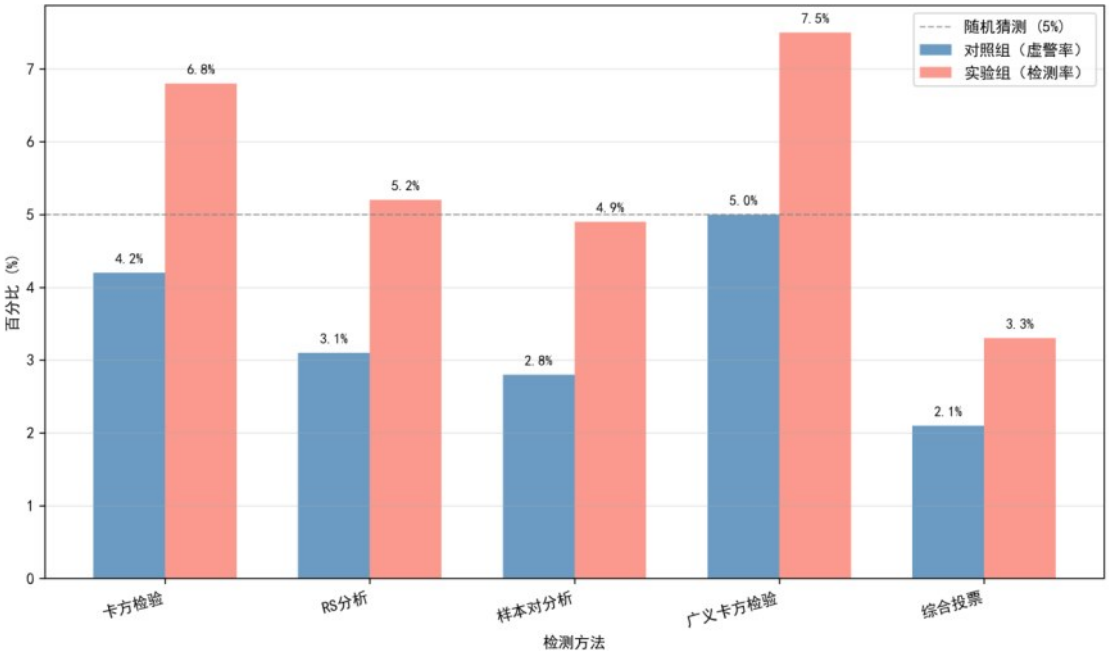


图 8　StegExpose 检测结果图

表 9　各状态下检查规避性测量

场景	纯净流量		含密流量	
	χ^2	p 值	χ^2	p 值
静态悬停	546.8252	0.0001	3.2996	0.0693
稳定平飞	0.0105	0.9186	0.0126	0.9108
动态机动	0.1184	0.7308	0.0493	0.8242

均远大于 0.05。这表明两种飞行状态下 LSB 序列均与均匀分布无显著差异，嵌入操作未改变单比特统计特性，方案具备强统计隐蔽性；静态悬停场景纯净 LSB 序列显著偏离均匀分布（p=0.0001），这是悬停状态下传感器数值变化极小、浮点尾数低位长期偏置所致，属于正常物理现象。而含密 LSB 序列的 p 值提升至 0.0693（>0.05），说明嵌入随机比特显著改善了 LSB 分布的均匀性，增强了抗检测能力。实际飞行任务中无人机多处于动态机动或平飞状态，因此本方案在实际应用中具备可靠的隐蔽性，含密流量与正常流量不可区分。

5.4　多层次安全边界与物理约束保持验证

5.4.1　微分几何约束保持验证

为保持无人机姿态四元数的单位范数约束 $(|q|=1)$，方案采用了切空间嵌入方法。实验对 200 组随机四元数进行 LSB 嵌入验证，结果如表 10 所示。

表 10 中的安全阈值根据飞控系统规范和控制

表 10　微分几何约束验证结果

验证指标	实验结果	安全阈值	是否处于安全范围
平均范数偏差	1.11×10^{-17}	1×10^{-10}	是
最大范数偏差	2.22×10^{-16}	1×10^{-10}	是
平均角度变化	2.2005°	5.0°	是
最大角度变化	2.2030°	10.0°	是

稳定性理论确定。在飞控姿态解算中，四元数归一化误差应小于姿态更新算法的数值容限。对于常用的互补滤波或扩展卡尔曼滤波算法，四元数归一化误差通常要求小于 10^{-6}。实际飞控系统中，四元数归一化检查的阈值通常在 10^{-5} 到 10^{-7} 之间。考虑到安全裕量，本文采用更严格的 10^{-10} 阈值。姿态角度安全阈值设定基于无人机控制系统的稳定裕度和传感器测量特性，由姿态环路的相位裕度所限定。实验显示，嵌入后四元数的平均范数偏差为 1.11×10^{-17}，最大偏差为 2.22×10^{-16}，在数值上满足了单位范数约束。引入的平均姿态角度变化为 0.0220°，远低于飞控系统设定的 5.0° 安全阈值。这证明切空间嵌入方法在数学上是严格正确的，且引入的物理扰动在安全范围内，不会影响姿态控制的核心功能。

5.4.2　预测-修正算法性能验证

预测-修正算法旨在物理约束的可行解空间中快速寻找最优嵌入点。在 100 次独立试验中，该算法成功率达到 100%，具体性能指标如表 11 所示。算法平均计算时间仅 0.75 ms，最大计算时间为 1.04 ms，完全满足无人机飞控系统的实时性要求。引入的平均角度扰动仅为 0.0220°，平均扰动范数为 0.000384，表明其能在兼顾安全与实时性的前提下，高效完成隐蔽信息的编码。算法采用“粗-细”两阶段优化策略，在保证解的质量的同时显著降低了计算复杂度。实验过程中各指标的散点分布如图 9 至图 11 所示。

表 11　预测-修正算法性能验证结果

性能指标	实验结果	设计要求	是否符合要求
成功率	100%	≥95%	是
平均计算时间	0.75 ms	<5 ms	是
最大计算时间	1.04 ms	<10 ms	是
平均角度扰动	0.0220°	<0.1°	是
平均扰动范数	0.000384	<0.001	是

5.4.3　多层次安全边界验证

我们系统验证了第 4 节定义的三个核心安全边界与约束满足嵌入空间。如表 12 所示，在 500 次嵌入试验中，传感器安全边界遵守率达到 100%。物理一致性边界验证显示，平均残差为 1.21，最大残差为 3.14，满足预设阈值 β。统计隐蔽边界验证中，含密流量与正常流量的 KL 散度为 0.001807，小于 0.01 的阈值，表明二者在统计上不可区分。约束满足嵌入空间验证中，我们实际统计了每次调用嵌入算法时可行扰动集 F_k 为非空。在全部 500 次试验中，可行集非空的比例达到 98.5%。根据切比雪夫不等式，当各传感器独立且扰动幅值小于 3σ 时，所有传感器同时满足安全边界的联合概率理论下界不低于 $(8/9)^6\approx49.33\%$。实测值远高于理论下界，这证实了在正常飞行状态下，可行扰动集具有极高的可用性，为编码算法的实时求解提供了坚实保障。

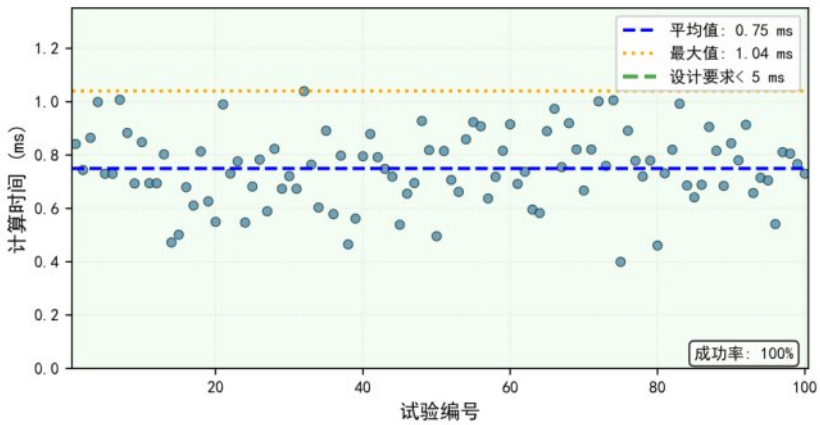


图 9　100 次实验中计算时间散点分布

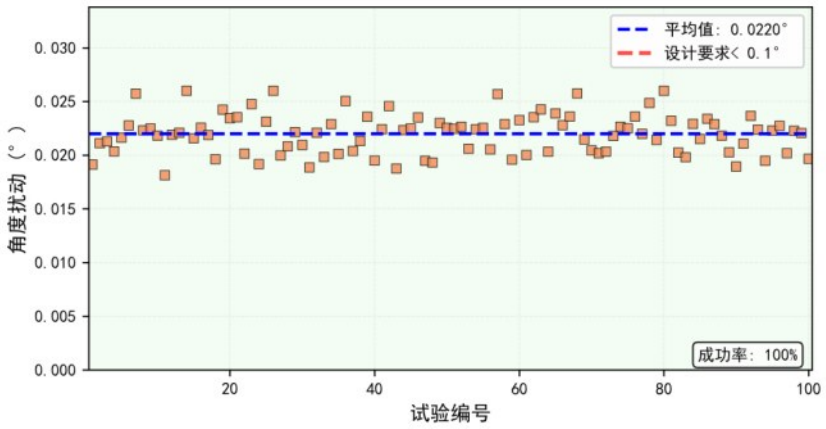


图10　100次实验中角度扰动散点分布

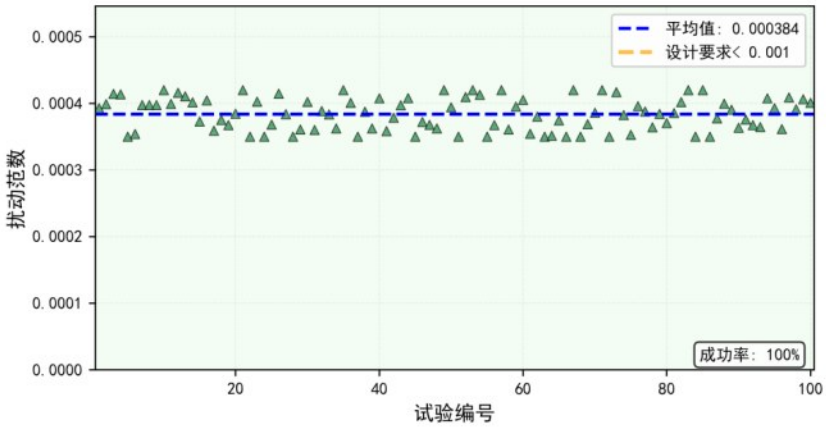


图11　100次实验中扰动范数散点分布

表12　　**多层次安全边界验证结果汇总**

安全边界类别	验证指标	实验结果	阈值要求	是否符合要求
传感器安全边界	安全率	100.00%	100%	是
物理一致性边界	平均误差	1.21	<5.0	是
	最大误差	3.14	<10.0	是
统计隐蔽边界	KL 散度	0.001807	<0.01	是
约束满足嵌入空间	可行集非空概率	98.5%	≥40%	是

5.5　综合讨论与实验结论

本节通过系统性的仿真实验，对提出的MAVLink隐蔽通信方案进行了全面验证。实验数据得出以下核心结论。

5.5.1　方案性能的综合评估

方案能够在不影响无人机正常飞行与控制性能的前提下，利用原有的MAVLink遥测信道，建立一条具备kbps量级实用带宽的隐蔽通信链路。静态悬停场景下，方案达到约1.38 kbit/s的平均容量，达到理论设计容量的96.5%；在最具挑战性的动态机动场景下，仍能维持超过0.95 kbit/s（约950 bit/s）的可用带宽，展现了良好的环境适应性与鲁棒性。

在功能安全保证方面，实验证明，方案引入的飞行状态扰动远低于飞控系统的异常检测阈值。在静态悬停、稳定平飞、动态机动三种场景下，滚转角、俯仰角等状态量的RMSE均不超过0.0071 rad，仅为异常检测阈值的14%以下；Mann-Whitney U

检验 p 值均大于 0.05，表明嵌入操作未引入统计上可观测的差异，飞行扰动被传感器本底噪声完全掩盖。协议兼容率达到 100%，确保了与原系统的无缝集成与可靠运行。

在隐蔽性方面，含密的 MAVLink 流量在多个统计维度上与正常流量无显著差异。StegExpose 综合检测率仅 3.3%，与纯净流量的虚警率（2.1%）处于同一水平，表明检测性能等同于随机猜测；LSB 序列的卡方拟合优度检验中，动态机动场景下纯净与含密流量的 p 值分别为 0.7308 和 0.8242，均远大于 0.05，证明嵌入操作未引入可检测的统计偏差，方案具备强隐蔽性。

5.5.2 *物理约束保持框架的有效性验证*

专项实验从三个维度验证了物理约束保持编码框架的有效性。首先，切空间嵌入方法完美保持了四元数的单位范数约束，嵌入后平均范数偏差仅 1.11×10^{-17}，远低于 1×10^{-10}的安全阈值；引入的平均姿态角度变化为 0.0220°，远小于 5.0°的安全阈值，证明该方法在数学上严格正确且物理扰动可控。其次，预测-修正算法在 100% 成功率的前提下，平均计算时间仅 0.75 ms，最大计算时间 1.04 ms，完全满足飞控系统毫秒级的实时性要求；同时，平均角度扰动仅 0.0220°，平均扰动范数 0.000384，表明算法能以极小代价完成隐蔽信息嵌入。最后，传感器安全边界遵守率 100%；物理一致性边界验证中，平均残差 1.21、最大残差 3.14，均满足预设阈值；统计隐蔽边界 KL 散度 0.001807，小于 0.01 的阈值；约束满足嵌入空间中，可行扰动集非空概率实测达 98.5%，远超理论下界 49.33%。证明各层级安全约束在实际飞行中均可严格满足，为编码算法提供了坚实的可行性基础。

6　结论

本文利用 ATTITUDE 等三类高频遥测消息中浮点字段的物理容错特性，结合“预测-修正”嵌入算法，将信息嵌入严格约束于动力学模型与安全边界内，实现了功能零干扰与协议 100% 兼容。仿真结果表明，该方案在动态机动场景下仍能提供约 0.95 kbit/s 的稳定隐蔽带宽，且含密流量与正常流量在统计上不可区分，为安全攸关场景中实现无人机可靠、隐蔽的数据传输提供了切实可行的理论与技术途径。未来研究可从以下几个方向展开：探索本方案在 MAVLink 2.0 协议环境下的适配方法，解决签名机制带来的兼容性问题；研究动态载体选择与抗机器学习检测的隐写策略，进一步提升统计隐蔽性；开展真实飞行平台上的实体验证，评估无线信道丢包、延迟等非理想条件下的鲁棒性。

参考文献：

[1] 王容,李云翔,张爽,等.多功能 RIS 辅助隐蔽通信的无人机位置优化方法 [J]. 电子测量技术, 2026, 49(02): 45-56. DOI: 10.19651/j. cnki. emt.2518971.

[2] 杨龙,郭建道,周雨晨,等.无人机干扰辅助的反隐蔽通信方案研究[J].移动通信,2025,49(09):130-137.

[3] 孙景科.无人机辅助的空地 ISAC 隐蔽通信研究[D].山东交通学院,2025.DOI:10.27864/d.cnki.gsjtd.2025.000243.

[4] 任远,闫钰卓,张雪薇,等.RIS 和无人机辅助系统中隐蔽传输速率最大化方案[J].西安邮电大学学报,2025,30(03):30-39.DOI:10.13682/j.issn.2095-6533.2025.03.004.

[5] 袁伟杰,伍军,时玉叶.基于多无人机协作通感一体化的隐蔽通信设计[J].雷达学报(中英文),2025,14(04):797-808.

[6] 宋鑫康,王翔,李信,等.基于混合 RF/FSO 链路的无人机隐蔽通信策略[J].光学学报,2025,45(08):92-103.

[7] 刘学敏,钱玉文,宋耀良,等.一种基于无人机与智能反射面的隐蔽通信系统研究[J].电子与信息学报,2025,47(02):386-396.

[8] 国明乾.基于深度强化学习的无人机辅助隐蔽通信研究[D].福州大学,2023.DOI:10.27022/d.cnki.gfzhu.2023.001695.

[9] Gu M ,Su Y ,Ma Z , et al.UAV-Assisted Covert Communication with Dual-Mode Stochastic Jamming[J]. Sensors, 2026, 26(2): 624-624. DOI: 10.3390/S26020624.

[10] Yang H ,Liu Y ,Li X , et al.Physical layer security and covert communication in UAV-ISAC networks: A comprehensive survey[J].Journal of King Saud University Computer and Information Sciences, 2025, 37 (10):312-312.DOI:10.1007/S44443-025-00291-0.

[11] 白恒志, 王海超, 李国鑫, 等. 无人机隐蔽通信网络研究综述[J]. 电信科学, 2024, 39(8): 1-16.

[12] 胡锦松, 吴林梅, 束锋, 等. 无人机中继协助的有限码长隐蔽通信[J]. 电子与信息学报, 2022, 44(3): 1006-1013.

[13] Emani R. Cybersecurity Analysis and Defense of the MAVLink UAS Protocol[J]. 2024.

[14] Allouch A, Cheikhrouhou O, Koubâa A, et al. MAVSec: Securing the MAVLink protocol for ardupilot/PX4 unmanned aerial systems[C]// 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC). IEEE, 2019: 621-628.

[15] Tufekci B, Arslan A, Tunc C, et al. Enhancing the security of the mavlink with symmetric authenticated encryption for drones[C]//2024 11th International Conference on Internet of Things: Systems, Management and Security (IOTSMS). IEEE, 2024: 58-65.

[16] Khan N A, Jhanjhi N Z, Brohi S N, et al. A secure communication protocol for unmanned aerial vehicles[J]. CMC-Computers Materials & Continua, 2022, 70(1): 601-618.

[17] Xu H, Zhang H, Sun J, et al. Experimental analysis of MAVlink protocol vulnerability on UAVs security experiment platform[C]//2021 3rd International Conference on Industrial Artificial Intelligence (IAI).

IEEE, 2021: 1-6.

[18] Veksler M, Akkaya K, Uluagac S. Catch me if you can: Covert information leakage from drones using mavlink protocol[C]//Proceedings of the 19th ACM Asia Conference on Computer and Communications Security. 2024: 902-914.

[19] Wang R Z, Lin C F, Lin J C. Image hiding by optimal LSB substitution and genetic algorithm[J]. Pattern recognition, 2001, 34(3): 671-683.

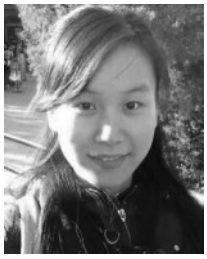
[20] Karim S M M, Rahman M S, Hossain M I. A new approach for LSB based image steganography using secret key[C]//14th international conference on computer and information technology (ICCIT 2011). IEEE, 2011: 286-291.

[21] Dumitrescu S, Wu X, Wang Z. Detection of LSB steganography via sample pair analysis[C]//International workshop on information hiding. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002: 355-372.

[22] Jung K H, Yoo K Y. Steganographic method based on interpolation and LSB substitution of digital images[J]. Multimedia Tools and Applications, 2015, 74(6): 2143-2155.

[23] Zhang T, Ping X. A new approach to reliable detection of LSB steganography in natural images[J]. Signal processing, 2003, 83(10): 2085-2093.

[作者简介]



黄冬艳 (1984–),女，广西南宁人，桂林电子科技大学副教授，硕士生导师，主要研究方向为区块链性能分析、隐蔽通信、区块链共识算法及物联网。

黄珉 (2001–)，男，广西南宁人，桂林电子科技大学硕士生，主要研究方向为区块链隐蔽通信。