研究与开发

基于混沌序列的无线水印物理层安全认证技术

陈松林

（中国电子科技集团公司第十研究所，四川 成都 610036）

摘　要：近年来，低空域的网联飞行器数量呈指数性增长，无线网络的开放性及广播性，使得未授权恶意节点更容易伪装成合法飞行器发起欺骗攻击与航线篡改，威胁低空产业的安全运转。传统单纯依靠特定密码算法难以抵御高强度、高算力的密码破解攻击，急需一种低成本、隐蔽认证方案来保障低空智联网安全。提出一种基于混沌序列的无线水印物理层安全认证算法，利用Tent-Map混沌系统生成极难破解的扩频射频水印信息和载体信息一同传输，实现业务数据安全传输，同时不占用系统额外的频带资源即可完成物理层身份认证。仿真实验分析，该方法能够在不同调制方式下嵌入扩频射频水印信息，通过调整水印功率系数显著提升物理层安全认证性能。

关键词：混沌系统；低空经济；无线物理层安全认证；扩频水印

中图分类号：TP393

文献标志码：A

doi: 10.11959/j.issn.1000−0801.2025129

Chaotic sequences based watermarking wireless physical layer security authentication algorithm

CHEN Songlin

The No.10 Institute of China Electronics Technology Group Corporation, Chengdu 610036, China

Abstract: In recent years, wireless mobile consumers have also grown exponentially. Due to the openness and broadcasting of the wireless networks, it is easier for unauthorized users to disguise themselves as legitimate users to launch spoofing attacks, resulting in insecurity in the low-altitude industry. Relying on specific cryptographic algorithms alone in the tradition was difficult to cope with password cracking abilities of high-intensity and high-computility. Meanwhile, a secure mechanism for covert communication was urgently needed. A chaotic sequences based watermarking wireless physical layer security authentication algorithm was proposed. This algorithm utilized the transmission of chaotic watermark and carrier information together to achieve covert transmission of service data, and physical layer identity authentication was completed without occupying additional frequency band resources of the system. Through analysis of simulation experiments, this method could embed watermark information by using different

收稿日期：2024−12−01；**修回日期：**2025−05−07

通信作者：陈松林，songlinch0061@163.com

基金项目：国家自然科学基金青年项目（No.62302082）

Foundation Items: The National Natural Science Foundation of China Youth Project (No.62302082)

modulation methods, and the physical layer security authentication performance was significantly improved via adjusting the watermark power coefficient.

Key words: chaotic system, low-altitude economy, wireless physical layer security authentication, spectrum watermarking

0 引言

随着低空经济的快速发展，低空空域逐渐成为各国经济发展和技术创新的重要领域。低空经济涵盖了无人机、通用航空、低空物流、空中游览等多个应用场景，并催生了大量的新兴商业模式与技术突破。然而，在低空经济蓬勃发展的同时，其背后所依赖的网络系统、通信链路、数据处理能力也面临着日益严峻的网络安全挑战。

低空经济的运行高度依赖智能化、信息化、网络化技术。无人机的远程控制、飞行数据的实时传输、地空通信网络、基于人工智能的自动驾驶决策，均需要通过高度互联的网络进行支持。然而，这种复杂的网络环境也使得低空经济面临多种潜在的网络安全威胁。例如，无人机通信链路可能遭受信号干扰或恶意劫持，飞行数据可能被窃取或篡改，甚至无人机群体的自主飞行控制系统可能遭遇分布式拒绝服务攻击，导致严重的安全事故[1]。此外，低空网络环境具有节点分布广、动态变化快、异构性强等特点，传统的网络安全防护手段难以满足这一新兴领域的需求。

基于以上背景，低空经济中的网络安全问题不仅是技术挑战，更是关乎工业发展和国家安全的重要议题。研究如何构建适应低空经济需求的网络安全技术，对提升低空经济的安全性、稳定性、可持续发展具有重要意义。因此，本文将以低空经济为背景，探讨适应低空环境的网络安全技术与策略，为低空经济的安全发展提供理论基础和实践指导。

目前，针对通信系统的安全机制主要依赖于传统密码学，且集中于计算机网络协议栈的应用层通过用户身份的索引方式构建对称密钥安全架构[2-3]。6G通信系统对网络时延、传输可靠性提出了更高的要求，当前的安全机制受限于通信速率与计算复杂度之间的矛盾[4]。由于传统密码学的高强度加密需复杂运算，如李维斯特-沙米尔-阿德曼算法（Rivest-Shamir-Adleman algorithm，RSA）、椭圆曲线密码学（elliptic curve cryptography，ECC），实时认证时延难以满足6G毫秒级要求，而轻量化密码算法（如轻量级AES）虽能降低时延，却容易被高算力节点破解，形成“安全-效率”失衡。例如，低空飞行器在密集航线中需频繁认证，若加密耗时超过信道切换周期（如5 ms），将引发通信中断或航线冲突。因此，当前急需一种增强安全手段与之对抗。

传统数字水印技术主要被应用到影像、声音、视频等多媒体信息的版权保护中，该技术主要是将有特殊含义的信号、文字、图像嵌入原始载体文件中，并不影响原始语音、图像文件的质量。当版权受到侵犯时，版权所有者能通过提取水印来达到保护原创作品的目的[5-7]。

本文将传统数字水印技术引入无线网络中，作为一种增强无线物理层安全认证机制，可应用于复杂电磁环境中的频谱管理、基站终端无线认证管理、广播管理系统[8]。该方法可通过提取水印对数据进行完整性认证，保证数据在传输过程中的完整性、真实性防篡改检测，实现较小开销的设备认证，适用于资源高度受限的无线网络环境。文献[9]针对二进制相移键控（binary phase shift keying，BPSK）调制的通信系统提出了一种嵌入式物理层认证方案，利用信号的实部对信号进行鉴别。文献[10]通过设计具有身份认证功能

的时分多址组网协议，在信息帧的介质访问控制层嵌入水印标签以完成用户入网身份认证。这些方法采用的算法需要计算复杂的协议，并且标识的唯一性较差，硬件实现所需资源多，所以上述方法无法保证认证的实时性。文献[11]中提出一种基于扩频的频谱水印嵌入方法，虽然该方法将扩频码调制为频谱水印易于实现，但是存在严重依赖于扩频码的选择问题，且该文献并未推导虚警率相关表达式，也没有讨论不同数字调制下算法的适应性。综上所述，当前大部分采用嵌入水印的无线认证技术所进行的数据完整性认证方案依然存在复杂度高[9]、数据利用率低[10]、虚警率过高[12]、水印提取困难[14]、受噪声影响大[15]等问题，而且缺乏分析嵌入水印功率在不同数字调制下的性能分析。

本文提出基于混沌序列的无线水印安全认证技术，该技术能在无线信号中嵌入不被察觉的微弱水印信息作为唯一身份标识以实现隐蔽认证。此外，对于水印信息的映射由离散混沌系统产生以增强水印信息的不可预估性，从而进一步提高水印信息的不可破解性。该方法可以以低成本的方式在资源受限的低空智联网中实现。

1　射频水印生成

射频水印是一种信息隐藏技术，能将不可见的微弱信号嵌入通信信号中，以实现安全通信。本文提出的一种基于混沌序列的无线水印生成方法，射频水印生成流程如图1所示，主要包括混沌水印序列生成与扩频射频水印生成两部分。生成的射频水印经历脉冲成形，载波调制后与原始通信信号嵌入后，其通信信号的质量不受显著影响。

1.1　混沌水印序列生成

混沌序列是根据在非线性动态系统中出现的确定性的、类似随机过程的混沌现象所产生的一系列非周期、不收敛的伪随机序列。离散时间的混沌系统有Logistic、Tent、Chebyshev。混沌系统对初始值非常敏感，基于这一特性能产生一系列的非相关、类随机再生序列，其不具备周期性，因此具有相当程度的保密性，难以破译。本文的原始水印信息由混沌系统Tent-Map生成，作为原始混沌水印序列，该方式有助于提升水印的难破解性。

基于Tent-Map的混沌系统迭代计算式如下所示。

$$x_{k+1}=\begin{cases}\dfrac{x_k}{a}, & 0<x_k<a\\ \dfrac{1-x_k}{1-a}, & a\leqslant x_k\leqslant 1\end{cases} \tag{1}$$

其中，$0<a<1$。

假设给定式（1）一个初始值x_0，就能生成一个混沌序列$\boldsymbol{x}=\{x_m\},m=1,2,\cdots,M,0<x_m<1$，该序列在区间（0,1）上的概率密度分布是均匀的，均值为0.5。令初始水印信息种子$\boldsymbol{w}=\boldsymbol{x}$，其中，$\boldsymbol{w}=\{w_m\},m=1,2,\cdots,M,0<w_m<1$由混沌序列

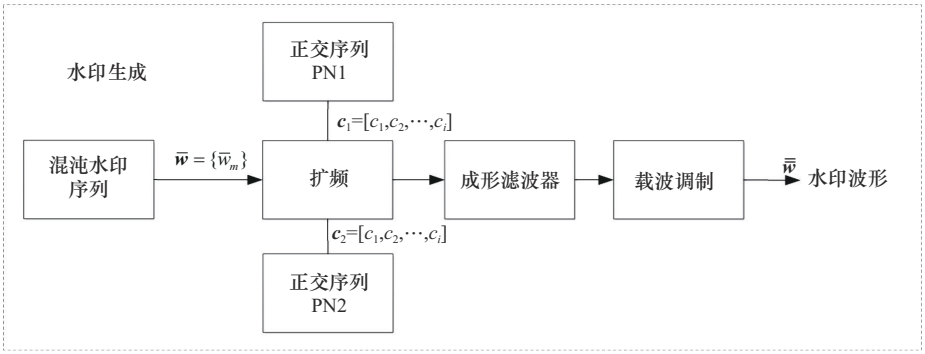


图1　射频水印生成流程

$\boldsymbol{x}$生成，其值为0到1浮点数。针对浮点数向量$\boldsymbol{w}$，设定固定门限值$\eta_1, 0<\eta_1<1$。

$$\bar{w}_m=\begin{cases}0, & 0<w_m<\eta_1\\ 1, & \eta_1\leqslant w_m\leqslant 1\end{cases} \tag{2}$$

其中，$\bar{w}_m\in\{0,1\}$。

即初始水印信息种子$\boldsymbol{w}=\{w_m\}, m=1,2,\cdots,M$, $0<w_m<1$中将大于门限值η_1的混沌值设为1，其余混沌值设为0，得到取整向量混沌水印信息$\bar{\boldsymbol{w}}=\{\bar{w}_m\}, m=1,2,\cdots,M, \bar{w}_m\in\{0,1\}$。

1.2 扩频射频水印生成

扩频通信系统具有很强的抗干扰、抗窄带干扰、抗多径干扰能力。扩频通信指待传输信息信号的频谱用某个特定的扩频函数（与待传输的信息信号无关）扩展频谱后成为宽频带信号，其信号带宽得到幅度延扩，信号强度大幅下降，随后通过信道进行传输。接收端再利用相应的方式将扩展的频谱完成压缩，恢复为原来待传输信息的带宽，该技术在CDMA中获得广泛应用。本文将第1.1节中的混沌水印信息进一步以特定的扩频方式形成扩频射频水印信息，扩频射频水印生成过程如图2所示。

（1）扩频正交PN1、PN2序列生成。为保证水印的检测与提取及认证率，本文构造相互正交的序列PN1、PN2，使两者互相关函数值为0。由于哈达玛矩阵$\boldsymbol{H}$为+1、−1元素组成的正交方阵，利用其任意两行（或两列）都是相互正交的特点构造PN1、PN2序列。首先，采用哈达玛矩阵$\boldsymbol{H}$分别迭代生成长度为l的2个相互正交序列c_1序列长度为$l=2^r, \boldsymbol{c_i}=[c_1,c_2,\cdots,c_l], c_i\in\{-1,1\}$，分别作为PN1、PN2序列。哈达玛矩阵递推关系如下。

$$\begin{aligned}\boldsymbol{H}_1&=\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\\ \boldsymbol{H}_2&=\begin{bmatrix}\boldsymbol{H}_1 & \boldsymbol{H}_1\\ \boldsymbol{H}_1 & -\boldsymbol{H}_1\end{bmatrix}\\ &\vdots\\ \boldsymbol{H}_r&=\begin{bmatrix}\boldsymbol{H}_{r-1} & \boldsymbol{H}_{r-1}\\ \boldsymbol{H}_{r-1} & -\boldsymbol{H}_{r-1}\end{bmatrix}\end{aligned} \tag{3}$$

取$\boldsymbol{H}_r$其中任意两列或任意两行，作为$\boldsymbol{c}_1$、$\boldsymbol{c}_2$，形成两个正交序列PN1、PN2，序列长度为l，$\boldsymbol{c}_{1,2}=[c_1,c_2,\cdots,c_l], c_i\in\{-1,1\}, i=1,\cdots,l$。

（2）扩频水印序列生成。利用生成的两个正交序列$\boldsymbol{c}_1$、$\boldsymbol{c}_2$，通过式（4）对混沌水印信息$\bar{w}$进行直接序列扩频得到扩频水印序列$\bar{\bar{\boldsymbol{w}}}=\{w_{22}(i)\}$, $w_{22}(i)=\{0,1\}$。

$$\bar{\bar{\boldsymbol{w}}}=\{w_{22}(i)\}=\begin{cases}\bar{\boldsymbol{w}}\{w_{21}(i)\}\otimes\boldsymbol{c}_1, & w_{21}(i)=0\\ \bar{\boldsymbol{w}}\{w_{21}(i)\}\otimes\boldsymbol{c}_2, & w_{21}(i)=1\end{cases} \tag{4}$$

其中，⊗代表直接序列扩频过程，水印扩频前水印信息为$w_{21}(i)$，水印信息扩频后的扩频水印值为$w_{22}(i)$。

（3）扩频射频水印信号生成。将生成的扩频水印序列$\bar{\bar{\boldsymbol{w}}}$代入式（5），经过成形滤波器形成脉冲波形。

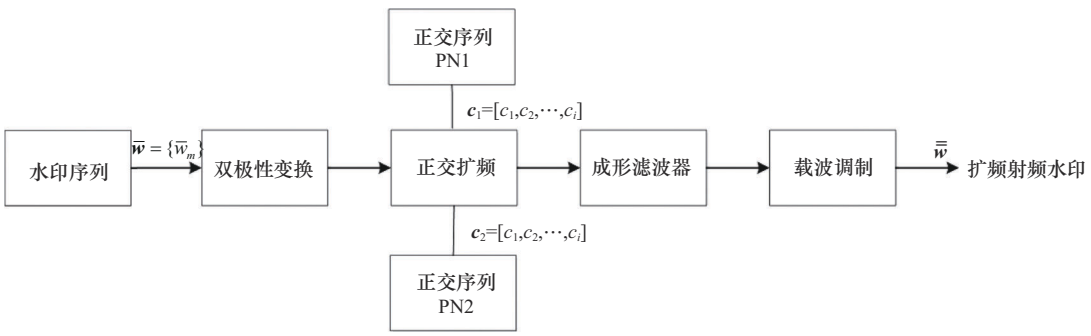


图2 扩频射频水印生成过程

$$X(f)=\begin{cases}T_s, 0\leqslant|f|\leqslant\dfrac{1-\alpha}{2T_s}\\ \dfrac{T_s}{2}\left\{1+\cos\left[\dfrac{\pi T_s}{\alpha}\left(|f|-\dfrac{1-\alpha}{2T_s}\right)\right]\right\}, \dfrac{1-\alpha}{2T_s}<|f|<\dfrac{1+\alpha}{2T_s}\\ 0,|f|>\dfrac{1+\alpha}{2T_s}\end{cases} \tag{5}$$

其中，α为滚降因子。最终，通过载波调制形成扩频射频水印信号，以待与原始通信信号进行嵌入。

2　扩频射频水印嵌入

本文所考虑的原始通信信号，通过信源编码、信道编码后再采用数字调制（包括BPSK、QPSK、8PSK、16QAM），成形滤波后，经过载波调制后与扩频射频水印嵌入，采用线性嵌入水印形式，扩频射频水印嵌入过程如图3所示。

对扩频后的水印信息完成成型滤波，形成发射波形，随后通过载波调制生成扩频射频水印信息$\bar{\boldsymbol{w}}$，再与基带信号$\boldsymbol{s}$进行线性叠加形成最终的发射信号$\boldsymbol{r}$：

$$\boldsymbol{r}=\boldsymbol{s}+\rho\bar{\boldsymbol{w}} \tag{6}$$

其中，ρ表示水印幅值系数，其值决定了水印信息的隐蔽性，水印幅值系数过大将增大原始通信信号恢复难度，影响基带误码率，水印幅值系数过小影响水印的检测与认证。此外，需选取信息的嵌入位置。考虑原始载体的长度比水印信息长，故实际选择水印线性叠加起始位在原始载体信息数据中间段。设原始载体数据长度为l_1，水印信息长度为l_2，水印线性叠加起始位为：

$$l_3=\frac{l_1-l_2}{2} \tag{7}$$

最终完成扩频射频水印与原始载体信息的嵌入。

3　扩频射频水印检测与提取

扩频射频水印的检测与提取关系到隐秘认证的性能，也决定着物理层安全认证的性能，合法接收方接收到未知信号$\boldsymbol{r}$后，执行载波解调，匹配滤波，再进行水印检测。如通过水印检测，则判决为合法发射方，进一步提取水印并移除，再执行抽样判决、解映射、还原出基带信号。否则，认证不通过，终止接收。扩频射频水印检测与提取过程如图4所示，主要通过对接收信号进行解扩、门限判决、水印提取、水印相似度对比认证构成。

图4　扩频射频水印检测与提取过程

3.1　扩频射频水印检测

本节首先确定二元假设检验模型，推导在假设H_0与H_1条件下的输出幅度$|y|$的概率密度函数。其次为了验证检测门限Γ的恒虚警性质，推导解扩后信号统计量变换下虚警概率P_{fa}，并得到阈值因子Γ与虚警概率P_{fa}的关系。最后推导了理论检测概率P_{d}。

（1）二元假设检验模型。假设噪声为加性高

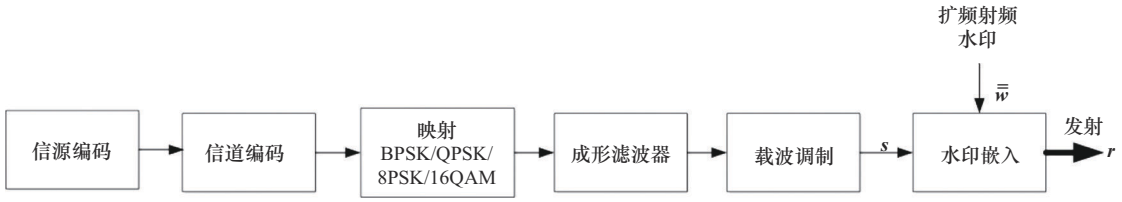


图3　扩频射频水印嵌入过程

斯白噪声$n(t)\sim N(0,\sigma_n^2)$，二元假设检验为：

$$\begin{aligned}H_0&:r(t)=x(t)+n(t)\\H_1&:r(t)=w(t)+x(t)+n(t)\end{aligned}\tag{8}$$

其中，H_0为无嵌入水印，H_1为嵌入水印，$x(t)$为基带信号，$w(t)$为水印信号。

（2）对接收信号进行解扩分析。对接收到的信号$\boldsymbol{r}$，按式（9）执行解扩：

$$\bar{\boldsymbol{r}}=\boldsymbol{r}\otimes\boldsymbol{c}_1\tag{9}$$

其中，$\bar{\boldsymbol{r}}$为解扩序列，$\boldsymbol{c}_1=[c_1,c_2,\cdots,c_l],c_i\in\{-1,1\}$，$i=1,\cdots,l$为PN1序列。代入二元假设检验模型后，展开$H_0$和$H_1$后得到：

$$\begin{aligned}H_0&:\boldsymbol{y}=\boldsymbol{x}\otimes\boldsymbol{c}_1+\boldsymbol{n}\otimes\boldsymbol{c}_1\\H_1&:\boldsymbol{y}=\boldsymbol{w}\otimes\boldsymbol{c}_1+\boldsymbol{x}\otimes\boldsymbol{c}_1+\boldsymbol{n}\otimes\boldsymbol{c}_1\end{aligned}\tag{10}$$

其中，由于$w(t)$含有$\boldsymbol{c}_1$和$\boldsymbol{c}_2$，由哈达玛矩阵$\boldsymbol{H}$产生的$\boldsymbol{c}_2$与$\boldsymbol{c}_1$正交近似为0，$\boldsymbol{w}\otimes\boldsymbol{c}_1$为扩频码能量。本文将解扩后幅度$|y|$作为检验统计量，同时避免了相关的干扰。

（3）解扩信号后统计量$|y|$构建与分析。假设H_0下的检验统计量为$|y|$，水印不存在时，噪声与$\boldsymbol{c}_1$独立，则接收信号为y。

$$\begin{aligned}&\boldsymbol{y}\sim N(0,\sigma_n^2E_c)\\&E_c=\sum_{n=1}^{N}\boldsymbol{c}_1^2[n]\end{aligned}\tag{11}$$

统计量$|y|$服从瑞利分布，概率密度函数（probability density function，PDF）为：

$$f_{x_i}(|\boldsymbol{y}||H_0)=\frac{|\boldsymbol{y}|}{\sigma_n^2E_c}\exp\left(-\frac{|\boldsymbol{y}|^2}{2\sigma_n^2E_c}\right)\tag{12}$$

累积分布函数（cumulative distribution function，CDF）为：

$$F_{x_i}(|\boldsymbol{y}||H_0)=1-\exp\left(-\frac{y^2}{2\sigma_n^2}\right)\tag{13}$$

假设$\mathcal{H}_1$下的检验统计量为水印存在时，对信号执行解扩后，接收信号。

$$\begin{aligned}&\boldsymbol{y}\sim N(\rho E_c,\sigma_n^2E_c)\\&E_c=\sum_{n=1}^{N}\boldsymbol{c}_1^2[n]\end{aligned}\tag{14}$$

统计量$|y|$服从莱斯分布，概率密度函数为：

$$f_{x_i}(|y||H_1)=\frac{|y|}{\sigma_n^2}\exp\left(-\frac{1}{2\sigma_n^2E_c}\left(|\boldsymbol{y}|^2+A^2\right)\right)\cdot I_0\left(\frac{A\cdot|y|}{\sigma_n^2E_c}\right)\tag{15}$$

其中，A为主信号幅度，$I_0(\cdot)$为修正的0阶第一类贝塞尔函数。

由上文H_0与H_1条件下得到统计量的概率密度函数，设定判决阈值Γ，统计量$z=|y|$，则$f_Z(z)$为不同恒虚警算法下的PDF，虚警概率P_{fa}[16]为统计量超过阈值的概率为：

$$P_{\mathrm{fa}}=\int_0^{\infty}f_Z(z)P\{|z|\geqslant\Gamma|H_0\}\mathrm{d}z=$$

$$\int_0^{\infty}f_Z(z)\int_{\Gamma}^{\infty}f_{x_i}(|\boldsymbol{y}||H_0)\mathrm{d}y\mathrm{d}z=\exp\left(-\frac{\Gamma^2}{2\sigma_n^2E_c}\right)\tag{16}$$

检测概率P_{d}[16]为莱斯分布下的积分，近似表达式为：

$$P_{\mathrm{d}}=\int_0^{\infty}f_Z(z)P\{|z|\geqslant\Gamma|H_1\}\mathrm{d}z=$$

$$\int_0^{\infty}f_Z(z)\int_{\Gamma}^{\infty}f_{x_i}(|\boldsymbol{y}||H_1)\mathrm{d}y\mathrm{d}z\approx Q\left(\sqrt{\frac{E_c}{\sigma_n^2}},\sqrt{\frac{2\Gamma}{\sigma_n^2E_c}}\right)\tag{17}$$

其中，Q函数表征信噪比与阈值的权衡关系。

（4）确定最优提取水印门限值：根据解扩序列$\bar{\boldsymbol{r}}$，与已知原混沌水印信息$\bar{\boldsymbol{w}}=\{\bar{w}_m\},m=1,2,\cdots,M,\bar{w}_m\in\{0,1\}$，求归一化系数（normalized coefficient，NC），如式（18）所示：

$$\mathrm{NC}=1-\frac{\sum_i\left(\boldsymbol{r}(i)-\bar{\boldsymbol{w}}(i)\right)^2}{\sum_i\boldsymbol{r}^2(i)}\tag{18}$$

本文实际通过遍历设定的水印提取门限值Γ_1，遍历范围为$-||\boldsymbol{c}_1||<\Gamma_1<||\boldsymbol{c}_1||$，$||\boldsymbol{c}_1||$为PN1

序列的模值。当NC最大时，取此时的最优值作为最佳提取水印门限值。

3.2　扩频射频水印提取

（1）水印提取分析。根据最优水印门限值Γ_1，按照式（19）提取出水印信息。

$$\hat{\boldsymbol{w}}_m=\{w_m\}=\begin{cases}0, 0<w_m<\Gamma_1\\ 1, \Gamma_1\leqslant w_m\leqslant 1\end{cases} \tag{19}$$

其中，$-\|\boldsymbol{c}_1\|<\Gamma_1<\|\boldsymbol{c}_1\|$。估计的水印信息为$\hat{\boldsymbol{w}}_m=\{w_m\}, m=1,2,\cdots,M, w_m\in\{0,1\}$，当原序列中的比特位小于$\Gamma_1$时，估计的比特位取0，反则取1。

（2）对比认证分析。接收方获取估计的水印信息后与收发端共享的已知混沌水印序列进行显示度比对，求得ρ_m，即将估计的水印序列逐个位与已知的符号比较，统计相同个数与整个序列的个数比。通过设定相关认证判决门限Γ_2判别发射方合法或非法身份。

$$\begin{cases}H_0\text{:发送方为合法方, } \rho_m\geqslant\Gamma_2\\ H_1\text{:发送方为非法方, } \rho_m<\Gamma_2\end{cases} \tag{20}$$

其中，Γ_2为认证门限值，ρ_m为接收方估计水印序列与共享已知水印序列的相似度。本文采用归一化系数NC与误码率（bit error ratio，BER）评价算法的透明性和鲁棒性，误码率越接近1，则水印的鲁棒性越差，误码率越接近0，则水印的鲁棒性越好。

4　仿真实验与结果

4.1　实验配置

本文选用基于混沌序列的无线水印安全认证算法，仿真实验参数配置见表1，基带码元长度5 760×10 bit，水印信息长度为150 bit，由周期为12 h的初始种子值与混沌系统函数产生。扩频序列PN1，PN0码率为128，信道编码采用卷积编码，卷积编码码率为3/4，数字调制采用BPSK、QPSK、8PSK、16QAM，线性叠加水印幅度系数为0.1、0.3、0.5、0.7，平方根升余弦滤波器滚降系数为0.35，载波频率为200 MHz，采集频率为1 000，码元速率为50 Bd，水印叠加位置为基带符号的中间位，高斯白噪声信道SNR为0~15 dB，步进为1 dB。接收端采用抽样判决，水印检测采用相关解扩，通过最佳门限值判断水印是否存在，并提取水印信息，计算基带、水印误码率曲线。

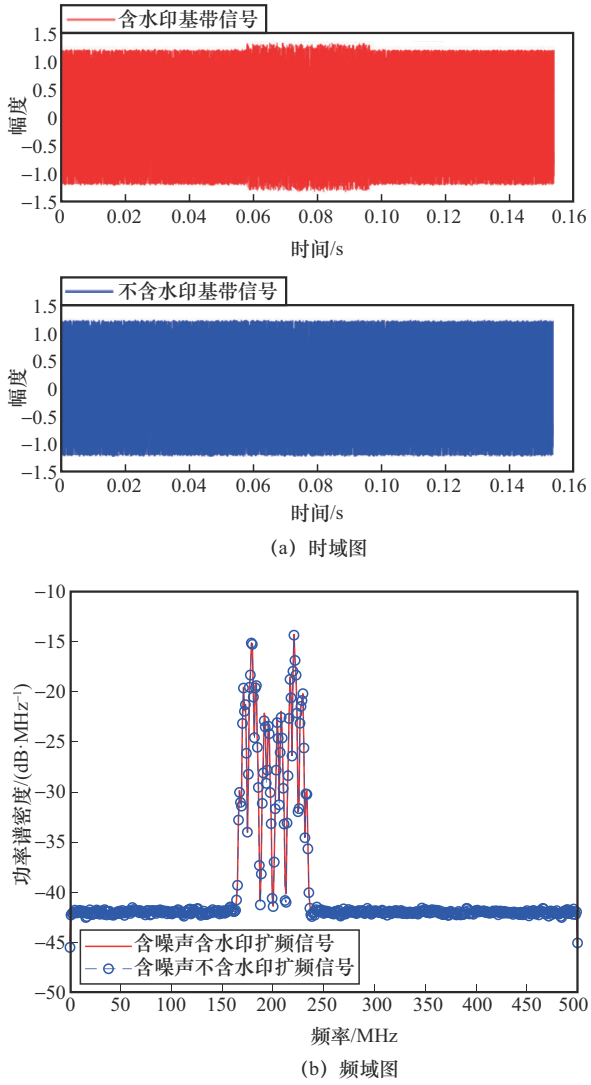
表1　仿真实验参数配置

参数名	数值			
基带码元长度	5 760×10 bit			
水印信息长度	150 bit			
码元速率	50 Bd			
载波频率	200 MHz			
数字调制方式	BPSK	QPSK	8PSK	16QAM
水印幅度系数	0.1	0.3	0.5	0.7
PN1、PN2序列长度	128 bit			
卷积码码率	3/4			
平方根升余弦滤波器滚降系数	0.35			
高斯白噪声SNR	0～15 dB			

4.2　仿真结果分析鲁棒性实验

（1）原始通信信号水印嵌入前后时域图、频域图对比分析

将Tent-Map混沌函数产生的扩频射频水印信息嵌入原始通信信号，当SNR=15、水印功率系数α=0.033 333时，对比分析嵌入水印信息与不含水印信息基带信号的时域图与频域图，水印前后时域与频域对比如图5所示。时域图如图5（a）所示，可观察到，嵌入基带信号的水印信息在加入段时域信号有弱信号叠加。另外，频域图如图5（b）所示，通过比较含水印扩频信号与不含水印扩频信号的频域图，视觉上两者基本重合无法辨别。



(a) 时域图

(b) 频域图

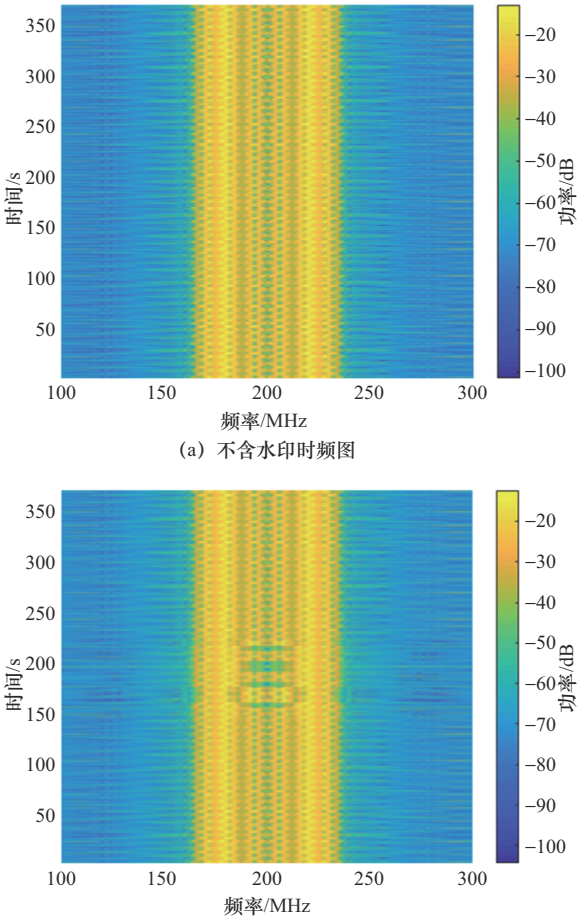
图5 水印前后时域与频域对比

（2）原始通信信号水印嵌入前后时频图对比分析

同样，分别对嵌入水印前后的原始通信信号进行时频分析，设置窗函数为汉明窗，窗大小为512，步进为256。对比分析时频图的变化，水印前后时频对比如图6所示，嵌入水印的信号在叠加时刻，有微弱信号表征，该物理特征可作为一种信号标识作为身份鉴定。

（3）基带采用不同调制方式下水印功率系数对基带误码率的影响

为分析本文所提方法在基带采用不同调制方式下，水印功率系数对基带误码率的影响，一方面需使基带误码率在合理水平，另一方面也需使水印能准确地被提取出来以便作为一种合理的认证手段，从而选取最佳水印功率系数。不同调制方式下水印功率系数对基带误码率的影响如图7所示，在功率系数相近的情况下，基带BPSK与QPSK的误码率表现性能类似，都优于基带8PSK和16QAM。相同调制方式下，水印功率系数越低，基带误码率越低。在水印功率系数一定的情况下，这4种调制方式的基带误码率都随着信噪比而逐渐降低，其中基带BPSK与QPSK的误码率下降速度更快，16QAM次之，基带8PSK的误码率下降速度最慢。基带BPSK，在信噪比为5 dB，功率系数为0.002 5时，解调后的误码率为10^{-5}。



(a) 不含水印时频图

(b) 含水印时频图

图6 水印前后时频对比

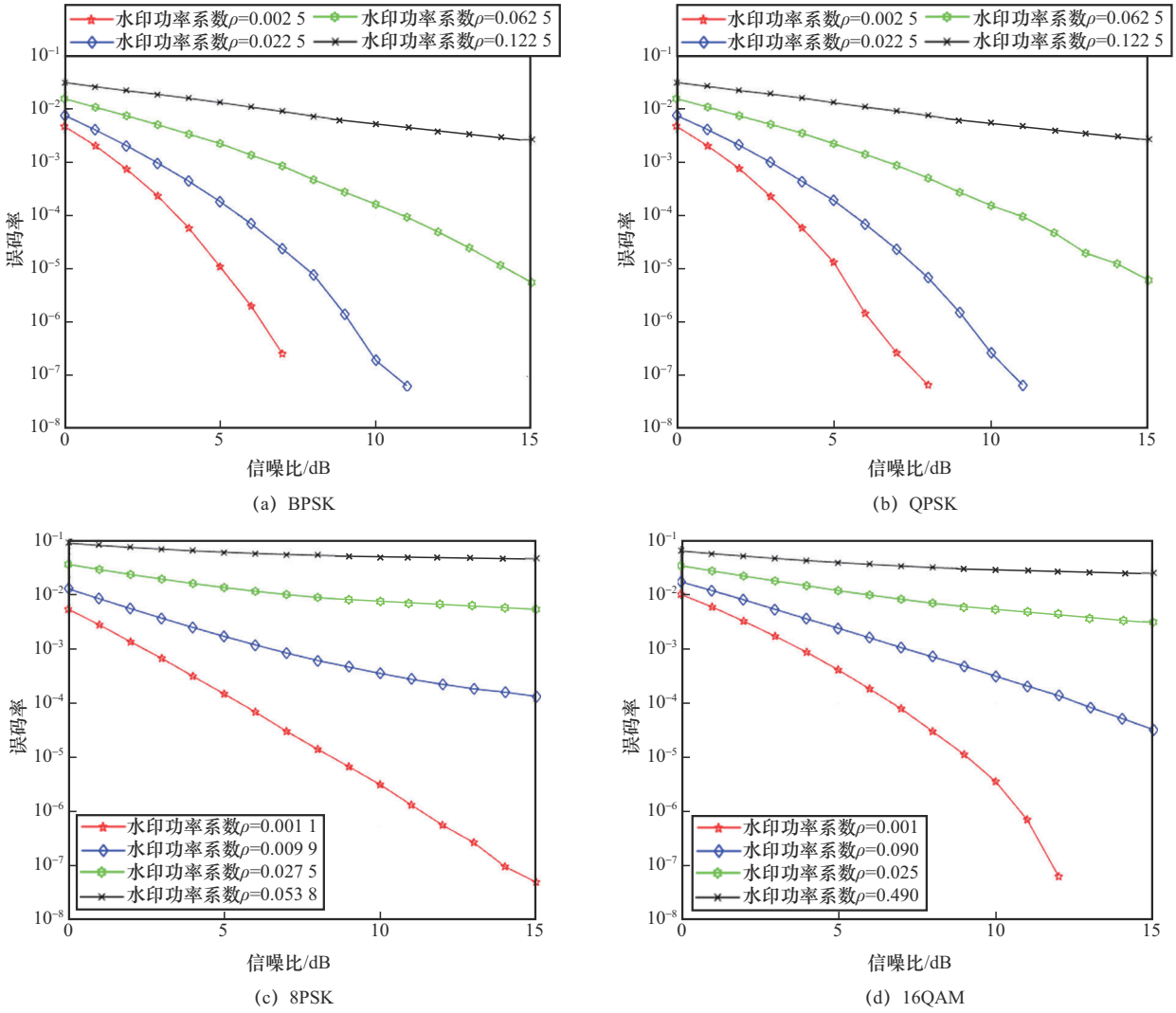


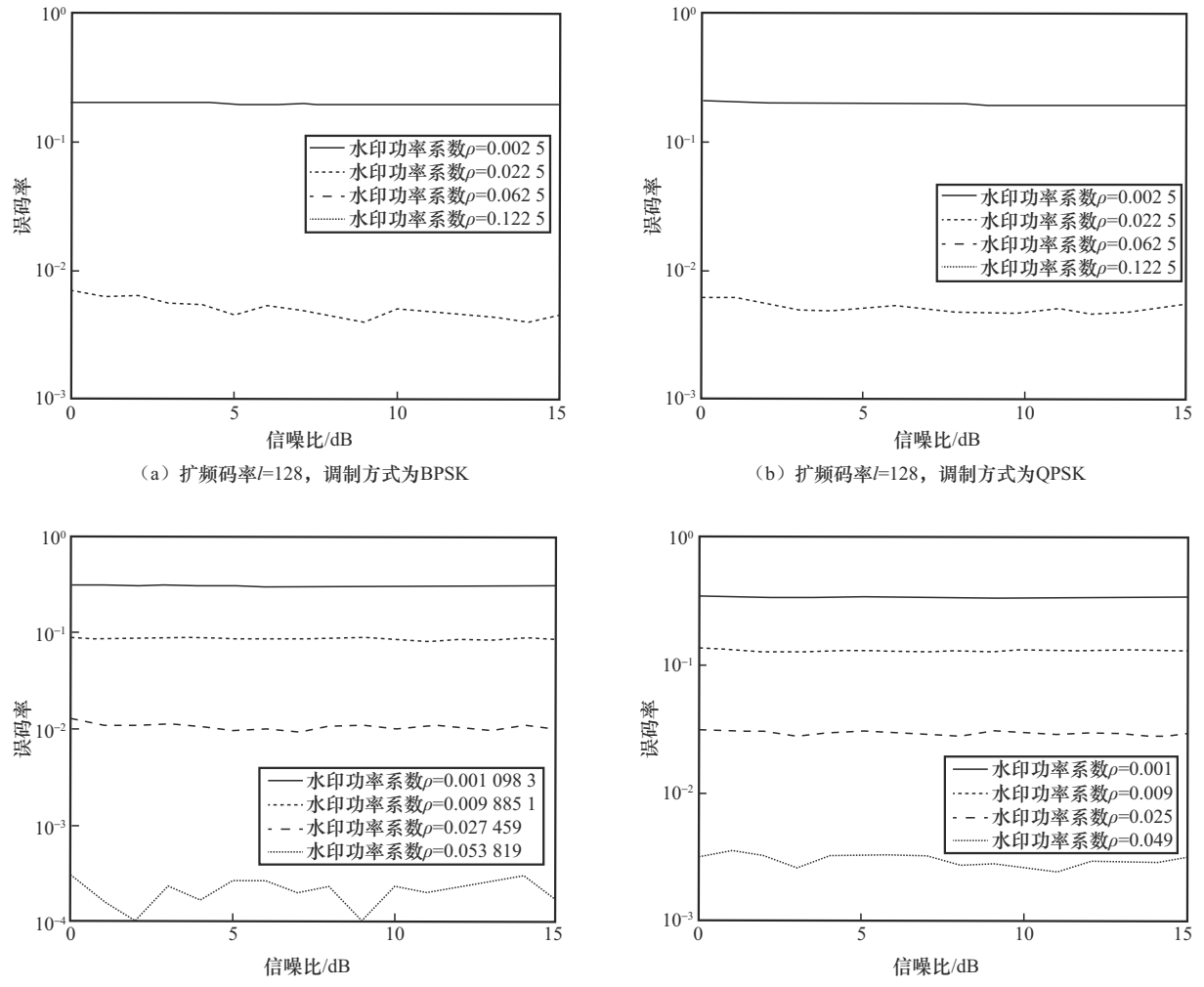
图7　不同调制方式下水印功率系数对基带误码率的影响

（4）基带采用不同调制方式下水印功率系数对水印误码率的影响

为分析水印功率系数在不同基带调制方式下对水印误码率的影响，本文通过仿真实验分别得到的不同调制方式下水印功率系数对水印误码率的影响如图 8 所示，从实验结果可知，水印误码率几乎不受高斯白噪声信噪比影响。随着水印功率系数的增加，水印误码率随之降低。在相近水印功率系数下，基带的调制方式为 BPSK 和 QPSK 时，水印误码率的表现性能相似，均优于基带采用 8PSK 和 16QAM 时。

5　结束语

针对低空经济无线网络易受欺骗攻击的问题，研究隐蔽安全通信机制，提出一种基于混沌序列的无线水印物理层安全认证技术，通过在波形域线性叠加正交扩频水印信号以达到通信信号的唯一身份标识，以保证数据在传输过程中的私密性。仿真实验表明该方式适用于不同数字调制方式，可通过调整水印功率系数动态调节算法鲁棒性。且该方案实现成本低，可在资源受限的低空场景中得到广泛应用。



（a）扩频码率l=128，调制方式为BPSK

（b）扩频码率l=128，调制方式为QPSK

（c）扩频码率l=128，调制方式为8PSK

（d）扩频码率l=128，调制方式为16QAM

图8　不同调制方式下水印功率系数对水印误码率的影响

参考文献：

[1] 田园, 吴峰, 欧阳俊, 等. 面向低空经济的无人机通信及标准进展分析[J]. 信息通信技术, 2023, 17(5):38-44.
TIAN Y, WU F, OUYANG J, et al. Analysis of the progress of UAV communication and standards for low altitude economy [J]. Information and Communication Technology, 2023, 17(5): 38-44.

[2] ZHANG Y, YUTAKA M, SASABE M, et al. Attribute-based access control for smart cities: a smart-contract-driven framework[J]. IEEE Internet of Things Journal, 2021, 8(8): 6372-6384.

[3] 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, 2023, 33(8):1-16.
BAI H Z, WANG H C, LI G X, et al. A review of research on unmanned aerial vehicle concealed communication networks[J]. Telecommunications Science, 2023, 33(8): 1-16.

[4] 王晴天, 刘洋, 刘海涛, 等. 面向6G的网络智能化研究[J]. 电信科学, 2023, 33(9): 151-160.
WANG Q T, LIU Y, LIU H T, et al. Research on network intelligence for 6G[J]. Telecommunications Science, 2023, 33(9): 151-160.

[5] MEHALLEGUE N, LOUKHAOUKHA K, ZEBBICHE K, et al. Ambiguity attacks on SVD audio watermarking approach using chatic encrypted images[J]. Multimedia Tools and Applications, 2020, 79(6):1-15.

[6] 蔡伟. 面向水印嵌入与提取的广播电视信号检测技术[J]. 电视技术, 2023, 47 (10): 30-32.
CAI W. Radio and television signal detection technology for watermark embedding and extraction[J]. Television Technology, 2023, 47 (10): 30-32.

[7] QUAN Y, TENG H, CHEN Y, et al. Watermarking deep neural

networks in image processing[J]. IEEE Transactions on Neural Networks and Learning Systems, 2021, 32(5): 1852-1865.

[8] BOUBICHE D E, BOUBICHE S, BILAMI A. A cross-layer watermarking-based mechanism for data aggregation integrity in heterogeneous WSNs[J]. IEEE Communications Letters, 2015,19(5): 823-826.

[9] 吴聪, 吴阳. 一种低复杂度的嵌入水印式物理层认证改进方案[J]. 物联网技术, 2021, 5: 31-35.
WU C, WU Y. A low complexity embedded watermark based physical layer authentication improvement scheme[J]. Internet of Things Technology, 2021, 5:31-35

[10] 王龙龙, 吴聪, 鲁兴波, 等. 无线自组网中一种基于嵌入式水印的身份认证方案实现[J]. 通信技术, 2021, 54(9): 2196-2201.
WANG L L, WU C, LU X B, et al. Implementation of an identity authentication scheme based on embedded watermarking in wireless ad hoc networks[J]. Communication Technology, 2021, 54(9): 2196-2201.

[11] 张余, 许金勇, 柳永祥, 等. 基于扩频的频谱水印嵌入与提取方法研究及实现[J]. 电波科学学报, 2016, 31(5): 920-926.
ZHANG Y, XU J Y, LIU Y X, et al. Research and implementation of spectrum watermark embedding and extraction method based on spread spectrum[J]. Journal of Radio Science, 2016, 31(5): 920-926.

[12] 刘忠英, 许金勇, 赵杭生. 基于频谱信号的频谱水印技术研究[J]. 河北科技大学学报, 2011, 32：116-118.
LIU Z Y, XU J Y, ZHAO H S. Research on spectrum watermarking technology based on spectrum signal[J]. Journal of Hebei University of Science and Technology, 2011, 32: 116-118.

[13] 张应宪, 刘爱军, 王永刚, 等. 卫星通信物理层安全技术研究展望[J]. 电讯技术, 2013, 53(3): 363-370.
ZHANG Y X, LIU A J, WANG Y G, et al. Prospects for research on physical layer security technology in satellite communication[J]. Telecommunications Technology, 2013, 53(3): 363-370.

[14] 徐争光. 无线通信中物理层认证关键技术的研究综述[J]. 华南理工大学学报(自然科学版), 2018, 46(5): 47-52.
XU Z G. A review of key technologies for physical layer authentication in wireless communication[J]. Journal of South China University of Technology (Natural Science Edition), 2018, 46(5): 47-52.

[15] 韩婷婷. 基于数字水印的无线传感器网络数据安全认证研究[D]. 南京: 南京信息工程大学, 2023
HAN T T. Research on data security authentication of wireless sensor networks based on digital watermarking [D]. Nanjing: Nanjing University of Information Science and Technology, 2023.

[16] KAY S M. Fundamentals of statistical signal processing: estimation theory[M]. Upper Saddle River: Prentice-Hall Inc., 1995.

[作者简介]

陈松林（1989– ），男，博士，中国电子科技集团公司第十研究所工程师，主要研究方向为网电对抗、信号处理、无线物理层安全。