# 基于压缩感知的船舶通信反探测系统

李 田[1*]
LI Tian

**摘 要** 随着电磁环境越来越复杂，船舶位置、航线、货物等信息在通信过程中面临的窃取风险也随之提升，商业机密与隐私泄漏的可能性越来越大。为此，在优化 AES-256 加密算法的基础上，结合压缩感知的稀疏性与随机性特征，文章提出了一种基于压缩感知的船舶通信加密反探测技术。该技术一方面提升了通信系统的抗截获与抗干扰能力，另一方面通过降低信号的可预测性来增强加密的鲁棒性，从而有效抵御黑客的解密攻击。仿真实验表明，在复杂电磁对抗场景下，该技术能明显提升通信的安全性与反探测性能，为船舶通信提供了可靠的技术支撑。

**关键词** 压缩感知；反探测技术；加密算法；船舶通信

doi：10.3969/j.issn.1672-9528.2026.04.034

## 0 引言

船舶通信是船舶间、船舶与港口等各类岸上通信站间进行目标坐标、航向、航线等多类敏感信息交换与互动协作的重要通道，也是船舶内部各部门间信息共享的重要平台[1]。得益于“数字航海”战略高速发展与“智慧航运”技术全球推进，船舶功能、种类、吨位不断发生变化，电子化、自动化程度越来越高，船舶通信安全性与可靠性面临的考验也随之增大。为保障船舶航行基础，保护海上人员及财产安全，必须确保船舶在任何情况下都可进行无干扰的通信联系。

现行船舶通信主要通过甚高频（VHF）、卫星、水下声学通信等方式实现。包括甚高频（VHF）在内的无线电通信系统，覆盖范围广，适应多种通信环境[2-3]，缺陷在于易受跳频攻击、硬件恐慌攻击或拒绝服务攻击令应答器失效，外界人员可能通过信号定位追踪船舶位置致敏感信息泄露[4-5]；卫星通信凭借卫星链路实现远距离通信的方式尤其适用于远洋航海行动，但卫星系统易受攻击并存在信号中断影响，可靠性存在隐患[6-7]；水下声学通信利用声波低失真度在水下传输信息，劣势在于传输速率相对易受洋流因素影响，且可能被高精度声纳探测，隐蔽性有限[8]。早期通信设备常以独立工作设备的形式出现于船舶中，伴随电子技术高速发展，独立工作单元逐渐被集成化通信网络替代，如何使用反探测加密算法对同一系统中各站点上报的大量错综复杂的通信数据进行综合分析处理，同时防止黑客攻击或病毒感染导致数据资料泄露是未来船舶通信发展的重要方面。

1. 海军装备部 陕西西安 710000

## 1 传统反探测加密算法

海上通信系统主要受到四类攻击动机，分别为直接盗取金钱、（非法）移动船只、窃取数据资料、造成航期延误[9]。国际海事组织（IMO）明确要求船舶需建立安全通信体系以应对船舶通信安全威胁，而加密算法作为信息安全体系的核心防线，其重要性在船舶通信领域日益凸显。如隐写术加密通信[10]在隐藏信息容量和载体质量间寻找平衡，通过载体源的选取与嵌入将重要敏感信息隐藏于公开信息的冗余部分，如果第三方精确区分出了载体对象和伪装对象，安全性将大大降低；量子加密通信（QKD）[11]基于量子力学分发获取一对完全随机且只有通信双方了解的量子密钥，因其无法兼容当前的通信网络，量子密钥的使用前提必须架设专用 QKD 网络，由此提供理论上不可破解的安全性；扩频通信在数据链中扩展原始信号的频谱，发送端采用直接序列跳频等跳频技术进行原始信号调制，将原始信号能量分散在宽频带上从而降低功率谱密度，在频谱有限的情况下将会引发频段冲突和自干扰。

高级加密标准（advanced encryption standard, AES）[12-13]作为 NIST 于 2001 年发布的一种对称分组双向加密算法，总共分为 128 位、192 位、256 位三种长度密钥，10 轮、12 轮、14 轮迭代轮数，基本运算包括 3 个代替和 1 个混淆在内的四个阶段，涉及字节替代、行移位、列混淆和轮密钥加操作来确保机密性，其中 AES-256 使用 256 位密钥对明文全量划分后的各 128 位明文块加密，轮密钥加中原数据与该次轮密钥做 XOR 运算，而每轮次密钥由种子密钥经过密钥扩展算法得到，因其高安全性和高效计算特性广泛应用于涉密通信，其在船舶通信应用方面主要存在两方面局限性，一是对原始

数据量要求较高，为维持船舶通信较短传输时间和较强的信息强度，原始数据需要压缩为更小的数据包；二是 AES-256 不适用于带宽有限的通信场景，在远洋航行的船舶通信中水下声学信道带宽有限。船舶通信数据产生过程与储存过程的传输步骤同样面临着数据窃取的风险，面对信息泄露威胁，AES 虽不直接属于反探测算法，但可以作为反探测系统中一个组成部分与其他技术结合使用，作为辅助加密工作帮助船舶通信实现更全面的安全保护。

## 2 基于压缩感知的 AES 反探测加密算法

AES 算法局限性显而易见，考虑到如何达到原始数据量要求并深度加密，压缩感知（compressed sensing, CS）可融入其中弥补缺陷。突破了奈奎斯特采样定理的约束，压缩感知根据信号在变换域（如小波变换）呈现的稀疏性，将高维信号通过观测矩阵投影至低维空间内，而后优化算法（如基追逐法）负责恢复数据，从少量测量值重建原始信号 [14-16]，该复合操作在传输较少数据的同时提供了较高有效信息，完成了边压缩边加密的双重安全保障。压缩感知观测信号可表示为：

$$\boldsymbol{Y}=\boldsymbol{\Phi}\cdot\boldsymbol{X}=\boldsymbol{\Phi}\cdot\Psi\cdot\boldsymbol{z} \tag{1}$$

式中：$\boldsymbol{X}$ 为原始信号（$N\times1$）；$\Psi$ 为稀疏基；$\boldsymbol{z}$ 为稀疏系数向量；$\boldsymbol{\Phi}$ 为测量矩阵（$M\times N$，$M<N$），原始信号重建通过利用 0 范数下的优化问题实现。

在压缩感知框架下对 AES-256 算法内核进行重构，船舶信号发送端首先将通信信号做稀疏化变换，转换为压缩感知后的低维度散列编码，随后通过 AES 算法配合 256 位密钥完成加密处理。信号采集过程中同步实现压缩，既降低了存储空间，也提高了有效信息的占比。发送端的具体流程如下：

（1）稀疏化处理。采用离散小波变换等方式，本研究把 $N$ 维原始信号 $\boldsymbol{X}$ 在 $N\times N$ 型的稀疏变换基下完成转化，生成稀疏度为 $k$ 的 $N$ 维稀疏向量 $\boldsymbol{z}$，表示为 $\boldsymbol{X}=\Psi\cdot\boldsymbol{z}$。稀疏系数向量 $\boldsymbol{z}$ 中有效数据的含量高于 $N$。

（2）压缩感知编码。原始信号 $\boldsymbol{X}$ 在 M×N 型测量矩阵 $\boldsymbol{\Phi}$ 的作用下，投影压缩为 $M$ 维测量向量 $\boldsymbol{Y}$，压缩后的数据长度比原始长度要小得多。$\boldsymbol{\Phi}$ 是数据接收端重建原始信号的必要条件，保存后可作为附加密钥来增强系统的安全性。

（3）AES-256 加密。首先将测量向量 $\boldsymbol{Y}$ 拆分为 128 块密文，叠加 AES-256 算法生成密码 $C$，$C=E_k(\boldsymbol{Y})$。其中，$E_k$ 表示使用 256 位密钥 $k$ 的 AES-256 加密操作。

船舶信号接收端流程包括：

（1）AES-256 解密。信号接收端掌握密钥 $k$ 进行解密，恢复测量向量 $\boldsymbol{Y}$，$\boldsymbol{Y}=D_k(C)$。其中，$D_k$ 是 AES-256 解密操作，为 $E_k$ 对称型逆运算过程。

（2）信号重建。利用已知的测量矩阵 $\boldsymbol{\Phi}$ 和稀疏基 $\Psi$，根据 $\boldsymbol{Y}=\boldsymbol{\Phi}\cdot\Psi\cdot\boldsymbol{X}$，通过求解范数最小化问题重建稀疏系数 $\boldsymbol{z}$，随后通过 $\boldsymbol{X}=\Psi\cdot\boldsymbol{z}$ 恢复原始信号。

基于压缩感知的 AES 反探测加密算法在信号传输的过程中完成信号压缩，在减少带宽需求的前提下提高了传输效率，处理后的信号在遗漏测量矩阵 $\boldsymbol{\Phi}$ 的前提下无法重构，通过 AES 自身附加的混淆步骤，令船舶通信信号被分析或识别的难度增大，被检测到的风险越来越低，船舶通信信号的安全性和稳定性可得到进一步的保障。

## 3 仿真实验结果分析

### 3.1 仿真平台搭建

为了深入分析和验证压缩感知式 AES 船舶通信反探测系统性能和效率，本研究在 PyCharm2025.1.3.1 开发环境中应用 Python 编程语言搭建了一套具有较高保真度的仿真平台，使用 Matlab/Simulink 外部自定义船舶航行通信环境，整体架构如图 1 所示。

具体包括以下五个关键模块：

（1）通信建模模块。该模块需要构建船舶信号源、调解器、滤波器等组部件，共同组成船舶通信系统模型单元，模拟输出船舶通信测试数据；

（2）稀疏变换模块。该模块将测试信号在小波变换作用下稀疏化，它的作用主要是降低压缩感知后 AES 反探测加密算法计算复杂度，从而减轻信号两端数据的传输负担；

（3）压缩编码模块。该模块将压缩感知编码集成至仿真平台，根据原始信号随机生成观测矩阵，将高维度的原始稀疏信号压缩为低维度的测量值，隐藏观测矩阵为附加密钥；

（4）加密处理模块。利用 AES-256 算法进行数据加密，每轮次密钥都需要安全保管储存，确保数据在传输过程中的机密性，该模块为基于压缩感知的反探测系统核心要点；

（5）解密与重建模块。经反探测系统处理后的密文数据先通过对称密钥转换为可读模式，再通过求解范数最小化问题恢复原始信息。

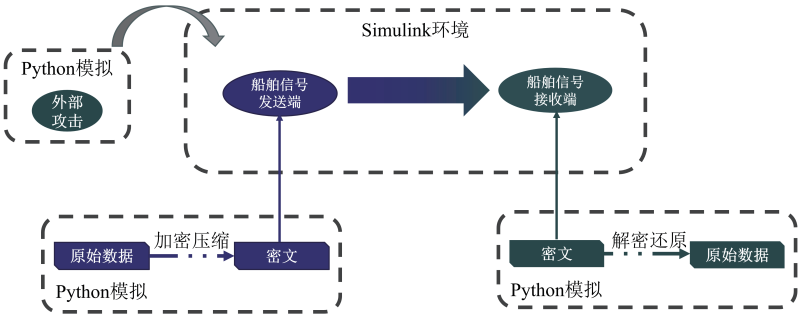


图 1 仿真平台架构图

3.2 仿真可靠性验证

利用 Python 脚本实现基于压缩感知的 AES-256 加密算法，于 simulink 的仿真环境中模拟船舶通信流程控制，在信号传输过程中捕获传输密文或篡改传输密文是干扰通信信号的最佳方式，故本文针对发送端发送密文及传输密文过程，分别添加暴力破解、差分密码分析、线性密码分析、已知明文攻击四种攻击类型，以第三方视角重建或破坏信息运输，收集不同攻击下计算复杂，抵御攻击能力如表 1 所示。

表 1 不同攻击类型下改进前后的计算复杂度

| 攻击类型 | 传统 AES-256 复杂度 | 改进算法复杂度 |
|---|---|---|
| 暴力破解 | 2^255 | 2^255 |
| 差分密码分析 | 2^140 | 2^(140+*N*) |
| 线性密码分析 | 2^150 | 2^150 |
| 已知明文攻击 | 2^256 | 2^(256×*N*) |

表 1 中，*N* 为测量矩阵 $\boldsymbol{\Phi}$ 的维度，基于压缩感知的 AES 反探测算法继承了 AES-256 的加密强度，将引入的测量矩阵 $\boldsymbol{\Phi}$ 作为额外密钥传输给信号接收方，外界对于信号的破解成功率小于千分之一，且篡改原始数据的难度极高。已知明文攻击中，假设攻击者拥有部分明文通信内容及对应密文，试图推断反探测算法的加密密钥，在这种不安全的传输环境内，攻击者依然需猜测 2^(256×*N*) 种组合才有可能破解原始数据，远超传统 AES-256 加密算法破解成本。

以研究基于压缩感知的 AES-256 加密算法安全性为目的，不断更改船舶信号发送端压缩率和稀疏度，探讨发送端压缩率与第三方检测概率的联系、发送端稀疏度与第三方重建精度的关系，结果如图 2 所示。

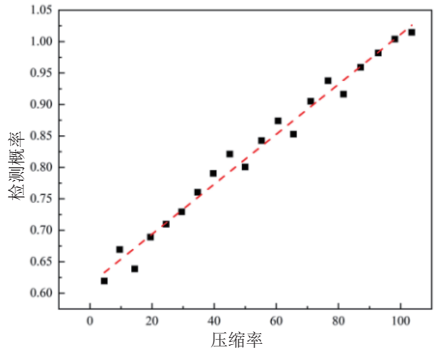


图 2 检测概率与压缩率的关系图

本文提出了一种压缩感知式 AES-256 加密算法，算法的压缩率越高，检测概率也越高，拟合结果斜率为正，$R^2$ 接近 0.95，可表明算法的强相关性。在持续提升船舶信号发送端的压缩率后，传输信号数据量显著减少，信号隐蔽性相对提升，相对于未进行压缩的 AES 反探测系统，敌方检测概率降低约 30%。

信号稀疏性是稀疏重建的前提，压缩感知中证明稀疏度越高的原始信号可在较高重建精度下尽可能减少采集成本和复杂度，然而过高的稀疏度可能会导致原始数据丢失。不断更改压缩感知稀疏矩阵特征数的尺寸，比较重建消息与原始消息相似度，如图 3 所示，船舶信号接收端在 60% 的稀疏性条件下，重建精度接近 100%，可确保重建信息完整性。

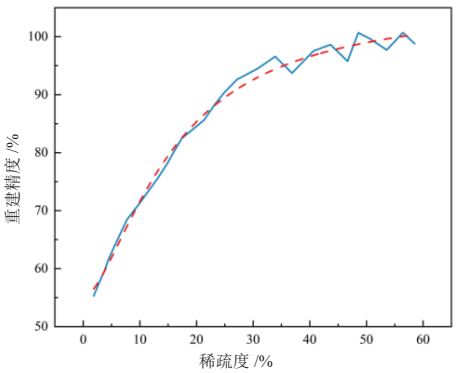


图 3 重建精度与稀疏度的关系图

## 4 结语

本研究从船舶通信的重要性切入，讨论了当前面临的信息安全挑战，系统分析了现有船舶通信风险，把压缩感知理论概念引入 AES-256 加密框架当中，集成了一种具备反探测能力的船舶通信加密算法。该方法能够压缩数据信号、降低信号被检测的可能性，并维持高强度的加密性能，从而达到提升通信隐蔽性同时兼顾安全性的目的。利用 Python 脚本进行仿真，结果表明，本研究的算法在加密强度、检测概率及重建精度方面都展示出了明显的优势。下一步，围绕重建算法优化，就可以增强其在复杂环境下的适应能力，最终为船舶通信提供更为可靠的技术支撑。

**参考文献：**

[1] 王玲，张彬祥．船舶通信导航技术及发展趋势 [J]. 舰船电子工程，2016,36(3):17-21.

[2] 金伟．船用甚高频无线电话的通信质量研究 [J]. 信息通信，2019(4): 171-174.

[3] 刘浪．船舶数字通信的分布式入侵防御系统构建 [J]. 舰船科学技术，2023,45(19):165-168.

[4] 黄智颖，冯新喜，张焕国．高级加密标准 AES 及其实现技巧 [J]. 计算机工程与应用，2002(9):112-115.

[5] 吴中岱，韩德志，蒋海豹，等．海洋船舶通信网络安全综述 [J]. 计算机应用，2024,44(7):2123-2136.

[6] 张振东，田建宇．船载卫星通信天线跟踪误差自动补偿研究 [J]. 舰船科学技术，2022,44(9):146-149.

[7] 张海勇，刘冠邑，马迁．海上卫星通信遮挡预报模型研究 [J]. 舰船科学技术，2019,41(21):160-164.

# 面向国土调查的高分遥感与 GIS 一体化地类识别方法研究

李 臻 [1]
LI Zhen

**摘 要** 针对 1:10 000 国土调查对高精度地类识别的迫切需求，文章构建了一种融合高分遥感影像与 GIS 矢量规则的一体化识别方法。研究以 GF-2 与 GF-6 影像为基础，融合图斑、坡度、权属等 GIS 要素，设计了包括多尺度特征提取、GIS 约束规则库、自适应融合模型在内的完整识别体系，实现遥感光谱—纹理与 GIS 拓扑—属性的深度协同。通过构建 ResNet50 与 Node2Vec 的联合特征表达，采用 RF-SVM 集成模型提升分类精度，并将空间邻接规则嵌入分类过程。实验在长三角典型区域开展，地类分类精度超过 95%，显著优于传统像素法与深度学习模型，验证了所提方法在复杂地貌与破碎斑块下的泛化能力，具备推广价值。

**关键词** 高分遥感；GIS 约束；地类识别；特征融合；集成分类模型

doi：10.3969/j.issn.1672-9528.2026.04.035

## 0 引言

为支撑“三条控制线”划定与耕地保护考核，我国于 2018 年启动新一轮 1:10 000 国土调查，并对高精度地类识别提出了更高要求 [1]。然而，面对高分辨率遥感数据与复杂地表形态，传统人工解译与纯像素算法存在精度瓶颈，GIS 约束信息未被有效利用，导致错分率居高不下 [2]。2022 年《国土变更调查技术指南》提出“AI+GIS”融合范式，要求突破遥感与 GIS 数据的异构壁垒，实现地类要素的精细识别 [3]。本文正是在此背景下，构建遥感与 GIS 协同处理体系，融合图像特征与地理规则，提升国土调查中耕地、园地等关键地类的识别精度。

1. 甘肃省地质矿产勘查开发局第四地质矿产勘查院
甘肃酒泉 735000

## 1 融合识别关键技术难点

当前国土调查工作中遥感影像与 GIS 数据融合仍面临多重技术挑战。首先，遥感数据为规则栅格格式，GIS 数据为不规则矢量格式，二者在空间基准、数据结构与语义粒度上存在本质差异，导致特征难以直接对齐与拼接。其次，现有分类模型多为端到端视觉模型，难以表达耕地连片性、园地

[8] 李建瑜 , 崔杰 . 基于傅里叶扩压频调制技术的水声通信 [J]. 声学技术 , 2024,43(5):661-667.
[9] 吴笑风 , 许攸 . 海上网络安全 : 航运与船舶工业的跨界挑战 [J]. 中国船检 ,2017(7):42-44.
[10] 赵佳颖 , 李加洪 , 洪涛 , 等 . 面向潜艇卫星隐蔽通信场景下的数字图像隐写技术综述 [J]. 舰船电子工程 , 2021, 41(7): 119-123.
[11] 钟海 , 叶炜 , 吴晓东 , 等 . 基于光前置放大器的量子密钥分发融合经典通信方案 [J]. 物理学报 , 2021,70(2):304-311.
[12] 何明星 , 林昊 .AES 算法原理及其实现 [J]. 计算机应用研究 , 2002(12): 61-63.
[13]NIST.Advanced Encryption Standard（AES）[M].Federal information Processing Standards Publication, 2001.
[14] 金坚 , 谷源涛 , 梅顺良 . 压缩采样技术及其应用 [J]. 电子与信息学报 ,2010,32(2):470-475.
[15]CANDÈS E J, WAKIN M B.An introduction to compressive sampling[J]. IEEE signal processing magazine, 2008, 25(2): 21-30.
[16] 戴琼海 , 付长军 , 季向阳 . 压缩感知研究 [J]. 计算机学报 , 2011, 34(3):3425-3434.

【作者简介】
李田（1996—），通信作者（email:litiannn@foxmail.com），女，山东寿光人，硕士研究生，助理工程师，研究方向：质量监督、水中兵器、加密算法、船舶通信。

（收稿日期：2025-08-28 修回日期：2026-04-07）