基于深度感知的光场图像高维混沌加密研究

仲昭宇，王尔馥
（黑龙江大学电子工程学院，黑龙江 哈尔滨 150080）

摘　要：针对光场图像在多视点、高维度结构下的安全传输问题，提出了一种基于深度感知的高维混沌加密方法。该方法通过极平面图像技术及结构张量法提取光场深度信息，并通过块内中位数阈值、自适应滤波等策略抑制遮挡与弱纹理场景下的深度误差。随后，基于图像哈希驱动的高维混沌系统生成多通道密钥流，实现基于深度感知的自适应像素置乱与扩散。系统设计了多级加密机制，包括视点级全局置乱、像素级全局置乱、块内深度感知局部置乱、多轮深度增强扩散及跨视点块级交换。实验结果表明，该方案构建了一套完整的光场图像加密流程，在安全性、鲁棒性、密文质量分析等方面展现出优越的综合性能，为光场图像的安全保护提供了有效解决方案。

关键词：光场图像；高维混沌序列；图像加密；深度感知
中图分类号：TN918
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2026019

Research on high-dimensional chaotic encryption of light field images based on depth perception

Zhong Zhaoyu, Wang Erfu
Electronic Engineering College, Heilongjiang University, Harbin 150080, China

Abstract: The secure transmission challenges of light field images were addressed due to their multi-view and high-dimensional structure, a high-dimensional chaotic encryption method based on depth perception was proposed. This method extracted light field depth information using polar plane imaging techniques and structural tensor methods, while suppressing depth errors in occluded and weakly textured scenes through strategies such as intra-block median thresholding and adaptive filtering. Subsequently, a high-dimensional chaotic system driven by image hashing generated a multi-channel key stream, enabling adaptive pixel scrambling and diffusion based on depth perception. The system incorporated a multi-level encryption mechanism, including view-level global scrambling, pixel-level global scrambling, block-wise depth-aware local scrambling, multi-round depth-enhanced diffusion, and cross-view block exchange. Experimental results demonstrate that this scheme establishes a comprehensive light field image encryption process, exhibiting superior overall performance in terms of security, robustness, and ciphertext quality analysis, which provides an effective solution for the secure protection of light field images.

Keywords: light field image, high-dimensional chaotic sequence, image encryption, depth perception

0　引言

随着多媒体数据在通信、医疗、虚拟现实等领域的广泛应用，海量信息存储与传输带来的安全保障隐患日益增加。光场图像作为新兴三维信息载体，能够同时保存空间和角度信息，为高质量场景重建和智能感知提供了重要支撑[1-2]。然而，光场

收稿日期：2025–11–12；修回日期：2025–12–29
通信作者：王尔馥，wangerfu@hlju.edu.cn
基金项目：黑龙江省自然科学基金资助项目（No.LH2019F048）
Foundation Item：The Natural Science Foundation of Heilongjiang Province (No.LH2019F048)

图像具有的高维结构与丰富信息，在开放网络环境下更加容易被非法窃取与篡改，造成严重的隐私泄露和安全风险。因此，设计安全且高效的光场图像加密方法具有重要的理论意义和实际应用价值。

目前，光场图像加密的研究主要集中在两个方面：一是将传统二维图像加密算法直接应用于光场图像的每一个视点，通过像素置乱和扩散等手段实现基本的安全保护[3-4]；二是根据光场图像的多维结构特性，结合混沌加密方法进行加密[5]。尽管这些方法在一定程度上提升了加密效果，但它们未能充分利用光场图像中子孔径图像间存在的关系，影响了加密强度与效率[6-7]。作为光场图像几何特征的重要组成部分，深度信息对实现高效且安全的加密至关重要。尤其在多视点图像的加密中，深度信息能够有效区分前景与背景，通过自适应加密策略提升安全性[8]。若能够将光场图像具备的深度信息与多维结构相结合，则有望进一步提升加密系统的安全性和鲁棒性。

针对现有光场图像加密方法普遍存在的多维结构协同加密能力弱、深度信息未能有效融入加密流程等问题，本文提出了一种基于深度感知的光场图像高维混沌加密方法，主要贡献如下。

1) 提出了融合深度感知与高维混沌序列的光场图像加密方法，利用极平面法高效提取深度信息并将其引入加密过程，实现了基于深度的自适应像素置乱与扩散。

2) 设计了多级混沌驱动的全局与局部置乱及深度感知扩散方法，通过深度信息的引导，提升了加密系统在不同光场视点和深度区域下的安全性。

3) 系统地实现了光场图像的加密流程，并进行了全面的实验分析。实验结果表明，所提方法在加密效果、信息熵、相关性分析及抗统计攻击等方面均优于现有主流加密方法，能够有效实现光场图像的安全保护。

1　光场图像的深度信息及估计方法

光场图像区别于传统二维图像的核心特征在于其同时记录“角度”与“空间”等多维信息[9-11]。深度信息作为光场图像几何特征的直接载体，是实现“内容自适应加密”的核心控制变量[12-14]。针对场景中深度小的前景，应当加强扰动以提高安全性；对于深度大的背景，可以减弱扰动以提高加密效率，使加密策略更匹配光场图像的三维结构特性，避免传统加密方式导致安全性与视觉质量失衡[15]。因此，选择适配性强、精度可靠的深度估计方法是重中之重。

1.1　光场深度估计方法

光场深度估计的本质是从多视点图像的关联中反推场景三维结构。现有的主流方法可分为3类：视差匹配法、深度学习法及极平面图像（epipolar plane image，EPI）法[16-18]。

视差匹配法通过计算不同视点间同一像素的位移（视差）反推深度，如Dansereau等[19]提出的光场相机标定解码。这种方式依赖高精度视点配准与纹理丰富的场景。光场图像通常包含遮挡区域或纯色墙壁等弱纹理区域[20]，此时视差匹配易出现误匹配，导致深度估计误差超过15%。而深度误差会直接引发加密时“前景”与“背景”的误判，进而削弱自适应加密的安全性。

深度学习法通过端到端卷积神经网络学习光场深度特征，如Shin等[21]提出的EPINET。这种方式虽然能实现高精度深度估计，但依赖大规模标注光场数据集（如Stanford Light Field Archive全量数据）与高性能计算资源（GPU显存≥11 GB），且推理耗时为0.93~2.04秒/幅（为EPI法的6~8倍）。加密系统需兼顾实时性，深度学习法的效率瓶颈难以适配。

EPI法通过提取光场的EPI，将深度估计转换为EPI中直线斜率的分析问题，不需要复杂配准与大规模数据，且在存在遮挡、弱纹理场景下的深度误差可控制在5%以内[22]。本文深度模块的目标不是得到高精度绝对深度，而是获得对视差结构稳定的相对深度/置信度，用于驱动局部置乱与扩散强度分配。因此本文选择与训练无关且几何可解释的EPI/结构张量路线，以避免引入深度网络的训练数据依赖与部署成本。此外，该方法具备并行化计算优势，可将EPI切片独立处理，满足精度可靠、效率适配、场景鲁棒的深度提取需求，因此本文选取EPI法作为深度信息提取的核心方法。

1.2　极平面图像法

设光场子孔径图像集合按照二维视点坐标(u,v)排布[23]，单幅分辨率为$H \times W$，分别从u、v两个维度构造水平和垂直EPI。

水平EPI（固定v，沿u聚合）：对于每个行y，

取 $E_h(u,x)=L(u,v_0,y_0,x)$，其中，$u=0,1,\cdots,U-1$，$x=0,1,\cdots,W-1$，结果是一个大小为 $U\times W$ 的图像，其中包含了一系列斜率与深度相关的直线纹理。

垂直 EPI（固定 u，沿 v 聚合）：对于每个列 x，取 $E_v(v,y)=L(u_0,v,y,x_0)$，$v=0,1,\cdots,V-1$，$y=0,1,\cdots,H-1$，结果是一个大小为 $V\times H$ 的图像。

对于每个像素位置，本文要估计其在该 EPI 上对应线条的斜率，并通过映射函数 ϕ 将斜率转换为深度值。在两平面参数化下，同一三维点 (x,y,z) 在不同视点 u 的像面坐标 $s_{(u)}$ 满足

$$s_{(u)}=\frac{f}{Z}(X-Bu)+c_s \tag{1}$$

其中，f 为等效焦距，B 为视点基线缩放系数，c_s 为像中心常数。将式(1)改写为直线形式

$$\begin{aligned} s_{(u)}&=ku+b\\ k&=-\frac{fB}{Z}\\ b&=\frac{fX}{Z}+c_s \end{aligned} \tag{2}$$

因此，斜率 k 与深度 Z 存在单调反比关系，深度 Z 可通过斜率反求

$$Z=-\frac{fB}{k} \tag{3}$$

2　深度估计鲁棒性增强

EPI 深度估计虽然通过斜率分析实现了遮挡、弱纹理场景下的基础深度提取，但在实际光场成像中，传感器噪声、EPI 直线误判仍会导致深度图存在局部误差，如边缘模糊、孤立点误判等[24]。若直接将此类深度图用于加密流程，则易引发前景/背景扰动强度错配，如将近景噪声误判为背景弱扰动。为此，需从误差隔离、噪声抑制、误差解耦 3 个方面引入鲁棒性增强策略，通过工程化设计降低深度误差对加密系统的影响，具体方法介绍如下。

1) 针对遮挡导致的局部深度失真，采用固定尺寸块内独立处理策略，避免局部误差传递至全局。将深度图与光场图像同步划分为 16 像素×16 像素的块，每个块内独立执行深度感知的置乱/扩散操作。这样的块大小既能覆盖足够的局部深度特征，避免块内深度差异过大，又能将误差限制在单个块内。若某块因遮挡导致深度误判，则仅影响该块内 256 个像素的置乱策略，不扩散至其他区域。

2) 弱纹理区域的 EPI 斜率易受噪声干扰，导致深度值波动，若采用均值阈值划分前景/背景，则易出现大量误判。通过块内深度中位数阈值替代均值阈值，提升对弱纹理噪声的鲁棒性。对于每个 16 像素×16 像素的块，计算块内所有像素深度值的中位数，将块内像素分为前景与背景，其中深度值大于中位数的像素归类为前景，反之归类为背景。相较于均值阈值，中位数阈值对弱纹理区域的孤立噪声点抵抗力更强，可有效避免弱纹理区域被误判为前景或背景。此外，对于深度值异常的块，自动启用邻域中位数补偿，进一步降低弱纹理导致的深度不确定性。

3) EPI 深度估计可能因相机标定误差（如基线 B、焦距 f 的微小偏差等）导致整体深度值偏移，若依赖固定绝对阈值，则会出现大规模误判。这里采用块内相对深度关系替代绝对深度阈值，即使深度图整体偏移（如将全局深度值增加 0.1），块内前景像素深度大于背景像素深度的相对关系仍保持不变，确保前景与背景的划分逻辑稳定。

4) 为抑制 EPI 斜率估计引入的高频噪声（如传感器噪声导致的深度值抖动），设计高斯滤波与双边滤波的两级后处理流程，在平滑噪声的同时保留深度不连续性。首先进行高斯滤波预处理，采用 5 × 5 窗口、标准差 $\sigma=1.0$，初步抑制小尺度噪声，如像素级深度抖动等，避免噪声被后续加密流程放大；其次进行双边滤波优化，采用窗口大小 $d=9$、颜色相似度标准差 $\sigma_{\text{color}}=0.1$、空间距离标准差 $\sigma_{\text{space}}=8$，通过空间距离与像素灰度相似度双重权重，在平滑深度图内部噪声的同时保留物体边缘的深度跳变。

5) 若深度误差直接主导加密密钥生成，则会导致加密强度随深度误差升高而下降。通过深度值弱调制混沌序列的设计，确保核心随机性由高维混沌系统主导，深度误差仅作为次要调节因子，减小其对加密随机性的影响。

3　混沌系统模型及其性能分析

混沌系统因具有初值敏感性、伪随机性、有界性等特性，可被广泛用于现代密码学中的“置乱与扩散”原则，在图像加密领域得到广泛应用[25-27]。但光场图像兼具“空间–角度”的高维结构与高冗余特性，其数十倍，甚至数百倍于二维图像的数据量且具有多维度关联特性，对混沌系统提出多序列

并行生成、超大规模密钥空间、强抗攻击能力等要求。传统低维混沌系统已无法满足其加密需求，设计高维混沌系统成为必然选择[28]。

3.1　高维混沌系统

高维混沌系统通过多状态变量耦合，打破低维系统局限，综合动力学复杂性、工程实现效率与光场适配性，本文设计了连续洛伦兹（Lorenz）系统 + 离散映射耦合的6维结构，具体介绍如下。

该系统由一组连续时间状态 $X=\left(x_0,x_1,x_2,x_3,x_4,x_5\right)^{\mathrm{T}}$ 的常微分方程与3个离散映射耦合而成。定义离散映射变量为 $x_{\log}$（Logistic 映射）、（Tent 映射）与 θ（Circle 映射）。连续部分的导数形式可写为

$$\begin{cases}\dot{x}_0=\sigma\left(x_1-x_0\right)+\alpha(t)y_{\text{tent}}+\gamma\theta+a_4x_3\\ \dot{x}_1=x_0\left(\rho-x_2\right)-x_1+a_5x_4\\ \dot{x}_2=x_0x_1-\beta x_2+a_6x_5\\ \dot{x}_3=-d_1x_0+e_1x_3\\ \dot{x}_4=-d_2x_1+e_2x_4\\ \dot{x}_5=d_3x_2+e_3x_5\end{cases}\tag{4}$$

其中，时间变系数 $\alpha(t)$ 由 Logistic 子映射调制

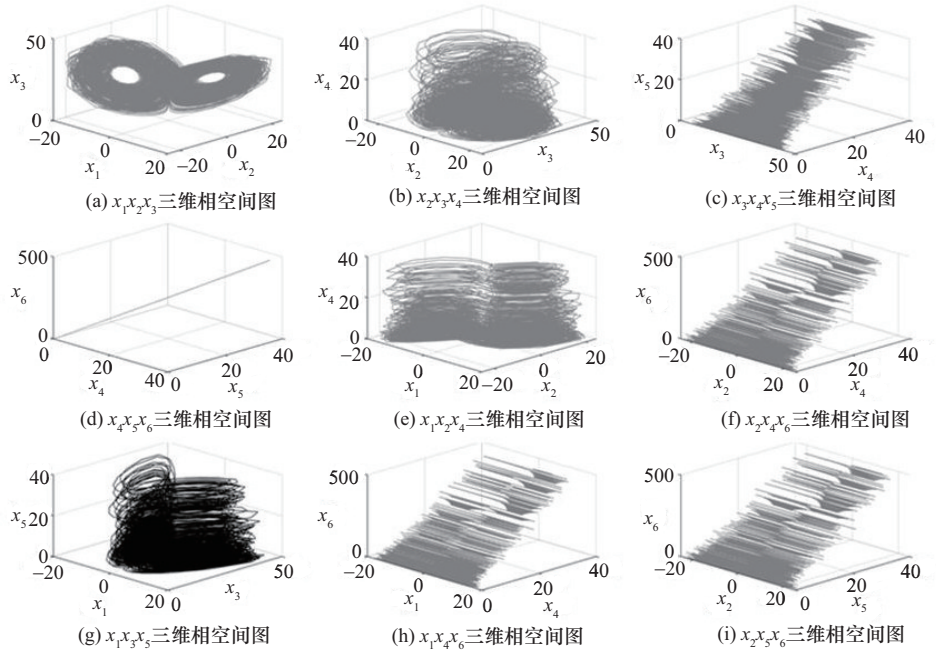
$$\alpha(t)=\alpha_{\min}+(\alpha_{\max}-\alpha_{\min})x_{\log}\tag{5}$$

$$x_{\log}{}^{(n+1)}=r_{\log}x_{\log}{}^{(n)}\left(1-x_{\log}{}^{(n)}\right)\tag{6}$$

在实现中，连续系统采用固定步长 dt 的4阶 Runge-Kutta（RK4）数值积分推进，迭代结果对每个分量取小数部分，以保持状态在[0,1)区间，从而确保后续映射为伪随机数。图1展示了6维混沌系统在9组典型三维子空间的投影。由图1可知，投影均呈现非周期、有界且拓扑复杂的轨迹形态，证明本文设计的混沌系统确实存在混沌吸引子。系统在前三维 (x_1,x_2,x_3) 的相空间图中呈现明显的蝴蝶状，这是因为该系统由 Lorenz 系统演化而来；涉及 x_6 的投影显示出缓慢演化并受到其他变量扰动的特征，后三维 (x_4,x_5,x_6) 呈现近线性相关，反映出快–慢耦合与分层动力学。上述结果共同表明本文设计的高维混沌系统具有强非线性耦合与高维混沌特性。

3.2　Lyapunov 指数

为估计系统的李雅普诺夫指数（Lyapunov exponent, LE），本文对状态方程与预期变分方程并行积分，并采用周期性正交（QR）分解重正交，按物理时间进行归一化处理。为避免初值依赖与瞬态污染，先丢弃一定步数的预热迭代阶段，再在有效区间内累积对角因子取对数并平均得到全谱 LE，如图2所示。结果谱为 { 0.978 3, −0.018 4, 0.009 9, 0.010 0, 0.010 0, −14.793 4 }，最大指数接近0.98，表明该系统对初值的敏感依赖显著；3个约为0.01的正指数



(a) $x_1x_2x_3$三维相空间图　(b) $x_2x_3x_4$三维相空间图　(c) $x_3x_4x_5$三维相空间图

(d) $x_4x_5x_6$三维相空间图　(e) $x_1x_2x_4$三维相空间图　(f) $x_2x_4x_6$三维相空间图

(g) $x_1x_3x_5$三维相空间图　(h) $x_1x_4x_6$三维相空间图　(i) $x_2x_5x_6$三维相空间图

图1　6维混沌系统吸引子在子空间的3D投影

源于从动子系统线性增益项$e_1 = e_2 = e_3 = 0.01$，代表弱扩张方向；−0.018 4为弱收缩；−14.793 4为强收缩。指数和为−13.803 6 < 0，说明系统整体为耗散；Kaplan-Yorke维数为5.067，显示吸引子具有分数维且嵌入在6维相空间中。

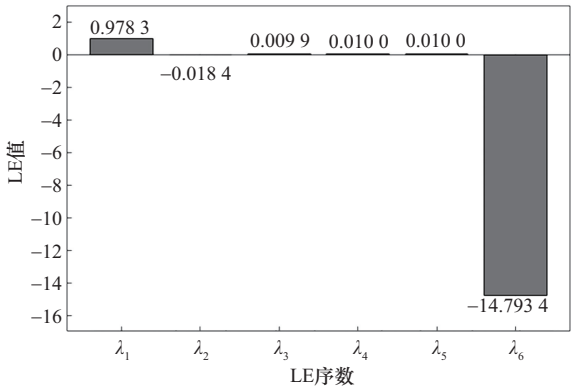


图2 全谱LE

3.3 NIST测试

本文参考NIST SP 800-22标准（National Institute of Standards and Technology, NIST）对提出的超混沌系统伪随机序列生成密钥的随机性进行了测试，测试结果如表1所示。

表1 密钥随机性NIST SP 800测试结果

测试项目	通过率	p值	评价
Frequency	99%	0.924 076	通过
BlockFrequency	98%	0.071 177	通过
CumulativeSums	99%	0.834 308	通过
Runs	98%	0.924 076	通过
LongestRun	99%	0.637 119	通过
Rank	98%	0.162 606	通过
FFT	99%	0.719 747	通过
NonOverlappingTemplate	97%	0.023~0.991	通过
OverlappingTemplate	98%	0.719 747	通过
Universal	99%	0.657 933	通过
ApproximateEntropy	98%	0.851 383	通过
RandomExcursions	98%	0.021~0.366	通过
RandomExcursionsVariant	96%	0.001~0.595	通过
Serial	100%	0.455~0.851	通过
LinearComplexity	97%	0.554 420	通过

从表1可以看到，本文提出的伪随机序列生成器生成的密钥通过全部测试，平均通过率为98.2%，体现了较强的加密随机性。由测试结果可知，该系统频率特性良好，序列复杂度高且统计分布均匀，证明了该混沌系统在生成高质量随机序列方面的有效性。

4 光场图像加密系统设计

本节提出了一种基于深度感知的光场图像高维混沌加密系统。首先介绍该系统总体架构，之后分析该系统的3个主要模块：EPI深度分析模块、混沌密钥生成模块以及多级加密处理模块。

4.1 加密系统架构

光场图像加密系统设计框架如图3所示。首先，将输入光场图像$L(x,y,u,v)$按视点顺序读入，作为EPI深度提取模块的输入，输出为归一化并后处理的深度图$D(x,y)$；其次，将所有子孔径图像的像素序列按固定顺序串接，输入SHA-256函数，得到256位图像哈希向量$\boldsymbol{H}$，作为混沌系统参数和初始状态向量生成模块的输入；再次，输出高维混沌序列，并被多级加密处理模块调用，实现视点级全局置乱、像素级全局置乱、块内深度感知局部置乱、多轮深度增强扩散及跨视点块级交换；最后，输出密文光场图像$L_c(x,y,u,v)$及元数据。

4.2 EPI深度分析

为使加密过程能够感知场景的三维结构，本系统在光场图像中提取基于EPI的深度信息，并对深度图进行规范化与鲁棒后处理。EPI中同一物体在不同视点的成像近似直线，其斜率与视差成比例关系，视差与逆深度近似线性相关，故可由“主方向一致性”估计深度。

图4展示了从Stanford光场数据“Lego Knights”中提取的水平与垂直EPI示例[29]。从图4可以观察到，场景中的物体在EPI中呈现出清晰的直线纹理，其斜率与物体到相机的距离成反比关系，即斜率绝对值越大，物体距离越近。

为量化分析EPI中的线条方向，系统首先将彩色EPI图像转换为灰度图，随后采用Sobel算子计算每个像素点在水平(x)和垂直(y)方向上的梯度值（∇_x,∇_y）。梯度幅值$\mathrm{Mag} = \sqrt{\nabla_x^2 + \nabla_y^2}$反映了该点边缘的强度，梯度方向$\theta = \arctan2\left(\nabla_y,\nabla_x\right)$展现了线条的法线方向信息。

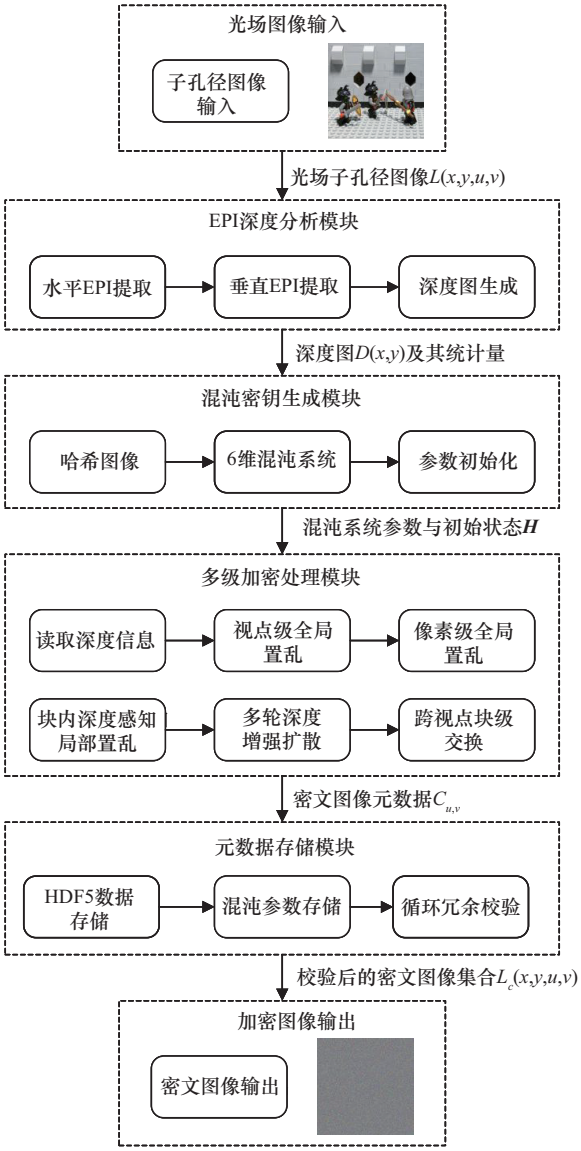
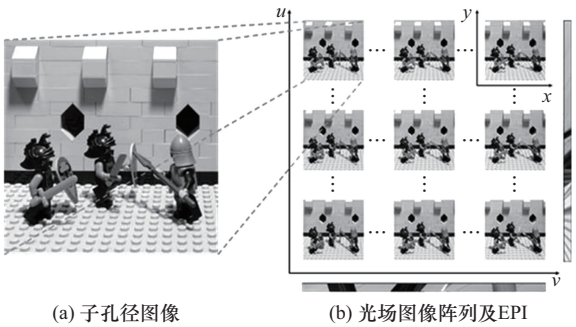


图3　光场图像加密系统设计框架



(a) 子孔径图像　　(b) 光场图像阵列及EPI

图4　光场子孔径图像及EPI

由于简单的斜率计算对噪声敏感，因此采用结构张量法计算EPI图像中每个像素点的局部主导方向。对于EPI图像中的每一个像素点，其周围窗口内的结构张量$\boldsymbol{M}$可表示为

$$\boldsymbol{M}=\begin{bmatrix}\sum\nabla^2 x & \sum\nabla x\nabla y\\ \sum\nabla x\nabla y & \sum\nabla^2 y\end{bmatrix} \tag{7}$$

其中，求和均在局部窗口内进行，计算结构张量$\boldsymbol{M}$的特征值和特征向量。其特征值的大小反映了该窗口内梯度的一致性程度，主导方向（最大特征值的特征向量方向）为该局部区域线条的法线方向。线条的斜率k可由法线方向推导。最终，该点的深度值d与斜率k的对应关系可简化为

$$d\propto\frac{1}{|k|} \tag{8}$$

通过对水平和垂直EPI图像中的每一个像素点进行上述计算，可以得到两个初始的深度估计图D_h和D_v。由于存在噪声、遮挡和边界效应，EPI从单一方向得到的深度图通常不完整且存在噪声。这里采用一种简单的像素级取大策略进行融合：对于空间中的每一个像素点(x, y)，其最终的深度值$D(x,y)$取$D_h(x,y)$和$D_v(x,y)$中绝对值较大的一个，即

$$D(x,y)=\max\left(D_h(x,y),D_v(x,y)\right) \tag{9}$$

只要一个结构在至少一个方向上能够被可靠地检测到，那么就应当保留其深度信息。融合后的深度图需进行后处理以平滑噪声并保持边缘，这里采用高斯滤波进行初步平滑，抑制小的噪声点。随后将深度值线性归一化到[0,1]，便于后续加密算法统一处理。最后采用双边滤波器进行最终优化。双边滤波能在平滑深度图内部区域的同时，较好地保留由物体边界不规律导致的深度不连续性边缘。

4.3　混沌密钥生成

系统采用基于内容哈希的全局密钥生成策略，通过SHA-256哈希函数生成确定性密钥，以确保加密过程的安全性与一致性。对于包含$u\times v$张光场子孔径图像的输入序列$\{I_1,I_2,\cdots,I_{uv}\}$，将所有子孔径图像按视点索引拼接为一维像素序列后，输入SHA-256算法，得到256位外部密钥向量，同时将深度值$D(x,y)$的统计特征（如均值、方差）拼入哈希输入，以引入内容相关性。该过程不仅考虑了图像的像素值信息，还包含了图像的几何结构与空间分布特征，从而生成唯一密钥。为了便于后续的混沌系统参数计算，系统将256位外部密钥K分为32个8位块，即

$$K=\{K_1,K_2,\cdots,K_{32}\} \tag{10}$$

其中，每个K_i为8位二进制数，$1\leqslant I\leqslant 32$。每个8位块可以表示[0,255]的数值范围，为混沌系统的参数调整提供了足够的精度。这种分块策略不仅简化了计算复杂度，还为不同维度的混沌系统提供了独立的参数空间。

基于密钥K的统计特性，系统生成高维混沌系统的初始状态向量。该初始状态的选择首先要求各分量数值处于较小量级。一方面，可避免在RK4数值积分初期出现状态急剧发散或进入饱和区，保证状态始终处于设定的有界吸引子内，从而维持混沌行为的稳定性；另一方面，小量级初始值结合步长dt有利于在双精度浮点表示下保持足够有效的位数，减小数值舍入误差对长期积分的累积影响，确保生成的密钥序列具有稳定的统计特性。

4.4 多级加密处理

为保证加密流程的模块化与安全性，本文利用6维混沌系统并行产生多条伪随机通道，将光场加密划分为5个相互协同的层级：Level 1视点级全局置乱、Level 2像素级全局置乱、Level 3块内深度感知局部置乱、Level 4多轮深度增强扩散以及Level 5跨视点块级交换。设光场子孔径图像集合为

$$\{I_{u,v}(x,y)|u=0,\cdots,U-1,v=0,\cdots,V-1\} \tag{11}$$

单幅分辨率为$H\times W$，共$N=U\times V$个视点。EPI深度估计和后处理得到的归一化深度图为$D(x,y)\in[0,1]$，并与各子孔径图像在空间上对齐。多级加密在角度维与空间维上逐级引入置乱和扩散，有效提升对统计分析与差分攻击的抵抗能力。

Level 1：视点级全局置乱使用S_3通道，对整个光场的视点顺序进行全局重置，通过改变子视点的索引顺序，提高跨视点攻击的难度。将二维视点坐标(u,v)按行优先方式展开为一维索引，由混沌系统得到经过归一化长度为N的序列$\{s_n\}$，对其按数值从小到大排序，获得置乱索引$p_{(n)}$。则置乱后的子孔径图像可表示为

$$I'_{\tilde{u},\tilde{v}}(x,y)=I_{u,v}(x,y) \tag{12}$$

其中，$(\tilde{u},\tilde{v})$对应置乱索引$p_{(n)}$。在最初阶段，打乱视点顺序可明显增加观察者与攻击者对视点间关联的恢复难度，且在解密时以相同的序列重排回到原始顺序。

Level 2：像素级全局置乱(S_1,S_2)对每个色彩通道内的像素执行全局置乱，打破整体与局部的空间统计特性。采用S_1+S_2的组合作为排序键可增加序列复杂度并降低单通道相关性，且在解密时以逆序恢复像素顺序。以视点(u,v)的某一色彩通道为例，将$I'_{u,v}(x,y)$按行优先展平为一维像素序列$X_{u,v}$。由混沌系统得到经过归一化长度为N_P的序列$\{s_{(u,v)}(k)\}$，按数值排序得到像素置乱索引$P_{u,v}$。像素级全局置乱后的序列为

$$X'_{u,v}(k)=X_{u,v}(P_{u,v}(k)),k=0,1,\cdots,N_P-1 \tag{13}$$

对RGB的3个色彩通道分别执行同样的置乱操作，最后将$X'_{u,v}$重构为二维图像$I''_{u,v}(x,y)$。该步骤打破了图像的局部空间相关性，使相邻像素在一维序列中的位置高度随机化，显著削弱了基于空间邻域统计的攻击。解密时按$P_{u,v}$的逆序置乱即可恢复像素位置。

Level 3：块内深度感知局部置乱(S_1,S_2)在块级范围内，结合深度图将块内像素分为“前景”与“背景”，并分别按通道分配的随机得分排序，实现深度感知的局部置乱。在块内保留深度结构相关性的同时，以深度为依据改变像素排列，有利于在不完全破坏可感知结构的同时提高安全性。将$I''_{u,v}(x,y)$与深度图$D(x,y)$同步划分为$B\times B$个像素块（本文取$B=16$）。记第(p,q)个块为

$$B_{p,q}=\{(x,y)|x\in[pB,(p+1)B-1],y\in[qB,(q+1)B-1]\} \tag{14}$$

对于每个块，收集对应的深度值集合为$\{D(x,y)|(x,y)\in B_{p,q}\}$，计算块内深度中位数阈值$T_{p,q}$。根据中位数将块内像素划分为“前景”与“背景”两个集合

$$\begin{aligned}\Omega_a^{p,q}&=\{(x,y)\in B_{p,q}|D(x,y)>T_{p,q}\}\\ \Omega_b^{p,q}&=\{(x,y)\in B_{p,q}|D(x,y)\leqslant T_{p,q}\}\end{aligned} \tag{15}$$

由混沌系统的伪随机通道为每个块分别产生两组实值序列$\{\alpha_i^{p,q}\}$与$\{\beta_j^{p,q}\}$，其中索引i与j对应$\Omega_a^{p,q}$与$\Omega_b^{p,q}$的像素位置。对这两组序列分别排序，得到块内前景和背景的置乱索引$P_a^{p,q}$和$P_b^{p,q}$。随后，在保持前景像素集合与背景像素集合互不交叉的前提下，仅改变集合内部像素的排列顺序，即对任意视

点(u,v)，有

$$I'''_{u,v}\left(\Omega_a^{p,q}(i)\right)=I''_{u,v}\left(\Omega_a^{p,q}\left(P_a^{p,q}(i)\right)\right)$$
$$I'''_{u,v}\left(\Omega_{\mathrm{b}}^{p,q}(j)\right)=I''_{u,v}\left(\Omega_b^{p,q}\left(P_b^{p,q}(j)\right)\right) \tag{16}$$

这样不仅保留了块内前景/背景的相对分布，有利于后续基于深度的扩散调制，在局部范围内也引入了较强的空间置乱，进一步削弱了可见结构。块间互不交叉，各块处理过程彼此独立，可并行实现。

Level 4：多轮深度增强扩散(S_1,S_2,S_3,S_4)通过前向/反向多轮扩散将像素值与伪随机流混合，在扩散过程中根据深度信息调整每个像素的密钥强度，以实现前景与背景不同强度的扰动。记经过 Level 3 处理后的视点(u,v)图像展平为一维序列$P_{u,v}$，对应位置的归一化深度值为$\left\{d_{u,v}(k)\in[0,1]\right\}$。定义深度权重为

$$\omega_{u,v}(k)=1+\gamma d_{u,v}(k) \tag{17}$$

其中，$\gamma>0$为调节系数，是线性调节权重跨度，当γ较小时，自适应差异不足；当γ过大时，深度噪声也会被同步放大，导致局部扰动出现过饱和。因此本文令$\gamma=1$，使ω的范围稳定在$[1,2]$，在保证自适应差异的同时抑制深度噪声放大风险。据此构造4组深度增强密钥序列

$$K_i(k)=\left[S_i(k)\cdot 10^8\cdot\omega_{u,v}(k)\right]\bmod 256,\ i=1,2,3,4 \tag{18}$$

多轮深度增强扩散采用“前向–反向–前向–反向”的4轮结构。记初始输入为

$$C^{(0)}(k)=P_{u,v}(k) \tag{19}$$

第1轮（前向）为

$$C^{(1)}(0)=C^{(0)}(0)\oplus K_1(0)$$
$$C^{(1)}(k)=C^{(0)}(k)\oplus K_1(k)\oplus C^{(1)}(k-1),k=1,\cdots,N_P-1 \tag{20}$$

第2轮（后向）为

$$C^{(2)}(N_P-1)=C^{(1)}(N_P-1)\oplus K_2(N_P-1)$$
$$C^{(2)}(k)=C^{(1)}(k)\oplus K_2(k)\oplus C^{(2)}(k+1),k=N_P-2,\cdots,0 \tag{21}$$

第3轮（前向）为

$$C^{(3)}(0)=C^{(2)}(0)\oplus K_3(0)$$
$$C^{(3)}(k)=C^{(2)}(k)\oplus K_3(k)\oplus C^{(3)}(k-1),k=1,\cdots,N_P-1 \tag{22}$$

第4轮（后向）为

$$C^{(4)}(N_P-1)=C^{(3)}(N_P-1)\oplus K_4(N_P-1)$$
$$C^{(4)}(k)=C^{(3)}(k)\oplus K_4(k)\oplus C^{(4)}(k+1),k=N_P-2,\cdots,0 \tag{23}$$

最终得到的序列$C_{u,v}=\{C^{(4)}(k)\}$重构为二维图像，即该视点的密文图像。可以看出，4轮扩散分别利用深度加权后的4条密钥流$\{K_i\}$，通过前向和后向的链式异或结构将单像素扰动在全局范围内传播。深度权重$w_{u,v}(k)$使深度较大的区域（如靠近相机的前景）在扩散过程中受到更强扰动，从而进一步提升对选择性明文攻击和局部篡改攻击的鲁棒性。

Level 5：跨视点块级交换(S_5,S_6)在每个视点层面将相同位置的块在不同视点间交换，破坏视点间的直接空间对齐关系，从而增加从少量视点恢复场景的难度。记Level 4输出图像在视点(u,v)、块索引(p,q)处的块为$B^{(4)}_{u,v,p,q}$，由混沌系统对每个块索引(p,q)产生长度为N的序列$\left\{S_{u,v,p,q}\right\}$，按值排序可得到跨视点置乱索引$P_{p,q}$。再将一维索引映射回对应的视点坐标，可得跨视点块级交换结果。跨视点交换在像素级别上增加了一层结构混淆，尤其是对基于视点一致性（如EPI方法）进行攻击时可显著降低可恢复信息量，且通过独立通道驱动可避免与像素级置乱及扩散序列产生直接相关性。

5　加密结果与分析

本节旨在通过全面的实验验证和性能分析，评估所提出的基于深度信息的光场图像混沌加密系统的有效性与安全性。经过逐级加密分析、密文图像分析及密文质量分析，本节有效地证明了本文设计的加密算法具有高质量加密强度及密文安全性。

5.1　实验条件

从计算复杂度角度看，所提加密流程的各个环节均只需要对全部像素或像素块进行有限次遍历。视点级全局置乱仅对$U\times V$个视点索引进行一次排序，时间复杂度约为$O(UV\log(UV))$，相对于光场总体像素规模可忽略不计；像素级全局置乱通过对单视点大小为$N_p=H\times W$的混沌序列进行排序生成置乱索引，严格意义上时间复杂度为$O(N_p\log N_p)$，对全部$U\times V$个视点执行该操作的时间复杂度约为$O(UVN_p\log N_p)$，其中，$\log N_p$在

典型分辨率（如512像素 × 512像素）下为一较小常数；块内深度感知局部置乱、多轮深度增强扩散以及跨视点块级交换等步骤均为线性扫描或常数规模块内操作，时间复杂度均为$O(N)$，其中$N = U \times V \times H \times W$为光场像素总数。因此，除像素级全局置乱中排序操作带来的$\log N_p$因子外，其余环节均为线性复杂度，整体时间开销随光场数据规模呈近似线性增长趋势。

本文采用斯坦福大学光场数据集（The Stanford Light Field Archive）中具有代表性的光场图像进行加密仿真。这里选择光场图像“Lego Knights”，其具有289（17 × 17网格）个视点，子孔径图像分辨率为1 024像素 × 1 024像素。在处理器 Intel Core i5-10200H、显卡 NVIDIA GeForce GTX 1650Ti、Python版本3.11.4运行环境下，完整加密总耗时约为1 500 s，如表2所示。

由表2可知，深度估计与混沌序列生成分别为474.71 s与370.22 s，为主要开销来源；Level 2、Level 3、Level 4、Level 5的额外计算耗时分别为7.24 s、51.00 s、58.32 s、7.20 s，且Level的增量代价很小。为便于不同分辨率与不同视点数量设置下的横向对比，本文除报告整组光场加密总时间外，进一步引入归一化效率指标吞吐率，其他耗时表示未细分到各模块的额外开销（如图像解码、内存分配与调度开销等）。考虑到本文在完整光场数据上引入了视点级全局置乱、块内深度感知局部置乱以及多轮深度增强扩散等额外安全机制，该加密效率对离线光场传输与存储等应用场景仍具有较好的工程实用性。后续可通过GPU并行化以及压缩编码联合优化等方式进一步降低加密时延，以满足对实时性要求更高的应用需求。为提升数值稳定性并保证混沌强度与可积性之间的平衡，混沌系统采用如下参数：$\sigma = 10.0$，$\rho = 28.0$，$\beta = \dfrac{8}{3}$，$\alpha_{\text{tent}} = 1.8$，$r_{\log} = 3.99$，$\gamma = 0.03$；耦合强度$a_4 = a_5 = a_6 = 0.01$；阻尼$d_1 = d_2 = d_3 = 0.001$；增益$e_1 = e_2 = e_3 = 0.01$。

5.2 加密过程分析

5.2.1 视点级全局置乱

对于“Lego Knights”光场图像，原视点索引i的范围是0~288（共289个视点）。通过置乱函数，得到如图5所示的结果。

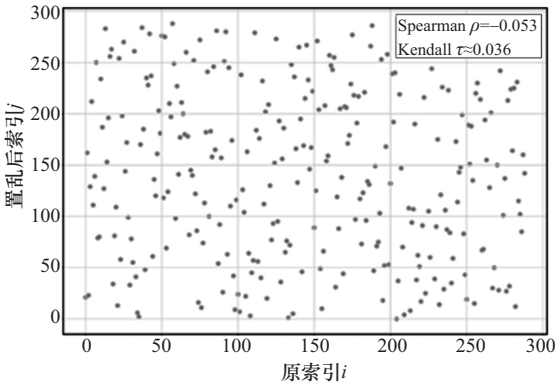


图5 索引置乱散点

从图5可以看到，点云均匀分布在整个平面内，无明显斜带与结构，说明通过置乱后序列与原序列几乎不存在线性或单调关系。其中，秩相关系数Spearman ρ与Kendall τ的值均接近0，表示单调性被破坏，置乱后序列与原序列基本不相关，与散点“均匀云团”的视觉效果一致。这说明视点级全局置乱有效破坏了原有的时序/邻近结构，为后续像素级与块级操作提供了更强的安全基础。

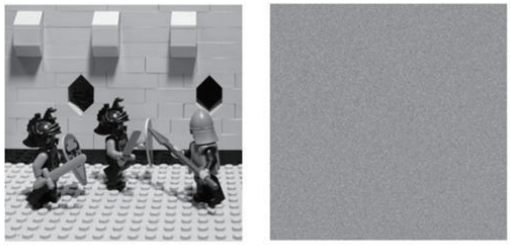
5.2.2 像素级全局置乱

由于视点级全局置乱不改变单个子孔径内部的像素分布，因此需要进行像素级全局置乱以改变每个像素点的位置。像素级置乱图像如图6所示。由图6(b)可知，通过像素级全局置乱后，子孔径图像呈现“彩色椒盐噪声”外观，这是因为

表2 逐级加密耗时分析结果

加密方案	总耗时/s	吞吐率/(Mpix·s^{-1})	深度耗时/s	混沌耗时/s	Level 2耗时/s	Level 3耗时/s	Level 4耗时/s	Level 5耗时/s	其他耗时/s
Level 1	889.642	1.021 9	—	384.50	—	—	—	—	471.92
Level 1~Level 2	799.004	1.137 8	—	370.93	7.44	—	—	—	390.63
Level 1~Level 3	906.412	1.003 0	—	374.29	7.25	50.75	—	—	448.69
Level 1~Level 4	1 511.078	0.601 6	471.02	380.73	7.15	51.12	60.40	—	515.16
Level 1~Level 5	1 513.825	0.600 5	474.71	370.22	7.24	51.00	58.32	7.20	519.78

像素被打乱，空间邻接关系被彻底破坏，总体像素分布不变，信息熵在统计上保持不变。



(a) 原始图像　　(b) 像素级置乱后图像

图6　像素级置乱图像

5.2.3　块内深度感知局部置乱

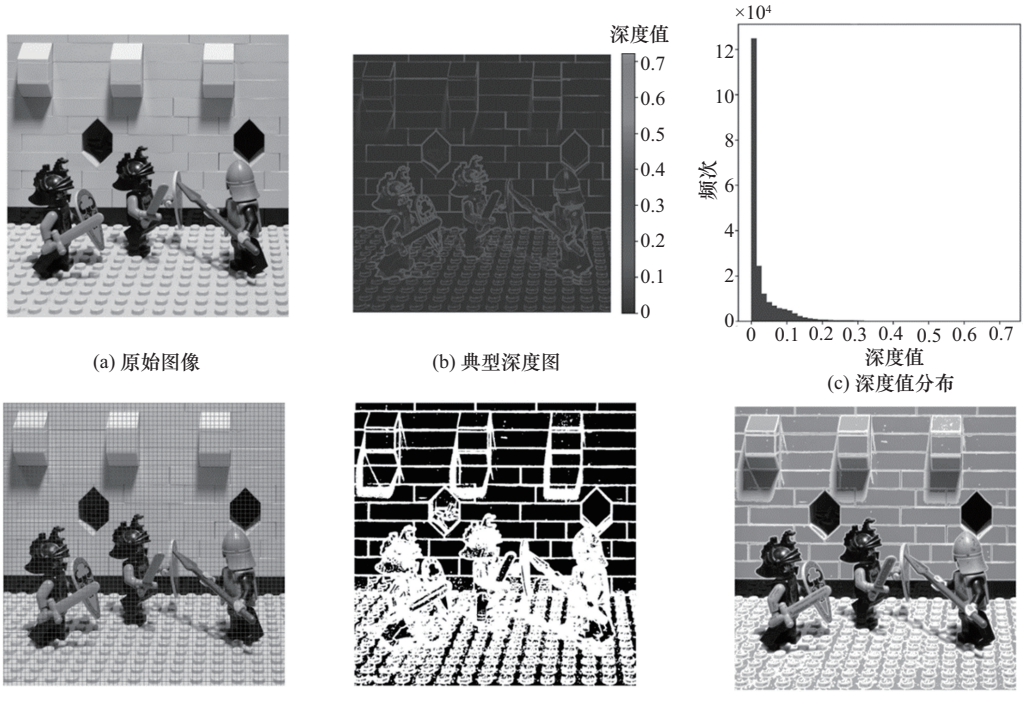
在像素级全局置乱的基础上，引入内容自适应的局部重排策略，利用深度信息对不同结构显著性区域实施差异化打散，进一步破坏空间相关性并增强抗几何/边缘重建攻击的能力。

采用基于EPI的结构张量法估算深度响应，对光场子孔径图像垂直和水平方向提取EPI切片，计算梯度方向一致性并归一化至[0, 1]。图7(b)为典型深度图，高亮区域对应高梯度、高结构显著性的前景物体边缘，深色区域对应低梯度背景平坦区。从图7(c)可以看出，深度值分布呈长尾特征，低值像素占绝大多数，高值像素较少，表示背景面积大，前景面积较小，最大深度值为0.722，均值为0.034，标准差为0.058，中位数阈值为0.009。

首先，根据中位数阈值将图像分为前景（2 824块像素）与背景（1 272块像素），前者对应物体轮廓、砖块边缘等高结构区，后者对应墙壁、地面等平坦区。然后，对前景块的块内像素进行排序，按排序后的索引重排像素值，由于前景区边缘梯度大，结构显著，强置乱可有效破坏边缘连续性与纹理相关性，抵抗轮廓提取、物体识别等攻击；对背景块仍然进行排序置乱，但由于平坦区像素值更均匀，置乱后视觉变化相对温和，在保证打散的同时降低计算开销与误差累积风险。块间不交叉，各块独立可并行计算，解密时按同一分区与序列生成逆排序恢复。

5.2.4　多轮深度增强扩散

本节采用的多轮深度增强扩散操作严格按照第4.4节Level 4中给出的算法实现：首先将经前三级置乱后的子孔径图像展平成一维序列$P_{u,v}$，并与对齐的归一化深度值构造深度权重$\omega_{u,v}(k)$；随后由混沌系统产生4条伪随机密钥流，完成“前向–反向–前向–反向”4轮链式异或扩散，得到最终密文序列。在此基础上，本节主要从信息熵、平均变化



(a) 原始图像　　(b) 典型深度图　　(c) 深度值分布

(d) 块分割（块大小16×16）　　(e) 前景（白色）/背景（黑色）分区　　(f) 分区叠加原图（亮=前景，暗=背景）

图7　块内深度感知分析

强度（unified average changing intensity，UACI）等角度分析扩散轮数对加密性能的影响。由图8(a)可知，UACI在第1轮扩散后约为32.43%，在第2轮扩散后即达到理论期望值，在第3轮扩散后不再显著提升，说明像素值差异已充分随机化，继续增加轮次对提升随机性帮助很小。由图8(b)可知，熵值在第1轮即达到饱和，各轮熵值≈ 7.999 8，像素值分布已接近均匀，信息含量达到上限。综合两条曲线可知，本实验采用3轮扩散，既能达到安全目标，又能避免过度计算。

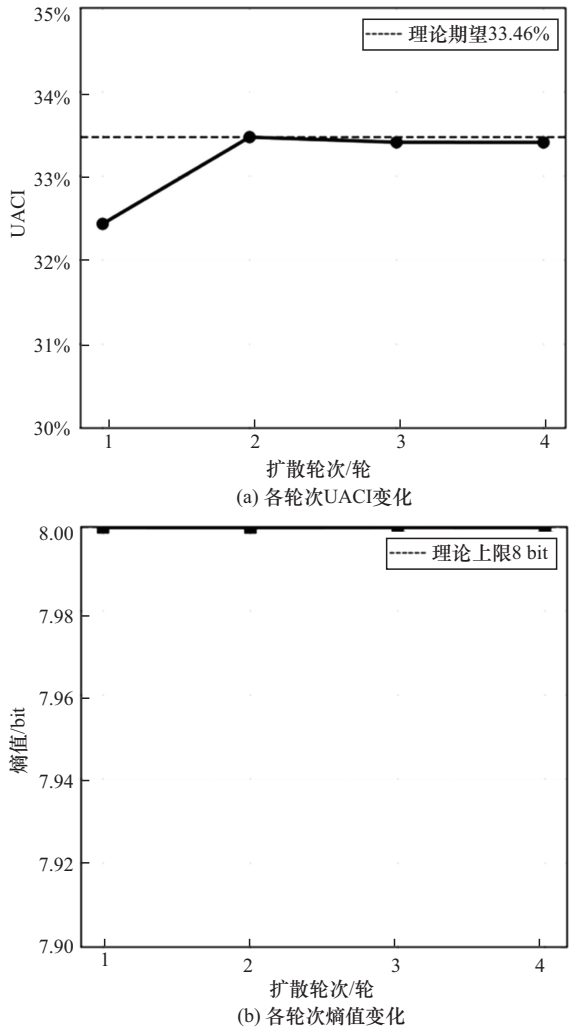


图8　多级扩散UACI与熵值变化

5.2.5　跨视点块级交换

图9(a)展示了跨视点块交换矩阵呈现细密均匀的噪声纹理，无明显条带、斑块或结构性图案，说明每个视点的每个块被交换到目标视点是接近等概率随机选择的。

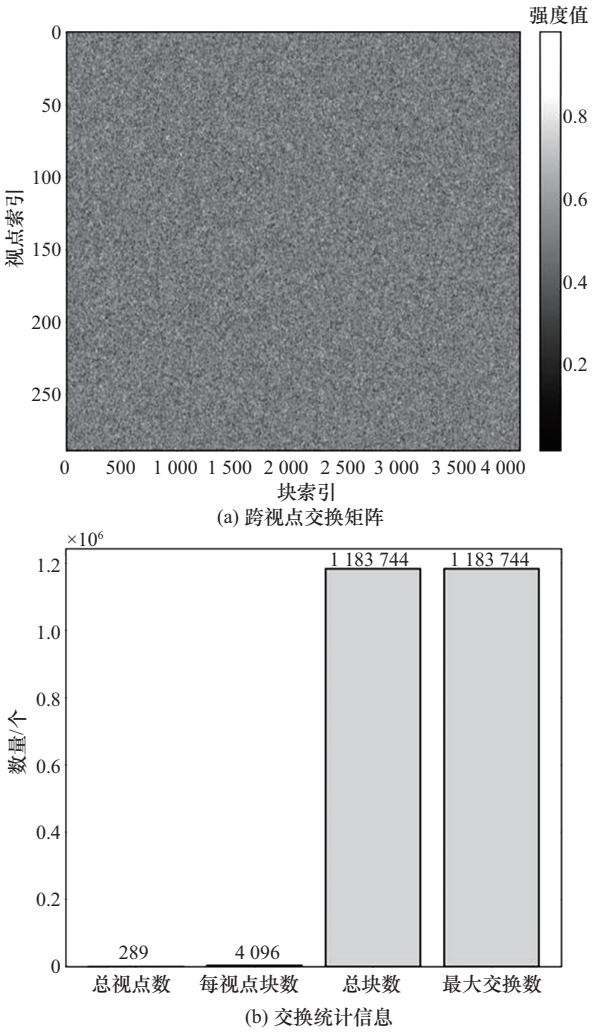


图9　跨视点块级交换分析

具体而言，交换算法对每个视点v的块b使用混沌序列生成目标视点索引，将视点v的块b与视点t的相同位置块互换。均匀噪声特征表明，交换目标的分布接近白噪声、无可预测模式，攻击者无法从交换规律推断视点间的几何关系或原始对应关系，即使掌握部分视点信息也难以重建其他视点。这一随机性特征最大化地打乱了多视点间的冗余相关性，为抵抗多视图重建、立体匹配、视点插值等攻击提供了有效保护。图9(b)通过柱状图量化了交换的规模与覆盖度，总块数与最大交换数相等，说明交换采用全覆盖策略，所有块均参与重组，无遗漏、无偏置。这一规模同时说明交换的范围广、强度大，能够充分削弱视点间的残余空间相关性。与视点级全局置乱互补，在块级别进一步跨视点重组内容，双重机制共同破坏了多视点光场原有的时序依赖与空间冗余。该层为整体加密提供了独特的多

视点维度防护，显著提高了对利用多视点几何约束进行重建或匹配类攻击的抵抗能力，是光场加密区别于单视点图像加密的关键安全增强环节。

5.2.6　各层级贡献分析

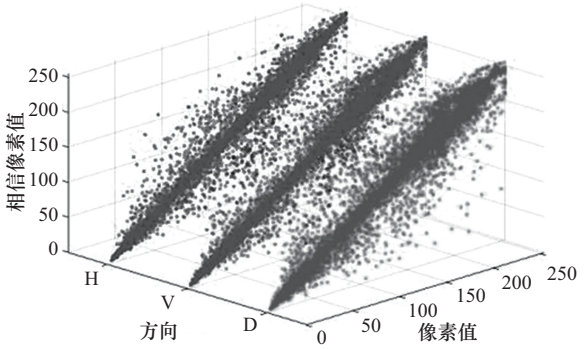
本节对加密过程进行拆解，构造了 5 种变体：仅 Level 1、Level 1~Level 2、Level 1~Level 3、Level 1~Level 4、Level 1~Level 5，在相同光场数据规模下进行评测（“Lego Knights”光场图像，289 个视点，1 024×1 024×3）。在每种变体下，本节分析以下指标：一阶统计随机性、局部结构泄露风险、光场角度冗余破坏以及差分扩散强度。逐层贡献分析结果如表 3 所示。由表 3 可知，五级架构并非简单叠加，而是针对不同攻击面形成互补增强。

从 Level 1 到 Level 1~Level 2，信息熵从 7.140 0 提升到 7.631 1，χ^2 从 1.83×10^6 下降到 416 332.278，同时差分扩散显著增强：像素变化率（number of pixel change rate，NPCR）从 93.516 0% 提升到 99.579 6%。这表明 Level 2 对直方图均匀化与差分扩散具有决定性作用。在熵已趋于饱和的情况下，Level 3 仍能把相邻像素相关性显著降低：水平相关性（corr_h）从 0.171 8 进一步降至 0.001 5，接近理想的 0；垂直相关性（corr_v）、对角线相关性（corr_d）也接近 0。这说明仅依赖熵这一阶统计指标不足以刻画密文的结构泄露风险，而 Level 3 对消除局部空间统计结构具有关键贡献。由于熵在 Level 2 后已基本饱和，Level 4 与 Level 5 对熵提升有限属正常现象，因此本节引入跨视点相关性作为光场数据的补充指标。结果显示：完整方案的跨视点相关性（cross-view corr）进一步降低至接近 0，说明跨视点角度冗余被彻底破坏，更符合光场多视点数据的安全保护目标。与此同时，NPCR 在 Level 1~Level 3 之后维持在高水平（约 99.610 0%），表明扩散能力在完整链路下已充分建立。

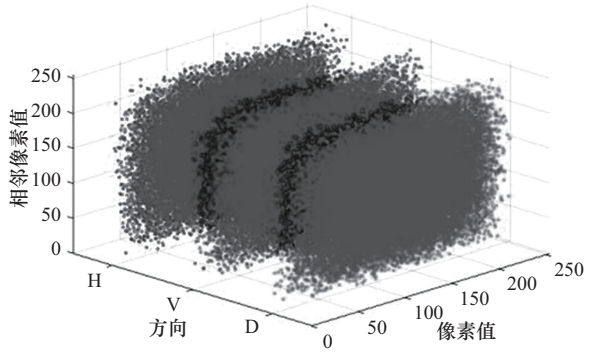
5.3　密文图像分析

5.3.1　相关性分析

为直观展示所提出的加密方法对像素间统计相关性的影响，本节在明文和密文上分别统计并绘制了相邻像素对的像素值分布，如图 10 所示。



(a) 明文图像相邻像素相关性



(b) 密文图像相邻像素相关性

图 10　加密前后像素相关性分析

相邻像素相关性系数计算式为

$$C_{xy}=\frac{L_s\sum_{i=1}^{L_s}\left(x_iy_i\right)-\sum_{i=1}^{L_s}x_i\sum_{i=1}^{L_s}y_i}{\sqrt{\left(L_s\sum_{i=1}^{L_s}x_i{}^2-\left(\sum_{i=1}^{L_s}x_i\right)^2\right)\left(L_s\sum_{i=1}^{L_s}y_i{}^2-\left(\sum_{i=1}^{L_s}y_i\right)^2\right)}} \tag{24}$$

其中，x_i 和 y_i 表示相邻像素值，L_s 表示随机所选总

表 3　逐层贡献分析结果

加密方法	信息熵	χ^2	corr_h	corr_v	corr_d	cross-view corr	NPCR
Level 1	7.140 0	1.83×10^6	0.974 7	0.974 1	0.952 3	0.723 38	93.516 0%
Level 1~Level 2	7.631 1	416 332.278	0.171 8	0.124 2	0.086 6	0.012 88	99.579 6%
Level 1~Level 3	7.632 4	414 202.514	0.001 5	−0.001 4	0.000 7	0.013 53	99.610 0%
Level 1~Level 4	7.632 3	414 436.589	0.000 6	−0.001 6	−0.000 2	0.013 64	99.610 6%
Level 1~Level 5	7.632 5	414 126.066	−0.000 1	0.000 5	0.002 9	−0.000 09	99.610 7%

像素对数。从原始光场子孔径图像中随机抽取 2 000 个像素位置，分别取其水平方向（H）、垂直方向（V）和对角线方向（D）的相邻像素构成像素对。从坐标系中可知，原始图像三方向像素值呈明显的线性分布，反映了高度的邻域相关性。在经过全局置乱与像素值扩散后，点云分布近似均匀并缺乏可辨识的线性结构。

5.3.2　直方图分析

为直观对比加密前后图像的像素分布变化，对原始图像和密文的像素分布进行直方图分析，如图 11 所示。

从图 11(b)~图 11(d)可以看出，原始图像的 RGB 三通道直方图呈现明显的峰值分布，像素值集中在特定区域；从图 11(f)~图 11(h)可以看出，密文的像素分布接近理想的均匀分布，所有像素值出现的频率大致相等。直方图分析显示，密文的像素分布通过了卡方检验。RGB 三通道的 χ^2 值分别为 255.7、278.9 和 245.5，均小于显著性水平 $\alpha = 0.05$ 下的临界值 293.2，对应的 p 值分别为 0.476、0.145 和 0.654，均大于 0.05。这证明密文的像素分布与理论均匀分布无显著差异。此外，密文的像素均值为 127.5 ± 0.1，标准差为 73.9 ± 0.0，与均匀分布的理论值（$\mu = 127.5, \sigma = 73.9$）高度吻合，进一步验证了系统的统计均匀性。这表明加密系统能够有效隐藏图像内容的统计规律，抵抗基于直方图的统计分析攻击。

5.3.3　密钥空间分析

理想图像加密算法需要足够的密钥空间来抵抗暴力攻击。根据 NIST 标准，当密钥空间大于 2^{100} 时，可以认为其具备足够的安全性。该系统密钥采用的密钥向量为

$$\begin{aligned}\mathbf{key} = \{ & y_0,z_0,w_0,u_0,v_0,\sigma,\rho,\beta,\alpha_{\min},\alpha_{\max},\alpha_{\text{tent}},\\ & r_{\log},\gamma,a_4,a_5,a_6,d_1,d_2,d_3,e_1,e_2,e_3\}\end{aligned} \tag{25}$$

其中，混沌参数部分，初始值 x_0,y_0,z_0,w_0,u_0,v_0 及其控制参数采用双精度浮点数存储，精度值为 10^{-15}，组合后密钥空间为 10^{90}；随机整数部分，深度强度因子为单精度浮点数，精度值为 10^{-7}，其密钥空间为 10^7。综上，总密钥空间为 $S_{\mathbf{key}} = 10^{90} \times 10^7 = 10^{97} \approx 2^{322}$，该密钥空间远超 NIST 标准要求的安全阈值 2^{100}，可有效抵抗暴力攻击。

5.3.4　差分攻击分析

差分攻击是密码学中一种重要的密码分析方法，通过分析明文微小变化对密文产生的影响来评估加密算法的安全性。在图像加密领域，差分攻击通过比较明文图像与加密图像之间的差异，量化加密算法对输入变化的敏感性，从而评估其抵抗差分

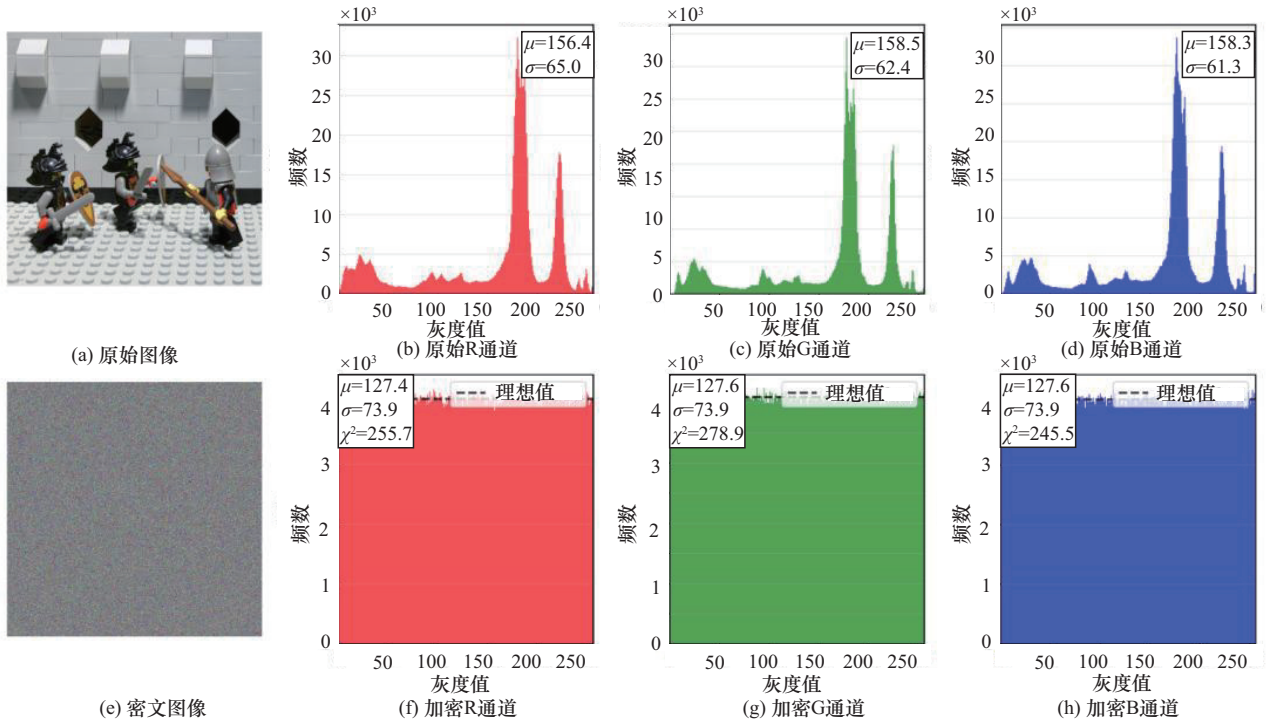


图 11　加密前后直方图分析

攻击的能力。本文采用两个关键指标来评估光场图像混沌加密系统的差分攻击抵抗力，分别为NPCR和UACI，计算式分别为

$$\mathrm{NPCR} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100\% \tag{26}$$

$$\mathrm{UACI} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{\left|P_1(i,j) - P_2(i,j)\right|}{255} \times 100\% \tag{27}$$

其中，$D(i,j)$为差分函数，$P_1(i,j)$和$P_2(i,j)$分别为在明文图像上稍加修改后得到的两个加密图像，$M \times N$为图像尺寸。明文敏感性分析结果如表4所示。

表4　　明文敏感性分析结果

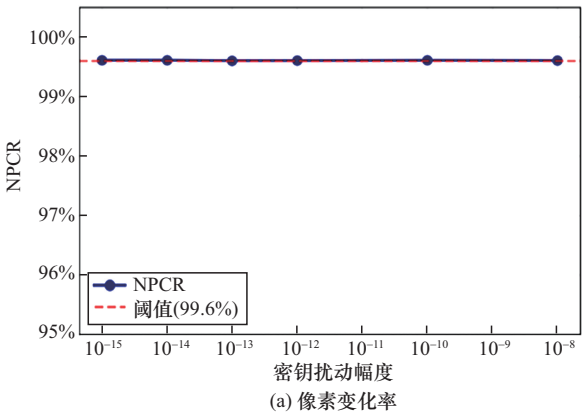
光场图像	NPCR	UACI
Lego Knights（1 bit改变）	99.361 2%	33.466 7%
The Stanford Bunny（1 bit改变）	99.549 2%	33.449 7%
Tarot Cards and Crystal ball（1 bit改变）	99.526 0%	33.457 0%
Lego Knights（2 bit改变）	99.619 6%	33.466 4%
The Stanford Bunny（2 bit改变）	99.549 2%	33.476 0%
Tarot Cards and Crystal ball（2 bit改变）	99.683 1%	33.484 2%

表4中的实验结果表明，所提出的混沌系统具有良好的明文敏感性，这里选取Stanford光场图像数据集中的Lego Knights、The Stanford Bunny和Tarot Cards and Crystal ball作为代表性图像。结果表明，两个差别极小的明文图像经过加密后得到的密文图像相差迥异，其NPCR和UACI计算结果与理论值相近。

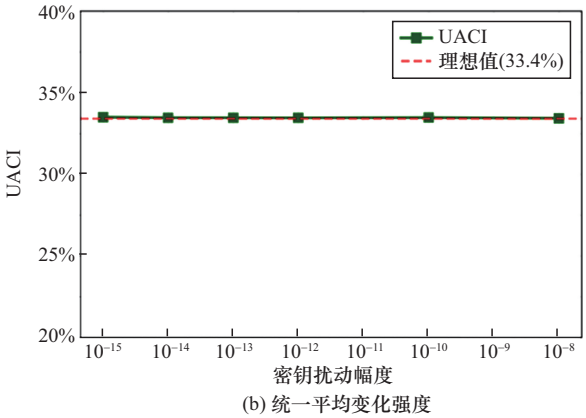
5.3.5　密钥敏感性分析

本节对原始密钥施加不同量级的扰动，生成扰动密钥，其中扰动范围为10^{-15}~10^{-8}。使用原始密钥和扰动密钥分别加密同一明文图像，计算两个密文间的差异。密钥敏感性分析如图12所示。所有测试的NPCR值均在99.6%附近，证明密钥改变几乎导致了所有像素的变化。

由图12可知，在8个数量级扰动范围内，所有测试的NPCR值均在99.6%附近，且NPCR波动仅为0.008 2%，证明密钥改变几乎导致所有像素的变化，密钥敏感性在整个密钥空间高度均匀；所有测试的UACI值均为33.429 0%~33.494 6%，说明密钥改变不仅导致像素改变，且改变幅度达到满幅的$\frac{1}{3}$，符合理想的均匀随机分布特征。表5结果表明，系统满足Shannon的混淆原则，相比近几年其他算法，本文设计的加密算法具有优异的密钥敏感性及密钥空间。



(a) 像素变化率



(b) 统一平均变化强度

图12　密钥敏感性分析

表5　　密钥敏感性分析结果

算法	NPCR	UACI	密钥空间
本文算法	99.611 2%	33.494 6%	2^{322}
文献[5]	99.432 9%	33.397 3%	2^{256}
文献[6]	99.610 0%	31.120 0%	2^{315}
文献[7]	99.610 0%	40.210 0%	10^{32}
文献[30]	99.270 0%	19.370 0%	—
文献[31]	99.608 6%	33.463 5%	2^{192}
文献[32]	99.611 3%	33.470 8%	2^{320}

5.4　密文质量分析

为了全面评估本文提出的光场图像加密算法的有效性和安全性，本节对加密后的密文图像进行定量分析。密文质量是衡量加密算法性能的重要指标，优秀的加密算法应当使密文图像具有高度的随

机性，破坏原始图像的统计特性并消除相邻像素间的相关性，从而有效抵抗各种密码分析攻击。本节采用结构相似性指数（SSIM）、均方误差（MSE）及峰值信噪比（PSNR）进行分析，通过对比分析原始图像与密文图像在这些指标上的差异，客观反映算法加密效果。

结构相似性指数从亮度、对比度和结构3个维度综合评估两幅图像的相似程度，是一种经典的图像质量评估方法。其计算式为

$$\mathrm{SSIM}(x,y)=\frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \tag{28}$$

其中，μ_x和μ_y表示图像x和y的均值，σ_x^2和σ_y^2表示图像x和y的方差，σ_{xy}表示图像x与y的协方差，c_1和c_2为避免除0而引入的稳定常数。SSIM取值范围为$[-1,1]$，当SSIM=1时，表示两幅图像完全相同；当SSIM=0时，表示两幅图像无结构相关性。

均方误差是评估两幅图像差异的经典指标，在图像加密场景中，MSE值越大，密文图像与原始图像差异越显著，加密效果也越好。MSE计算式为

$$\mathrm{MSE}=\frac{1}{M\times N}\sum_{i=1}^{M-1}\sum_{j=1}^{N-1}\left[I(i,j)-E(i,j)\right]^2 \tag{29}$$

其中，$M\times N$表示图像的尺寸，$I(i,j)$和$E(i,j)$分别表示原始图像和密文图像在(i,j)位置处的像素值。

峰值信噪比通常用于评估图像处理算法对图像质量的影响，其计算式为

$$\mathrm{PSNR}=10\lg\frac{\mathrm{MAX}^2}{\mathrm{MSE}} \tag{30}$$

其中，MAX表示像素最大可能值，对于8位图像，MAX取值为255。在图像加密领域中，PSNR值应当越低越好，这是因为低PSNR值意味着密文与原文差异巨大，攻击者无法从视觉或统计角度获取有用信息。

本节以“Lego Knights”和HCI数据集中additional文件下的“dishes”“town”“antinous”光场图像为例[33]进行密文质量分析与测试，结果如表6所示。

由表6可知，密文图像与原始图像的SSIM远低于阈值0.1，说明加密算法完全破坏了原始图像的结构特征。3个通道的MSE值均很高，其中，“Lego Knights”图像中的平均MSE值超过10 326，证明加密算法对原始图像进行了彻底的扰乱与变换，密文图像与原始图像在像素层面上存在显著差异，有效地隐藏了原始信息。从PSNR结果来看，加密后的密文图像与原始图像在视觉特征上已完全不同，观察者无法通过密文图像推断出原始图像的任何内容。这一结果与MSE分析相互印证，共同证明了算法的强加密特性。

6 结束语

本文围绕光场图像4D特性，设计了一种基于深度感知的光场图像高维混沌加密系统。采用EPI方法提取深度信息并结合混沌系统实现像素级、视点级与块级的置乱与扩散，有效地实现了光场图像加密。由密文结果与质量分析可知，该系统在加密

表6 密文质量分析结果

测试图像	SSIM			MSE			PSNR		
通道	R	G	B	R	G	B	R	G	B
Lego Knights	0.009 2	0.009 0	0.008 6	10 156.121 6	10 297.308 0	10 527.718 1	8.063 5	8.003 5	7.907 4
dishes	0.010 0	0.009 6	0.008 1	7 036.732 2	7 263.895 0	8 320.017 7	9.657 0	9.519 1	8.929 5
town	0.009 1	0.009 9	0.010 4	9 615.057 1	7 742.827 6	6 699.234 2	8.301 2	9.241 8	9.870 5
antinous	0.008 8	0.009 4	0.008 8	8 833.950 1	8 489.641 5	9 413.198 3	8.669 2	8.841 9	8.393 4
antinous(文献[34])	0.009 5	0.009 5	0.008 9	8 823.665 0	8 477.704 9	9 495.004 2	8.674 3	8.848 0	8.355 9
图4.1.03(文献[35])	0.000 5	0.000 3	−0.001 1	6 734.320 0	6 475.130 0	6 545.550 0	9.847 9	10.018 0	9.971 3
Airplane(文献[36])	0.013 2(灰度图像)			7 654.840 0(灰度图像)			8.918 0(灰度图像)		
Tree(文献[37])	0.009 8(灰度图像)			10 029.606 3(灰度图像)			8.118 0(灰度图像)		

效果、统计特性、密钥空间、差分攻击抵抗力和随机性等方面均表现优异。然而本文方法需要对所有子孔径图像进行处理，当其数据量大时加密效率略低。因此，未来研究将聚焦光场图像数据压缩，降低时延，以适用于光场图像的实时加密。

参考文献：

[1] Levoy M, Hanrahan P. Light field rendering[C]//Proceedings of the 23rd Annual Conference on Computer Graphics and Interactive Techniques. New York: ACM Press, 1996: 31-42.

[2] Ng R, Levoy M, Bredif M, et al. Light field photography with a hand-held plenoptic camera[R]. 2005.

[3] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps[J]. International Journal of Bifurcation and Chaos, 1998, 8(6): 1259-1284.

[4] Chen G R, Mao Y B, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons & Fractals, 2004, 21(3): 749-761.

[5] Lima V , Ferreira F , Madeiro F, et al. Light field image encryption based on steerable cosine number transform[J]. Signal Processing, 2023, 202: 108781.

[6] Wen W Y, Wei K K, Zhang Y S, et al. Colour light field image encryption based on DNA sequences and chaotic systems[J]. Nonlinear Dynamics, 2020, 99(2): 1587-1600.

[7] Wei K K, Wen W Y, Fang Y M. Light field image encryption based on spatial-angular characteristic[J]. Signal Processing, 2021, 185: 108080.

[8] Sun C Y, Wang E F, Zhao B. Image encryption scheme with compressed sensing based on a new six-dimensional non-degenerate discrete hyperchaotic system and plaintext-related scrambling[J]. Entropy, 2021, 23(3): 291.

[9] Levoy M. Light fields and computational imaging[J]. Computer, 2006, 39(8): 46-55.

[10] Hog M, Sabater N, Vandame B, et al. An image rendering pipeline for focused plenoptic cameras[J]. IEEE Transactions on Computational Imaging, 2017, 3(4): 811-821.

[11] Tao M W, Hadap S, Malik J, et al. Depth from combining defocus and correspondence using light-field cameras[C]//Proceedings of the 2013 IEEE International Conference on Computer Vision. Piscataway: IEEE Press, 2014: 673-680.

[12] 杜雪萍, 胡娟梅, 楼益民. 基于EPI融合的光场图像生成与消隐算法[J]. 浙江理工大学学报, 2025, 53(5): 416-424.
Du X P, Hu J M, Lou Y M. Light field image generation and hidden algorithm based on EPI fusion[J]. Journal of Zhejiang Institute of Science and Technology, 2025, 53(5): 416-424.

[13] Yang Z Y, Sang X Z, Yan B B, et al. Real-time light-field generation based on the visual hull for the 3D light-field display with free-viewpoint texture mapping[J]. Optics Express, 2023, 31(2): 1125-1140.

[14] Chen R S, Sheng H, Cong R X, et al. Stereo matching on epipolar plane image for light field depth estimation via oriented structure[J]. Engineering Applications of Artificial Intelligence, 2025, 151: 110608.

[15] Wang X Z, Huang W H, Chen K Q, et al. EAT: epipolar-aware Transformer for low-light light field enhancement[J]. Multimedia Tools and Applications, 2025, 84(12): 10609-10630.

[16] Kalantari N K, Wang T C, Ramamoorthi R. Learning-based view synthesis for light field cameras[J]. ACM Transactions on Graphics, 2016, 35(6): 1-10.

[17] Yan W B, Zhang X G, Chen H. Occlusion-aware unsupervised light field depth estimation based on multi-scale GANs[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2024, 34(7): 6318-6333.

[18] Chen L M, Zhang S. Electrically tunable lens assisted absolute phase unwrapping for large depth-of-field 3D microscopic structured-light imaging[J]. Optics and Lasers in Engineering, 2024, 174: 107967.

[19] Dansereau D G, Mahon I, Pizarro O, et al. Plenoptic flow: closed-form visual odometry for light field cameras[C]//Proceedings of the 2011 IEEE/RSJ International Conference on Intelligent Robots and Systems. Piscataway: IEEE Press, 2011: 4455-4462.

[20] Wanner S, Goldluecke B. Variational light field analysis for disparity estimation and super-resolution[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2014, 36(3): 606-619.

[21] Shin C, Jeon H G, Yoon Y, et al. EPINET: a fully-convolutional neural network using epipolar geometry for depth from light field images[C]//Proceedings of the 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE Press, 2018: 4748-4757.

[22] Heber S, Pock T. Shape from light field meets robust PCA[C]//Computer Vision – ECCV 2014. Berlin: Springer, 2014: 751-767.

[23] Wanner S, Goldluecke B. Globally consistent depth labeling of 4D light fields[C]//Proceedings of the 2012 IEEE Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE Press, 2012: 41-48.

[24] Zhang S L, Liu Z D, Liu X L, et al. A light field depth estimation algorithm considering blur features and prior knowledge of planar geometric structures[J]. Applied Sciences, 2025, 15(3): 1447.

[25] Shannon C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 656-715.

[26] Pankaj S, Dua M. Chaos based medical image encryption techniques: a comprehensive review and analysis[J]. Information Security Journal: A Global Perspective, 2024, 33(3): 332-358.

[27] Ge B, Qu G Q, Shen Z H, et al. A counter mode and multi-channel based chaotic image encryption algorithm for the Internet of things[J]. Frontiers in Physics, 2024, 12: 1494056.

[28] 刘雨欣, 栗风永. 融合全置乱超混沌序列和DNA编码的图像加密[J]. 计算机工程, 2025, 51(1): 235-245.
Liu Y X, Li F Y. Image encryption integrating fully scrambled hyperchaotic sequences and DNA encoding[J]. Computer Engineering, 2025, 51(1): 235-245.

[29] Stanford Computer Graphics Laboratory. The (new) Stanford light field archive[R]. 2008.

[30] Wei K K, Wen W Y. Light field image encryption based on pixel substi-

tution and double random phase encoding[C]//Proceedings of the 2019 3rd International Conference on Graphics and Signal Processing. New York: ACM Press, 2019: 13-17.

[31] Wan Y J, Wang S M, Du B X. A bit plane image encryption algorithm based on compound chaos[J]. 2022, 82(14): 22103-22121.

[32] Chen Z F, Yang Y, Jiang X M. An image-encryption algorithm based on stage-merging bit scrambling[J]. Applied Sciences, 2022, 12(14): 6972.

[33] Honauer K, Johannsen O, Kondermann D, et al. A dataset and evaluation methodology for depth estimation on 4D light fields[C]//Computer Vision – ACCV 2016. Berlin: Springer, 2017: 19-34.

[34] Shao J R, Bai E J, Jiang X Q, et al. Multi-view light field images compression and encryption using enhanced 3D chaotic system and pixel-bit-scrambling[J]. IEEE Access, 2024, 12: 156471-156491.

[35] Elmenyawi M A, Abdel Aziem N M, Bahaa-Eldin A M. Efficient and secure color image encryption system with enhanced speed and robustness based on binary tree[J]. Egyptian Informatics Journal, 2024, 27: 100487.

[36] Kumar B S, Revathi R. An efficient image encryption algorithm using a discrete memory-based logistic map with deep neural network[J]. Journal of Engineering and Applied Science, 2024, 71(1): 41.

[37] He Z Q, Rauf A, Nazir A, et al. Design and analysis of a secure image encryption algorithm using proposed non-linear RN chaotic system and ECC/HKDF key derivation with authentication support[J]. Scientific Reports, 2025, 15: 39951.

[作者简介]

仲昭宇（1998– ），男，辽宁鞍山人，黑龙江大学博士生，主要研究方向为光场图像处理、混沌加密。

王尔馥（1980– ），女，黑龙江哈尔滨人，黑龙江大学教授、博士生导师，主要研究方向为保密通信、阵列信号处理、传输干扰抑制等。