第 43 卷 第 19 期/2023 年 10 月/光学学报 研究论文

光学学报

基于混沌加密和Kramers-Kronig接收机的光直接检测系统

巩小雪[1]，张天天[1]，张琦涵[2*]，张铁凝[2]，郭磊[1]

[1]重庆邮电大学通信与信息工程学院，重庆 400065；

[2]东北大学计算机科学与工程学院，辽宁 沈阳 110819

摘要 为了实现直接检测(DD)光正交频分复用(OOFDM)系统安全可靠通信，在发送端利用混沌加密技术来提高DD-OOFDM系统的安全性，在接收端采用Kramers-Kronig(KK)接收机来解决OFDM信号子载波拍频干扰的问题。利用混沌加密前后的图像像素值分布对系统的安全性进行分析验证。此外，分析了KK接收机的结构和其实现的条件，仿真测试了基于混沌加密和KK接收机的DD-OOFDM系统的误码率性能。

关键词 直接检测；光正交频分复用；子载波拍频干扰；混沌加密；Kramers-Kronig接收机

中图分类号 TN91 **文献标志码** A **DOI**：10.3788/AOS230594

1 引 言

光正交频分复用(OOFDM)技术具有频谱效率高、抗色散能力强等优点，成为光通信的研究热点。相比相干检测系统，直接检测(DD)-OOFDM系统由于成本低、结构简单及对频率偏移和相位噪声不敏感等优点，在中短距离的光接入网和城域网中得到了广泛的研究[1-4]。然而，在DD-OOFDM系统中，OFDM子载波相互拍频产生的子载波之间的拍频干扰(SSBI)会落在有效信号频谱区间，从而降低了系统的传输性能[5-6]。为了减轻SSBI的影响，研究人员提出了多种SSBI抑制方法，其中，采用Kramers-Kronig(KK)接收机来恢复信号以此消除SSBI的方法备受关注[7-8]。

此外，随着物理层光纤窃听技术的发展，非法人员可以通过弯曲光纤、监听邻信道的冗余串扰等方式使微量光信号泄漏从而获得信息[9-10]。目前大多数光通信系统都没有在物理层安全方面采取相应措施，仅仅采用了传统的在数据链路层及以上层次进行加密的方式，显然已不能保证全部信息在物理层进行可靠传输[11-14]。数字混沌具有随机、对初始值敏感、不可预测等特性，将数字混沌应用到OFDM系统中，为OFDM系统的底层信息安全提供了新的保障。文献[11]提出了基于混沌三维星座扰动的相干光OFDM加密技术。文献[12]在OFDM系统中提出了固定点数字混沌加密算法，增强了数据的安全性。文献[13]提出基于混沌压缩感知的OFDM加密技术，实现了对数据的压缩和安全性提升。文献[14]提出了一种基于三维Arnold变换和混沌Frank序列的加密算法，解决了数据安全性低和峰值平均功率比高的问题。相关的研究工作也正在不断进行着。

因此，为了实现DD-OOFDM系统安全可靠通信，本文提出基于混沌加密和KK接收机的DD-OOFDM系统。在发送端，对原始数据利用双混沌序列加密的方式进行加密处理，降低原始数据之间的关联性，以保证数据的安全传输；在接收端，采用KK接收机来恢复信号，消除SSBI。仿真分析了所提系统的误码率性能。结果表明，所提系统的误码率低于前向纠错门限值，传输可靠性较高。

2 DD-OOFDM系统

DD-OOFDM系统的结构如图1所示。相比相干检测OOFDM系统，DD-OOFDM系统在接收端更加简单，只需要1个光电二极管(PD)，成本低，适合于中短距离光通信的应用场景。

经过OFDM调制后的电信号可表示为

$$s_{\mathrm{elec}}(t)=\sum_{k=0}^{N-1}d_k\exp\left(\mathrm{j}2\pi\frac{k}{T}t\right),\tag{1}$$

式中：d_k表示第k个子载波上承载的符号数据；N表示

收稿日期：2023-02-24；**修回日期**：2023-03-28；**录用日期**：2023-04-23；**网络首发日期**：2023-05-08

基金项目：国家自然科学基金(62075024，62025105，62071076，62205043，62201105)、重庆市自然科学基金(CSTB2022NSCQ-MSX1334，cstc2021jcyj-msxmX0404)、重庆市教委创新研究群体项目(CXQT21019)

通信作者：*qihanzhang@stumail.neu.edu.cn

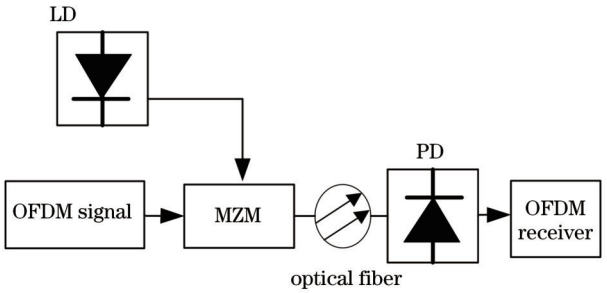

图 1 DD-OOFDM 系统的结构

Fig. 1 Structure of DD-OOFDM system

子载波总数；T 表示 OFDM 符号间隔。若使调制后的电信号经快速傅里叶逆变换(IFFT)后的数据为实数，则输入数据 X_N 要满足条件 $d_0,\cdots,d_{N-1}=X_0,X_1,\cdots,X_{N/2-1},X_{N/2},X^*_{N/2-1},\cdots,X^*_1$。假设马赫-曾德尔调制器(MZM)的直流偏置电压为 0，则输出的光信号场强为

$$E_{\text{out}}(t)=\frac{1}{2}E_{\text{in}}(t)\cdot\left[\mathrm{e}^{\mathrm{j}\pi\left[\frac{s_{\text{up}}(t)}{V_\pi}\right]}+\mathrm{e}^{\mathrm{j}\pi\left[\frac{s_{\text{low}}(t)}{V_\pi}\right]}\right],\tag{2}$$

式中：$E_{\text{in}}(t)$ 表示输入的光信号场强；$s_{\text{up}}(t)$ 和 $s_{\text{low}}(t)$ 分别表示 MZM 上臂和下臂的射频驱动电压；V_π 表示 MZM 的射频半波电压。由于 MZM 上下两臂输入的 OFDM 信号相同，则有

$$s_{\text{up}}(t)=s_{\text{elec}}(t),\tag{3}$$

$$s_{\text{low}}(t)=s_{\text{elec}}(t),\tag{4}$$

所以得

$$E_{\text{out}}(t)=E_{\text{in}}(t)\cdot\exp\left\{\mathrm{j}\pi\left[\frac{s_{\text{elec}}(t)}{V_\pi}\right]\right\}。\tag{5}$$

在小信号调制的情况下，式(5)可近似表示为

$$E_{\text{out}}(t)=E_{\text{in}}(t)\left[1+\frac{\mathrm{j}\pi}{V_\pi}s_{\text{elec}}(t)\right]。\tag{6}$$

令 $\mathrm{j}\pi/V_\pi=m$，则 MZM 输出的光信号场强为

$$E_{\text{out}}(t)\approx E_{\text{in}}(t)\left[1+m\cdot s_{\text{elec}}(t)\right]。\tag{7}$$

如果不考虑各种干扰噪声，则 PD 平方率检测后的输出电流为

$$i(t)\approx r\cdot P_{\text{s}},\tag{8}$$

式中：r 为 PD 的响应系数。P_{s} 为输入光信号的功率，与光信号的能量 E_{s} 成正比，有

$$P_{\text{s}}\propto E_{\text{s}},\tag{9}$$

式中：$E_{\text{s}}\propto E^2_{\text{out}}(t)$，$P_{\text{s}}\propto E^2_{\text{out}}(t)$。PD 的输出电流近似为

$$i(t)=\kappa\cdot r\cdot E_{\text{out}}(t)\cdot E^*_{\text{out}}(t),\tag{10}$$

式中：κ 为常数。

3 基于混沌加密的 DD-OOFDM 系统发送端

3.1 双混沌序列加密

主要对 DD-OOFDM 系统所发送的图像信息进行双混沌序列加密。利用两个不同的混沌序列分别对图像奇数位置的像素点和偶数位置的像素点进行加密，然后与 OFDM 调制结合在一起进行光调制。对于数字图像加密，主要是对图像的像素值进行改变、位置替换等操作，其加解密框架如图 2 所示。明文空间对应图像的像素信息，而密文空间表示加密后的像素信息。本文加密时采用两个混沌加密序列，旨在使加密密钥空间变大，使得密钥具有更好的随机性，从而使加密后图形的像素信息关联性降到最低，达到良好的安全性。图像双混沌加密框架如图 3 所示。

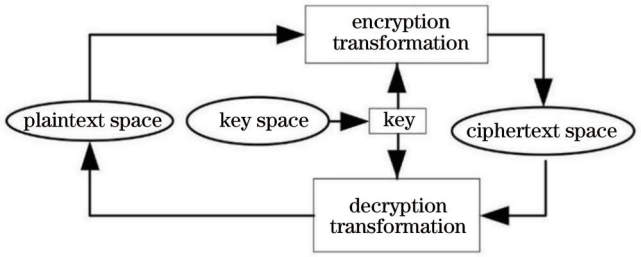

图 2 图像加解密框架

Fig. 2 Image encryption and decryption framework

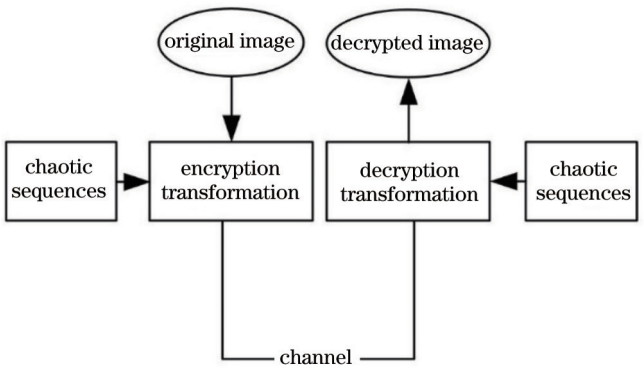

图 3 图像双混沌加解密模型

Fig. 3 Image double chaotic encryption and decryption model

混沌加密主要利用混沌映射表达式迭代产生序列值，将这些序列值作为密钥，而这些密钥呈无规律性。混沌映射是指一类动态系统，其状态值的演化表现出非线性、不可预测和极复杂的特点。混沌映射模型通常由一个简单的非线性方程定义，该方程包含一个或多个控制参数，这些参数可以改变系统的行为。相比 Henon、Chebyshev 和 Singer 等映射模式，Logistic 模式具有简单易实现、参数可调节、混沌性质良好等优势。因此本文采用 Logistic 映射模式，表达式为

$$x_{n+1}=\mu x_n(1-x_n),\tag{11}$$

式中：μ 是控制参数，$0<\mu\leqslant 4$；$x_n\in[0,1]$。在一定迭代次数 n 下，随着 μ 的改变，混沌序列值 x 呈现的虫口模型图像如图 4 所示。此外，采用 Lyapunov 指数 λ 来判断时间序列是否处于混沌状态[15-16]，经验证，当 Lyapunov 指数 $\lambda>0$ 时，混沌序列值会进入混沌状态，

此时 $3.57<\mu\leqslant 4.0$。也就是说在选取混沌序列值作为密钥时，μ 的取值至少要大于 3.57，此时由混沌序列产生的混沌值有不可预测、随机性很强的特点。

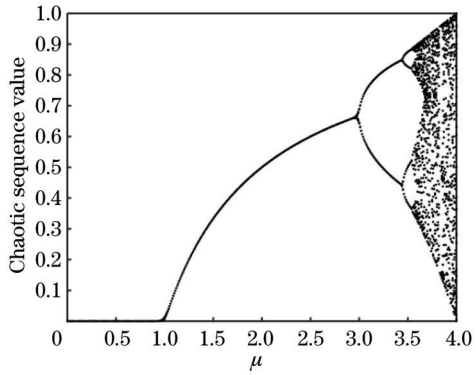

图 4　混沌虫口模型

Fig. 4　Chaos insect-population model

为了验证混沌序列对初始值 x_0 的敏感性，选取 $\mu=3.99$，将式(11)中的 x_0 随机选取为 $x_0=0.615648$ 和 $x_0=0.615647$，得出对应的混沌序列值分布图像，如图 5 所示。从图 5 可以看出，在保证 μ 相同的情况下，初始值 x_0 仅发生 10^{-6} 数量级的变化，而且迭代次数小于 100，两者产生的混沌序列完全不同。下面从密钥空间的角度分析该加密方法的破解难度。理论上来说，初始值 x_0、控制参数 μ、迭代次数 n 都会影响密钥空间。在双混沌序列加密中，以 x_0 为例，该数据有 32 个比特位，混沌的特性使 x_0 有 1 个比特偏差时，也能产生完全不同的混沌序列，因此密钥空间约为 2^{64}。综合上述因素，系统的总体密钥空间约可以达 2^{192}，有效防止暴力破解。

3.2　DD-OOFDM 系统发送端的设计

在 OOFDM 系统发送端，首先将图片作为发送的信源，先将图片的像素值(范围为 0～255)转换为 8 位的二进制数，再转换成一串二进制比特流，然后进行加扰，转换为随机的二进制比特流；接着采用双混沌序列对比特流进行加密，对两个混沌序列分别设置初始值，为 0.2 和 0.7，μ 设置为 4.0，如果对应的像素点位置是奇数，则利用第一个混沌序列进行加密，如果对应的像素点位置是偶数，则利用第二个混沌序列进行加密。在加密过程中，由于混沌映射序列产生的值分布在区间[0, 1]，如果不进行处理，在 MATLAB 软件中就会直接变成 0 或者 1，这样会使得加密精度降低，同时也会增大混沌序列的迭代次数。将产生的每个混沌值乘以较大的数，如 10^{15}，然后将这个混沌值对 256 取余数，保证结果与像素值进行异或时都为 8 位的二进制数，这样可以对一个混沌值与一个对应的像素值进行处理，使得混沌加密算法的迭代次数降低。具体流程如图 6 所示。将加密后的图像信息转换为二进制的比特流进行 OFDM 调制，再进行相应的光调制等操作。

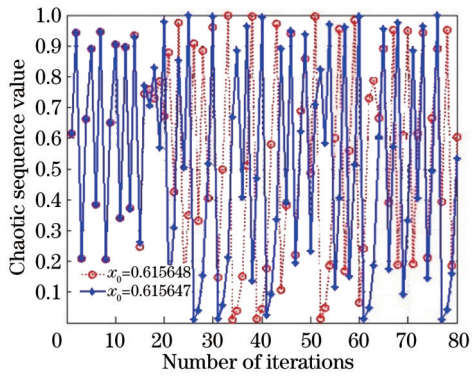

图 5　初始值不同的混沌序列值图像

Fig. 5　Image of chaotic sequence values with different initial values

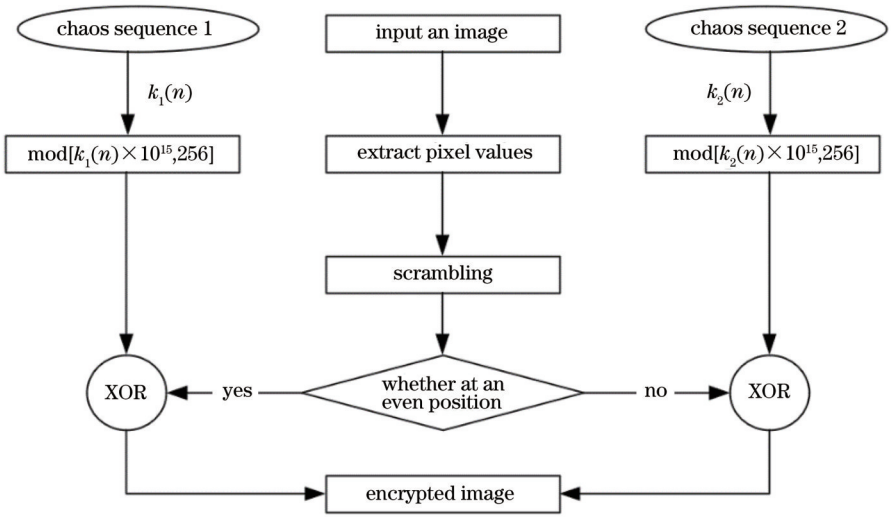

图 6　双混沌序列加密流程

Fig. 6　Flowchart of double chaotic sequence encryption

4　基于 KK 接收机的 DD-OOFDM 系统接收端

4.1　希尔伯特变换

定义一个实值函数 $x(t)$，其希尔伯特变换记为 $\hat{x}(t)$，则有

$$\hat{x}(t)=H[x(t)]=\frac{1}{\pi}\int_{-\infty}^{\infty}\frac{x(\tau)}{t-\tau}\mathrm{d}\tau, \tag{12}$$

式中：$H[\cdot]$表示希尔伯特变换；τ表示积分变量。希尔伯特逆变换为

$$x(t)=H^{-1}[\hat{x}(t)]=-\frac{1}{\pi}\int_{-\infty}^{\infty}\frac{\hat{x}(\tau)}{t-\tau}\mathrm{d}\tau。 \tag{13}$$

希尔伯特变换表达式实际上对原始信号和 $h(t)$ 进行卷积操作，其中

$$h(t)=\frac{1}{\pi t}, \tag{14}$$

所以希尔伯特变换可以看作将原始信号输入一个传递函数为 $h(t)$ 的系统得到的响应函数，其傅里叶变换为

$$H(\omega)=-\mathrm{j}\,\mathrm{sign}(\omega), \tag{15}$$

式中：sign(•)是符号函数，从频谱上来看，该函数可以将原始信号的正频率乘以 −j，也就是将相位移动 −90°，而对于负频率则乘以 j，即相位移动 90°。复数信号可以表示为一个实数信号和一个虚数信号的形式，如果实部和虚部具有一定关系，则可以在已知其中一项的情况下，利用希尔伯特变换求出另一项。

4.2　最小相位信号

在接收端接收光信号时，设在 PD 处产生的电场包络信号为 $E_s(t)$，带宽为 B，而激光器产生的连续信号幅度为 E_0，其位于信号带宽的左侧，如图 7 所示。

图 7　光电二极管处的电场信号

Fig. 7　Electric field signal at the photodiode

假设此时电场为 $E(t)$，则有

$$E(t)=E_s(t)+E_0\mathrm{e}^{\mathrm{j}\pi Bt}, \tag{16}$$

通过 PD 产生的电流为

$$I=|E(t)|^2, \tag{17}$$

当激光器产生的连续信号的幅度 E_0 足够大时，则 $E(t)\mathrm{e}^{-\mathrm{j}\pi Bt}=E_0+E_s(t)\mathrm{e}^{-\mathrm{j}\pi Bt}$ 为最小相位信号。设线性因果系统表达式为

$$E_{\mathrm{out}}(t)=\int_{-\infty}^{+\infty}h(t-t')E_{\mathrm{in}}(t')\mathrm{d}t', \tag{18}$$

如果式(18)傅里叶积分是收敛的，那么 $H(\omega)$ 在复平面中是连续解析的，则对于 $h(t)$，延时 $\delta(t-\tau_0)$，$\tau_0\geqslant 0$，也是连续解析的。为了解析方便，令

$$H(\omega)=a_0+H_0(\omega), \tag{19}$$

式中：$a_0=\lim\limits_{\omega\to\mathrm{j}\infty}H(\omega)$，且 $\lim\limits_{\omega\to\mathrm{j}\infty}H_0(\omega)=0$。在这里，当 ω 趋于无穷大时，有

$$h(t)\sim\mathrm{e}^{\mathrm{j}\omega\tau_0}, \tag{20}$$

系统响应表达式为

$$H(\omega)=|H(\omega)|\mathrm{e}^{\mathrm{j}\phi(\omega)}, \tag{21}$$

由于 $H(\omega)$ 在复平面的上半部分（包括实轴）没有奇异点，根据柯西定理，有

$$\int_{\Gamma}\frac{\ln[H(\omega')/a_0]}{\pi(\omega-\omega')}\mathrm{d}\omega'=0, \tag{22}$$

式中：Γ 表示复平面区域轮廓，如图 8 所示。

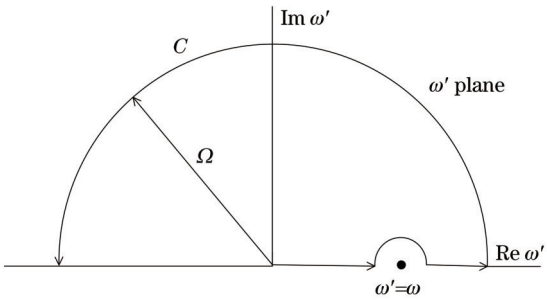

图 8　积分区域示意图

Fig. 8　Schematic of the integration area

$$\mathrm{p.v.}\int_{-\Omega}^{\Omega}\frac{\ln\left[\dfrac{H(\omega)}{a_0}\right]}{\pi(\omega-\omega')}\mathrm{d}\omega'+\mathrm{j}\ln\frac{H(\omega)}{a_0}+\varepsilon_c=0, \tag{23}$$

式中：p. v. 表示积分的柯西主值。ε_c 表示弧 C 的积分，即

$$\varepsilon_c=-\mathrm{j}\int_0^{\pi}\frac{\Omega\mathrm{e}^{\mathrm{j}\phi}\ln\left[\dfrac{H\left(\Omega\mathrm{e}^{\mathrm{j}\phi}\right)}{a_0}\right]}{\pi\left(\Omega\mathrm{e}^{\mathrm{j}\phi}-\omega\right)}\mathrm{d}\phi, \tag{24}$$

对式(24)两边同时取实部，得

$$\phi(\omega)=\phi_0+\mathrm{p.v.}\int_{-\Omega}^{\Omega}\frac{\ln\left[\left|\dfrac{H(\omega')}{a_0}\right|\right]}{\pi(\omega-\omega')}\mathrm{d}\omega+\mathrm{Re}(\varepsilon_c), \tag{25}$$

式中：$a_0=|a_0|\mathrm{e}^{\mathrm{j}\phi_0}$。当 $\Omega\to\infty$ 时，$\varepsilon_c\to 0$，则有

$$\phi(\omega)=\phi_0+\lim_{\Omega\to\infty}\mathrm{p.v.}\int_{-\Omega}^{\Omega}\frac{\ln\left[\left|\dfrac{H(\omega')}{a_0}\right|\right]}{\pi(\omega-\omega')}\mathrm{d}\omega'。 \tag{26}$$

所以，$\phi(\omega)-\phi_0$ 是 $\ln[|H(\omega)/a_0|]$ 的希尔伯特变换，那么相位信息 $\phi(\omega)$ 可从信号的幅度响应 $|H(\omega)|$ 中获得。即当 $|H_0(\omega)|<|a_0|$ 时，则系统响应函数 $H(\omega)$ 满足最小相位条件，可以根据幅度信息还原出相位信息。

4.3　KK 接收机的设计

由于直接检测会产生 SSBI，为了解决该问题，考虑利用 PD 检波后的 $I=|E(t)|^2$ 得到的幅度信息来计算出信号的相位信息，进而重组信号。KK 接收机则

利用希尔伯特变换原理对干扰后的信号进行重组。KK接收机结构如图9所示，KK接收机的核心在于KK算法，其中，ln(•)表示对数运算，$F\{(\bullet)\}$表示对离散数据进行傅里叶变换，$\exp\{\mathrm{j}(\bullet)\}$表示对输入的数据乘以j，然后进行指数运算。

在4.2节中，如果一个信号为最小相位信号，则需要保证$|H_0(\omega)|<|a_0|$，在这里光调制后为SSB-OOFDM信号，则假设通过PD后信号表达为

$$b(t)=E_0+E_s(t)\mathrm{e}^{-\mathrm{j}\pi Bt}, \tag{27}$$

式中：$b(t)=E(t)\mathrm{e}^{-\mathrm{i}\pi Bt}$；$E_0$表示光载波的幅度，是一个常量；$E_s(t)$表示光OFDM信号。当$|E_0|>|E_s(t)|$，即当光载波功率大于OFDM信号功率时，可以保证信号$b(t)$为最小相位信号。由于此时电流为$|b(t)|^2$，所以如图9所示，首先需要进行开根号运算，因为此时$b(t)$为最小相位信号，则可根据希尔伯特变换得出相位$\phi(t)$：

$$\phi(t)=\frac{1}{\pi}\mathrm{p.v.}\int_{-\infty}^{\infty}\frac{\ln[|b(t')|]}{t-t'}\mathrm{d}t'。 \tag{28}$$

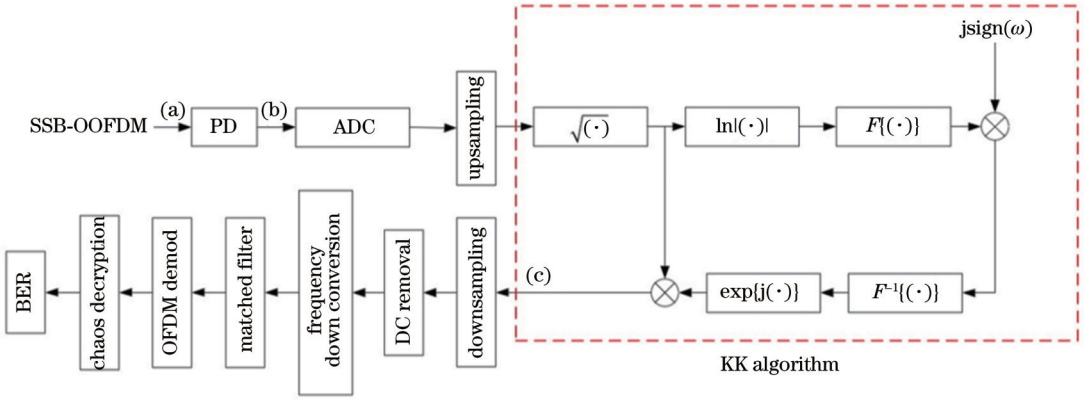

图9　KK接收机的结构

Fig. 9　KK receiver structure

式(28)在频域的表达式为

$$\phi(\omega)=\mathrm{jsign}(\omega)F\{\ln[|b(t)|]\}。 \tag{29}$$

将在频域得出的相位信号$\phi(\omega)$傅里叶逆变换到时域，然后重组原始信号，得

$$H(t)=|H(t)|\mathrm{e}^{\mathrm{j}\phi(t)}。 \tag{30}$$

在进行KK处理时，由于平方根运算和对数运算使得信号带宽变大，所以需要进行上采样。此外，为了保证KK处理利用幅度时可以还原相位，即要保证输入的信号为最小相位信号，需要足够大的光载波功率，更准确地说是需要足够高的光载波与电信号的功率比(CSPR)。本文采用调节直流偏置电压的方式来调节CSPR。

5　系统搭建与仿真分析

采用VPI Transmission Maker 9.1和MATLAB 2014a联合仿真，其中混沌加解密、OFDM信号调制解调及KK处理在MATLAB 2014a中处理，而光调制、传输链路及接收端在VPI Transmission Maker 9.1中搭建。整体系统如图10所示，该系统主要包括混沌加密、OFDM调制、SSB-OOFDM产生、光传输链路、光电探测、KK处理、OFDM解调及混沌解密。首先对原始图像信息进行混沌加密，即将图像的像素值转换为二进制的比特流后进行加扰，产生随机二进制比特流；再采用双混沌加密的方式分别对奇数位置和偶数位置的数据进行加密，从而改变原像素点的像素值，以保证更大程度降低图像信息的关联性，从而提高安全性；然后对加密后的数据进行QPSK调制，再将数据输入到OFDM调制模块进行相应的OFDM调制。其中，OFDM符号数为400，子载波个数为256，携带信息的子载波个数为127，循环前缀比例为1/8。调制后的OFDM信号通过MZM驱动光载波产生双边带光信号，其中，激光器的中心频率设置为193.1 THz，线宽为

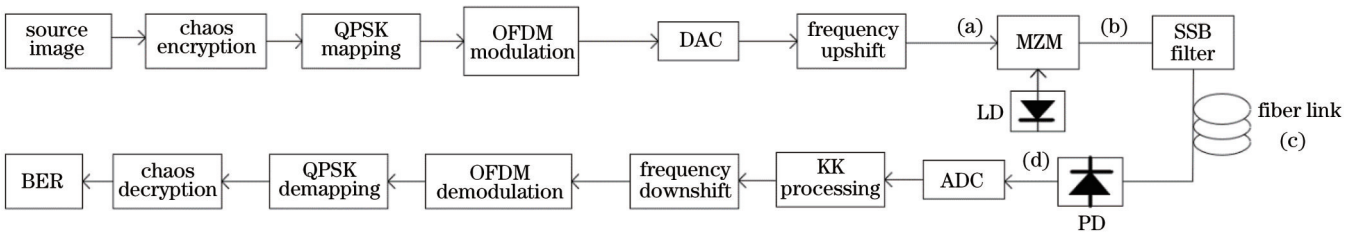

图10　基于混沌加密和Kramers-Kronig接收机的光直接检测系统框图

Fig. 10　Block diagram of optical direct detection system based on chaotic encryption and Kramers-Kronig receiver

0.1 MHz，MZM 的消光比为 35 dB，插入损耗为 6 dB。采用光带通滤波器来滤除双边带信号的低频带，得到单边带（SSB）光信号。单模光纤长度为 20 km。光纤功率衰减为 0.2 dB/km，色散斜率为 0.08 ps/nm^2/km，克尔系数为 2.6×10^{-20} m^2/W，有效纤芯面积为 80.0 μm^2。

图 11 为双混沌加密前后的图像和直方图。图 11（a）是原始图像，图 11（b）为其像素值的分布直方图，可以看出像素值范围在[0，255]，且大部分像素点的像素值集中分布在 250 附近，分布极不均匀，一定程度上展示了像素点之间的关联性，容易被窃密者破解，安全性较低。图 11（c）和图 11（d）是比特加扰后的图像和像素值的分布直方图，图 11（e）和图 11（f）是双混沌加密后得出的图像和像素值的分布直方图，加扰和加密后的图像和像素值的分布直方图具有类似的变化，即图像相比于原图像已完全不同，说明图像原来位置的像素值已发生改变，图像的像素值均匀地分布在[0，255]之间，破坏了原始图像中像素值的关联性，使得窃密者很难从中推出原始图像，具有很高的安全性。

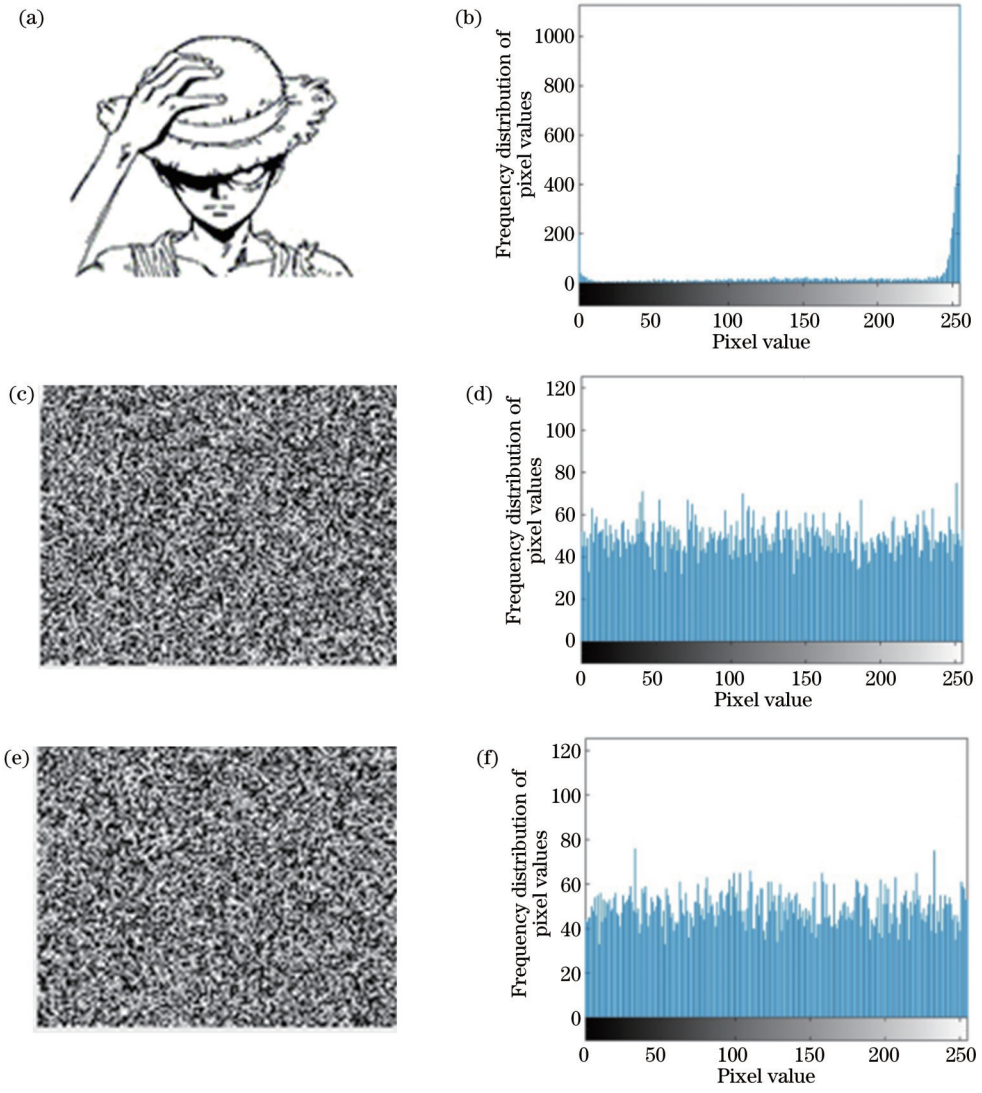

图 11　双混沌加密前后的图像和像素直方图。（a）原始图像；（b）原始图像直方图；（c）加扰后的图像；（d）加扰后的图像直方图；（e）混沌加密图像；（f）混沌加密图像直方图

Fig. 11　Image and pixel histogram before and after double chaotic encryption. (a) Source image; (b) source image histogram; (c) scrambled image; (d) scrambled image histogram; (e) chaotic encryption image; (f) chaotic encryption image histogram

图 12 给出了系统在是否采用 KK 接收机的情况下误码率（BER，R）随 CSPR 的变化关系。从图 12 可以看出：当 CSPR 小于 8 dB 时，相比使用 KK 接收机的情况，未使用 KK 接收机的误码率较低，那是由于 CSPR 没有达到足够大，输入 KK 接收机的信号是最小相位信号，从而不能得出相位信号来重组原信号，且当 CSPR 小于 8 dB 时，由于 SSBI 的存在，两者的误码率始终都要高于前向纠错门限值 3.8×10^{-3}；当 CSPR 大于 8 dB 之后，未使用 KK 接收机的情况下误码率变大，这是由于随着光功率的增大，光纤中发生了克尔效

应，引起了非线性失真。在不插入保护间隔的情况下，由于非线性失真和SSBI的同时存在，未用KK接收机的系统误码率始终高于前向纠错门限值；而对于使用KK接收机的系统，由于CSPR已经足够大，KK接收机满足最小相位条件，故可以根据幅度信息还原出相位信息，进而对接收信号进行重组，从而消除SSBI，降低了误码率。

此外，在接收端对经OFDM解调后的信号再进行混沌解密，得出图像，假设接收端有正确的密钥，则通过图像的清晰度也可以直观看出利用KK接收机和未用KK接收机两者的区别。图13为当CSPR为11 dB时，未用KK接收机和利用KK接收机进行混沌解密后的图像。图13左边为未用KK接收机进行混沌解密的图像，可以看出图像上充满了噪声点，表明系统在接收端受到SSBI影响较大，系统整体性能较差；图13右边为利用KK接收机进行混沌解密的图像，可以看出与原始图像基本相同，仅有少量的噪声点，这主要是光

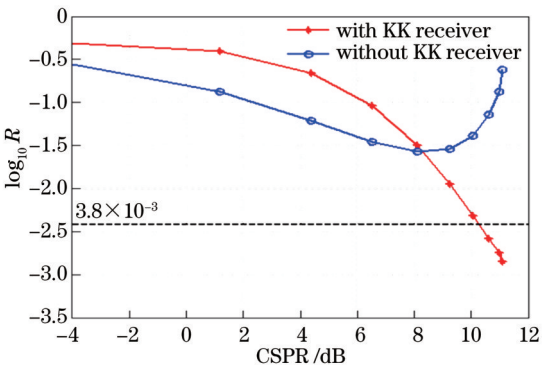

图12　KK接收机引入前后的处理结果

Fig. 12　Processed results before and after the introduction of KK receiver

OFDM信号在光纤传输中的色散引起的。对比两幅图可以看出，利用KK接收机的DD-OOFDM系统性能较好。

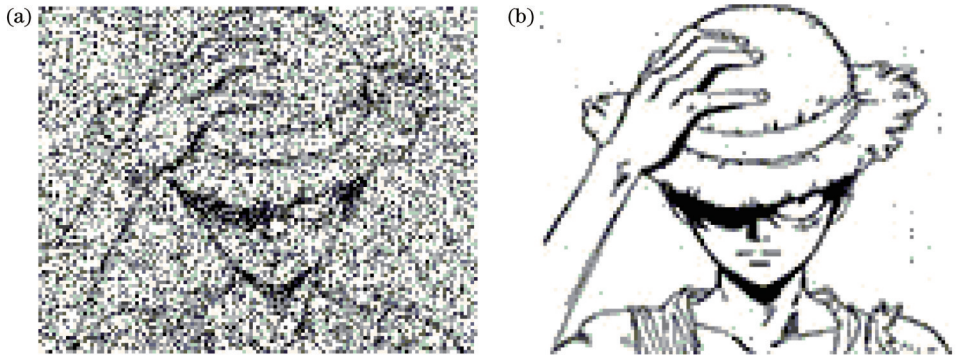

图13　未用KK接收机和利用KK接收机进行混沌解密后的图像

Fig. 13　Chaotic decrypted images without and with KK receiver

6　结　　论

DD-OOFDM系统具有较高的传输性能，但是面临着光纤弯曲等物理窃听攻击引起的信息泄露问题，并且接收端存在的SSBI使得系统误码率增加。为了解决这两个问题，在发送端对图像信息采用双混沌序列进行加密，即对图像像素点为奇数和偶数的点采用两个不同的混沌序列进行加密，从而增大了破解难度。在接收端，采用KK接收机，系统可以从接收到的幅度信息中恢复出相位信息，进而得到全场信息。同时采用KK接收机可以消除SSBI，从而有效降低误码率，提高整个系统的传输性能。在未来的工作中，将联合非线性补偿算法和KK接收机提升系统性能，并比较分析不同的CSPR提升方法对系统性能的影响。

参　考　文　献

[1] Anusha M, Murthy T S N. PAPR analysis of MB-OFDM UWB signal using hybrid PS-GW optimized PTS technique [C]//2022 International Conference on Computing, Communication and Power Technology (IC3P), January 7-8, 2022, Visakhapatnam, India. New York: IEEE Press, 2022: 219-221.

[2] Li Z, Erkılınç M S, Shi K, et al. Digital linearization of direct-detection transceivers for spectrally efficient 100 Gb/s/λ WDM metro networking[J]. Journal of Lightwave Technology, 2017, 36(1): 27-36.

[3] Halabi F, Chen L, Giddings R P, et al. Subcarrier grouping-enabled improvement in transmission performance of subcarrier index-power modulated optical OFDM for IM/DD PON systems [J]. Journal of Lightwave Technology, 2018, 36(20): 4792-4798.

[4] 李炉焦，陈君，唐志军，等. 光无线通信中基于哈特莱变换的翻转OFDM技术[J]. 光学学报，2021，41(19)：1906002.
Li L J, Chen J, Tang Z J, et al. Flip-OFDM based on Hartley transform for optical wireless communications[J]. Acta Optica Sinica, 2021, 41(19): 1906002.

[5] Zhou K J, Cui S. Complex signal field retrieval based on improved Kramers-Kronig coherent receiver without digital upsampling[C]//2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), June 12-14, 2020, Chongqing, China. New York: IEEE Press, 2020: 180-183.

[6] An S H, Zhu Q M, Li J C, et al. Accurate field reconstruction at low CSPR condition based on a modified KK receiver with direct detection[J]. Journal of Lightwave Technology, 2020, 38(2): 485-491.

[7] 孙梦凡，蔡沅成，朱敏，等. 直接探测光纤通信系统场信号恢

复技术综述[J]. 激光与光电子学进展, 2022, 59(11): 1100002.
Sun M F, Cai Y C, Zhu M, et al. Summary of field signal recovery technology in direct detection optical fiber communication system[J]. Laser & Optoelectronics Progress, 2022, 59(11): 1100002.
[8] 巩小雪, 胡婷, 张琦涵. 色散抑制单边带数字滤波多址-无源光网络系统[J]. 光学学报, 2022, 42(14): 1406002.
Gong X X, Hu T, Zhang Q H. Dispersion suppression single sideband digital filtering multiple access-passive optical network system[J]. Acta Optica Sinica, 2022, 42(14): 1406002.
[9] Gong X X, Zhang Q H, Zhang X, et al. Security issues and possible solutions of future-oriented optical access networks for 5G and beyond[J]. IEEE Communications Magazine, 2021, 59(6): 112-118.
[10] Shen J J, Liu B, Mao Y Y, et al. Enhancing the reliability and security of OFDM-PON using modified Lorenz chaos based on the linear properties of FFT[J]. Journal of Lightwave Technology, 2021, 39(13): 4294-4299.
[11] Zhang Y Q, Jiang N, Zhao A K, et al. Security enhancement in coherent OFDM optical transmission with chaotic three-dimensional constellation scrambling[J]. Journal of Lightwave Technology, 2022, 40(12): 3749-3760.
[12] Li S S, Cheng M F, Deng L, et al. Secure strategy for OFDM-PON using digital chaos algorithm with fixed-point implementation[J]. Journal of Lightwave Technology, 2018, 36(20): 4826-4833.
[13] Wu T W, Zhang C F, Chen Y H, et al. Compressive sensing chaotic encryption algorithms for OFDM-PON data transmission [J]. Optics Express, 2021, 29(3): 3669-3684.
[14] 周玉鑫, 毕美华, 滕旭阳, 等. 基于混沌映射的OFDM-PON物理层加密及系统性能增强算法[J]. 光学学报, 2021, 41(16): 1606002.
Zhou Y X, Bi M H, Teng X Y, et al. Physical layer encryption and system performance enhancement algorithm based on chaos mapping in OFDM-PON[J]. Acta Optica Sinica, 2021, 41(16): 1606002.
[15] 刘公致, 吴琼, 王光义, 等. 改进型Logistic混沌映射及其在图像加密与隐藏中的应用[J]. 电子与信息学报, 2022, 44(10): 3602-3609.
Liu G Z, Wu Q, Wang G Y, et al. Improved logistic chaotic mapping and its application in image encryption and hiding[J]. Journal of Electronics & Information Technology, 2022, 44(10): 3602-3609.
[16] 陈树彬. 混沌图像加密算法安全性能研究[J]. 软件工程, 2022, 25(11): 56-59.
Chen S B. Research on security performance of chaotic image encryption algorithm[J]. Software Engineering, 2022, 25(11): 56-59.

Optical Direct-Detection System Based on Chaotic Encryption and Kramers-Kronig Receiver

Gong Xiaoxue[1], Zhang Tiantian[1], Zhang Qihan[2*], Zhang Tiening[2], Guo Lei[1]

[1]*School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing* 400065, *China*;

[2]*School of Computer Science and Engineering, Northeastern University, Shenyang* 110819, *Liaoning, China*

Abstract

Objective Optical orthogonal frequency division multiplexing (OOFDM) technology features the advantages of high spectral efficiency and strong anti-dispersion ability and is of immense interest in optical communication. Additionally, based on the different detection methods at the receiver, optical communication systems are divided into direct detection (DD) and coherent detection systems. Compared with the coherent detection system, DD-OOFDM system has the advantages of low cost, simple structure, and insensitivity to spectral offset and phase noise. Therefore, DD-OOFDM optical communication systems have been widely used. The realization of high-speed information transmission in the DD-OOFDM communication systems ensures convenience; nonetheless, information security issues are emerging, such as illegal personnel stealing information through fiber bending and other means; therefore, securing optical communication has become crucial. Compared with traditional encryption methods, chaotic encryption is advantageous because of its hard-to-predict nature and limitless chaotic sequence values. Using chaotic mapping sequences to derive keys with no regularity can improve the security of the system. However, in a DD-OOFDM communication system supporting chaotic encryption, since the receiver needs to receive sufficient encrypted information to decrypt it correctly, higher requirements are posed on the system BER. The presence of OOFDM subcarrier beat interference (signal to signal beat interference, SSBI) at the receiver end of the DD-OOFDM system significantly increases the system BER; thus, reducing SSBI becomes the key to improving transmission performance. The traditional method is to insert a protection interval to avoid the overlap of SSBI and OFDM signals, thus eliminating SSBI. However, this decreases the spectrum utilization of the system. The Kramers-Kronig (KK) receiver has the advantages of high spectrum utilization, low hardware complexity, and simple implementation, which can solve the aforementioned problem efficiently. For this reason, the use of a KK receiver at the receiver side is recommended to eliminate SSBI.

Methods In this study, image transmission is considered as an example; at the transmitter side, the image pixel values

(range 0-255) are first converted into 8-bit binary numbers, subsequently into a string of binary bit streams, and finally scrambled into random binary bitstreams. Thereafter, a double chaotic sequence is used to encrypt the bitstreams, with two chaotic sequences set to initial values of 0.2 and 0.7, respectively, and set μ to 4.0. The first or second chaotic sequence is used for encryption based on if the corresponding pixel location is odd or even, respectively. In the encryption process, since the chaotic mapping sequence generates values distributed in the interval [0, 1], if left untreated, they will directly become 0 or 1 in MATLAB software, thereby causing the encryption accuracy to decrease and number of iterations of the chaotic sequence to increase. Therefore, in this study, each chaotic value generated is multiplied by a larger number, such as 10^{15}, and subsequently, this chaotic value is remaindered against 256 to ensure that it is an 8-bit binary number when it is heterogeneous with the pixel value. This allows a chaotic value to be processed with a corresponding pixel value, lowering number of iterations of the chaotic encryption algorithm. Subsequently, the encrypted data are combined with OFDM modulation for optical modulation. This study proposes eliminating the SSBI existing in the receiver side of the DD-OOFDM system using the KK receiver to reduce the BER and improve the system transmission reliability on the basis of secure transmission. Specifically, this study analyzes the structure of the KK receiver and the condition of its function that the input signal is the minimum phase signal, and simulates and tests the BER of the DD-OOFDM system based on the KK receiver.

Results and Discussions At the transmitter side, this study uses two chaotic sequences for data encryption, where the initial value x_0 of the logistic chaotic mapping changes only by 10^{-6} orders of magnitude, and less than 100 iterations are need to produce completely different chaotic sequences (Fig. 5). Theoretically, the initial value x_0, control parameters μ, and number of iterations n all affect the key space. For example, in double chaotic sequence encryption, the data x_0 has 32 bits, and the nature of chaos enables the generation of a completely different chaotic sequence even at one bit deviation in x_0; thus, the key space is approximately 2^{64}. Combining the above factors, the overall key space of the system can reach approximately 2^{192}, which effectively prevents brute force cracking. Most of the image pixel point values before encryption are concentrated around 250, an extremely uneven distribution, demonstrating the correlation between pixel points to a certain extent, is easy to be cracked by the eavesdropper and hence is less secure. The scrambled and encrypted image and pixel values are completely different compared with the original image, and the pixel values of the encrypted image are uniformly distributed between [0, 255], which destroys the correlation of pixel values in the original image with high security, rendering it difficult for an eavesdropper to launch the original image from it (Fig. 11). At the receiver side, when the CSPR is sufficiently large to cause the KK receiver to meet the minimum phase condition, it can eliminate the SSBI and reduce the BER (Fig. 12). The image after chaotic decryption using the KK receiver is essentially the same as the original image, with only a few noise points (Fig. 13).

Conclusions To achieve a safe and reliable data transmission in DD-OOFDM systems, this study conducted specific analysis, design, and implementation. To solve the security problem in DD-OOFDM systems, chaotic encryption is proposed. Chaotic mapping has the characteristics of randomness and limit nonconvergence, rendering the key space extremely large and thereby improving the encryption security. The original data are processed by double chaotic sequence encryption at the transmitting end of the system to reduce the correlation between the data substantially and ensure data security. To improve the spectral efficiency of the system, OFDM is used to modulate the encrypted data at the transmitter side of the system. At the receiver side, the SSBI in the signal after direct detection is processed, and a KK receiver is proposed to solve this interference. The structure of the KK receiver and the minimum phase signal conditions that render it successful are analyzed at the receiver side. Thereafter, the optical carrier power is changed by controlling the DC bias voltage of the laser driver so that the signal input to the KK receiver meets the minimum phase. With a CSPR of 11 dB, the system performs efficiently, with the KK receiver below the forward error correction threshold of the unutilized KK receiver.

Key words direct detection; optical orthogonal frequency division multiplexing; signal to signal beat interference; chaotic encryption; Kramers-Kronig receiver