基于印刷量子点的可靠性复合光谱图像编解码算法研究

赵文康，曹鹏*

（北京印刷学院 高端印刷装备信号与信息处理北京市重点实验室，北京 102600）

摘要：目的 为提高印刷量子点图像的鲁棒性、识读速度和信息隐藏容量，提出一种可靠性复合光谱印刷量子点图像编解码算法。**方法** 首先结合 ChaCha20 加密算法、SHA-256 哈希算法、(331, 225, 367)卷积码和交织编码，将明文信息编码成具有安全验证和纠错能力的二进制秘密信息，再插入伪随机同步信息，并进行掩膜矩阵置乱，映射成可通过相邻数据联合解算的印刷量子点图像，最后利用 2 组印刷量子点图像对载体图像进行信息调制，实现复合光谱大容量信息隐藏。**结果** 实验结果显示，生成的复合光谱印刷量子点图像可抵抗 20%以内的噪声攻击，识读时间在 0.1 s 左右，嵌入率为 2 bpp，与原始载体图像的峰值信噪比（Peak Signal-to-Noise Ratio，PSNR）约为 40 dB，结构相似性（Structural Similarity，SSIM）约为 0.97。**结论** 本算法与其他算法相比，在高嵌入率下具有更高的鲁棒性和更好的不可见性，识读速度更快。

关键词：印刷量子点图像；复合光谱；卷积码；信息隐藏

中图分类号：TN911.3 **文献标志码：**A **文章编号：**1001-3563(2025)07-0173-10

DOI：10.19554/j.cnki.1001-3563.2025.07.021

Encoding and Decoding Algorithms for Image Information of Composite Spectrum Based on Printed Quantum Dots

*ZHAO Wenkang, CAO Peng**

(Beijing Key Laboratory of Signal and Information Processing for High-end Printing Equipment, Beijing Institute of Graphic Communication, Beijing 102600, China)

ABSTRACT: In order to improve the robustness, reading speed and information hiding capacity of printed quantum dot images, the work aims to propose a reliable encoding and decoding algorithm for composite spectral printed quantum dot image. Firstly, ChaCha20 encryption algorithm, SHA-256 hash algorithm, (331, 225, 367) convolutional code and interlacing coding were combined to encode the plaintext information into binary secret information with security verification and error correction capabilities, and then pseudo random synchronization information was inserted, and mask matrix scrambling was carried out, which was mapped into a printed quantum dot image that could be solved jointly by adjacent data. Finally, two sets of printed quantum dot images were used to modulate the carrier image to realize the large-capacity information hiding of composite spectrum. The experimental results showed that the generated composite spectral printed quantum dot image could resist the noise attack within 20%, the reading time was about 0.1 s, the embedding rate was 2 bpp, and the Peak Signal-to-Noise Ratio (PSNR) value was about 40 dB compared with the original carrier image and the structural similarity (SSIM) value was about 0.97. Compared with other algorithms, this algorithm

收稿日期：2024-10-08

基金项目：国家自然科学基金面上项目（61972042）；北京市基金-市教委联合项目（KZ202010015023）；北京印刷学院科研平台建设项目（KYCPT202509）；北京印刷学院信息与通信工程一级学科博士点培育项目（21090525004）

***通信作者**

has higher robustness, better invisibility and faster reading speed under high embedding rate.

KEY WORDS: printed quantum dot image; composite spectrum; convolutional coding; information hiding

尽管数字化生活日益普及，但大量图文信息仍然以印刷品的形式存在和传播，盗版和造假行为给印刷品的版权保护带来很大的挑战。现有防伪技术中，一部分通过特殊的纹理特征来实现真假验证，一般需要特定的扫描设备才能检测，无法满足大众便捷的识别需求[1-3]；另一部分则通过特殊材料来提高伪造的门槛，虽然有不错的防伪性能，但是成本昂贵[4-6]。因此，研究一种利用手机端轻松验证真伪的防伪溯源技术显得尤为重要。

在打印处理图像时，通常会进行半色调技术处理，印刷的最小半色调网点因不可再分被称为印刷量子点。印刷量子点是一组半色调网点数据，其图像为一种矢量点阵图像，点阵最小单元为一个单像素印刷量子点，通常为微米级。通过印刷量子点图像对载体图像进行网点调制来记录信息，具有抗复制、隐蔽等优势，但由于印刷过程中存在油墨飞溅、网点错位等实际问题，会造成网点丢失或污损，对印刷量子点的鲁棒性提出更高的要求。

在通信传输过程中，利用可靠性编解码技术可有效解决信道干扰，提高信号传输的可靠性，有研究人员利用信道编码技术处理图像数据，以此提高图像数据的鲁棒性，主要包括以下 3 个方面。

1）汉明码的使用。研究人员利用汉明码的纠错能力与其他方式结合来实现隐藏数据的恢复及安全性，Datta 等[7]将(7, 4)汉明码与方块截断编码（Block Truncation Coding，BTC）相结合，专门针对高度压缩的图像，在保持图像质量的同时实现数据隐藏的鲁棒性和安全性；Li 等[8]将(7, 4)汉明码与单位平滑检测函数相结合，将数据嵌入加密图像，在不损失原始图像数据的情况下保证隐藏数据的安全性和可分离性；Kim 等[9]结合(3, 1)汉明码和优化像素调整过程（Optimal Pixel Adjustment Process，OPAP）实现双重高效可逆数据隐藏；Lien 等[10]提出空间填充曲线分解方法，将数据进行汉明码编码后分散嵌入图像的不同区域，实现数据隐藏的鲁棒性和恢复能力；Wu 等[11]使用汉明码对隐藏数据进行编码，通过优化图像区域选择和嵌入策略，使编码数据嵌入对图像质量影响较小的部分；Nguyen 等[12]结合(5, 3)汉明码并引入灰度图像重叠像素块，在减少数据嵌入对图像质量影响的同时，可提供额外信息用于数据恢复。

2）BCH（Bose-Chaudhuri-Hocquenghem）码的使用。Wang 等[13]将 BCH 码与离散傅里叶变换（Discrete Fourier Transform，DFT）相结合，使秘密信息嵌入原始图像的局部区域，同时添加 2 条结构模板线，验证其在多种畸变攻击下具有良好的鲁棒性；Vinoth 等[14]使用颜色分割构建可嵌入的颜色三元组，利用 SHA-256 哈希函数和 BCH 码对秘密信息进行编码，不仅提高秘密信息的鲁棒性和抗篡改性，而且具有更高的嵌入率；Zhu 等[15]将 BCH 码与奇偶校验码相结合，为了实现与载体图像尺寸匹配，进行随机迭代置乱交错排列；王育军等[16]利用 BCH 码与交织编码加二维奇偶校验码的方式，与文献[15]相比，对突发噪声攻击具有更强的鲁棒性，其局限性在于只能处理一定数量的错误。

3）卷积码的使用。王育军等[17]利用数据加密标准（Data Encryption Standard，DES）加密、二维奇偶校验编码和 Turbo 码对秘密信息进行编码，提高加密数据的鲁棒性和安全性，同时对信息进行调制，生成可通过局部印刷量子点图像识读秘密信息的加密图像；邱英英等[18]改进文献[16]，结合(171, 133)卷积码和随机交织编码，在突发污损情况下识别准确率更高。

基于上述分析，采用信道编码技术可以有效增强印刷量子点图像的鲁棒性，但仍存在一些问题。首先，当前算法在鲁棒性上仍有待提升；其次，由于识别设备的升级，攻击者可以轻松获取印刷量子点信息，秘密信息的安全性有待加强；再次，当前算法在识读速度方面无法达到更好的用户体验；最后，虽然当前算法能够实现较好的嵌入率，但随着高容量数据的加入，算法性能有所下降。

针对以上问题，本研究基于印刷量子点，采用(331, 225, 367)卷积码加维特比软判断译码的方式，进一步提高印刷量子点图像的鲁棒性；结合流比特加密和哈希函数提高印刷量子点图像的安全性；引入同步分散插入策略，实现通过相邻数据联合解算，极大地提高识读速度；结合同色异谱技术[19]，将 2 b 信息嵌入载体图像的同一像素，在不同光源下显示不同信息点，从而在不改变图像质量的情况下达到高容量数据隐藏。

1 基本原理

1.1 复合光谱印刷量子点图像

根据视觉系统特性，人眼对 42~160 μm 的网点敏感度非常低[20]。600 dpi 以上打印设备打印的印刷量子点直径在 42 μm 以下，因此通过印刷量子点图像对载体图像进行信息调制并打印，可实现隐形、弱隐形或可视的信息加密。

颜色是人眼对特定波长光的感知，而波长或频率决定了光的颜色，人眼在不同的光谱功率下会产生

相同的视觉颜色感知[21]。不同的墨水对可见光（400~700 nm）和红外光（>700 nm）的吸收与反射特性不同，其中 K 墨对红外光波段具有极强的响应。在 CMYK 4 色打印中，打印图像的 C_{MYK} 灰色值可以控制打印机对 4 个通道的喷墨用量，在印刷图像前改变图像中 K 值为 0 的像素点，可保证这些点在红外光下突显。另外，人眼对黄色的敏感度较低，改变原图像 Y 通道的灰色值，使该点与原图像产生一定的颜色差异，可使其在可见光下弱隐形。

通过模拟计算得到 3 组 C_{MYK} 灰色值。1）$C_{MYK,1}$ 灰色值组，其中 $K\neq0$，并保证其与原图像的人眼视觉颜色一致，实现在可见光下不可见，红外光下可见；2）$C_{MYK,2}$ 灰色值组，其中 $K=0$，$200\leqslant Y\leqslant255$，实现在可见光下可见，红外光下不可见；3）$C_{MYK,3}$ 灰色值组，其中 $K\neq0$，并保证其与 $C_{MYK,2}$ 的人眼视觉颜色一致，实现可见光与红外光下均可见。整体实现流程见图 1。

1.2　卷积编译码

卷积码作为一种高效的纠错编码方式，将输入的数据序列通过多个移位寄存器进行卷积运算，生成具有冗余的输出序列，这些冗余在接收端能够检测并纠正传输过程中出现的错误[22]。卷积码纠错性能与自由距离有关，一般情况下，自由距离越大，卷积码的纠错能力越强。卷积码的性能更接近香农极限，随着自由距离的增加，译码时的时间开销也会增大[23]。通过实际程序运行比较约束长度为 9 时不同码率卷积码之间的编码效率、最大自由距离以及相对编译码时间（表 1），其中生成的多项式用八进制表示。本研究综合考虑纠错能力和译码时间开销，选择码率为 1/3 的(331, 225, 367)卷积码作为纠错编码。为了确保编码的准确性和译码效率，在卷积码编码算法设计时对寄存器进行清空操作。

卷积码的解码采用维特比算法，其目的是通过动态规划方法寻找最优路径，即输出的比特序列[24]。假设用 s_t 表示 t 时刻的状态，对于每个状态的 s_t，定义路径度量 $\gamma(s_t)$,表示从初始状态到 s_t 的累计误差，通过计算接收的码字与预期码字之间的汉明距离 $d_H(y_t, \bar{y}_t)$来更新路径度量值。当处理完接收的所有码字后，从终止状态开始，沿着存储的前驱状态回溯，得到最优路径，即译码结果 Y_a，见式（1）。

$$Y_a=\arg\min_{s_{t-1}}\left[\gamma(s_{t-1})+d_H(y_t,\bar{y}_t)\right] \tag{1}$$

式中：y_t 为 t 时刻接收的码字；$\bar{y}_t$ 为从 s_{t-1} 转移到 s_t 所期望的输出。

2　算法设计

2.1　复合光谱印刷量子点信息隐藏算法

本研究结合 ChaCha20 流比特加密[25]、SHA-256 数字签名算法[26]、(331, 225, 367)卷积码编码及交织编码，将秘密信息编码成差错可控的编码二进制数据，通过掩膜矩阵进行伪随机置乱，并将伪随机同步信息分散插入后一起映射生成印刷量子点图像，最后通过信息调制算法将不同明文信息生成的印刷量子点图像植入载体图像，实现复合光谱印刷量子点图像信息隐藏。

2.1.1　印刷量子点图像生成算法

1）对输入的秘密信息 *str* 进行规范化二进制处理，使其转化为明文二进制码组 B，B 的长度为 h。

2）输入 32 B 密钥 K、12 B 随机数 N、常量 c 和计时器 *counter*，构成 4×4 的初始状态矩阵 $\boldsymbol{S}_1$，见式（2）。

$$\boldsymbol{S}_1=\begin{pmatrix} c_0 & c_1 & c_2 & c_3 \\ K_0 & K_1 & K_2 & K_3 \\ K_4 & K_5 & K_6 & K_7 \\ counter & N_0 & N_1 & N_2 \end{pmatrix} \tag{2}$$

式中：K_0—K_7 为密钥 K 的 4 B 分量；N_0—N_2 为随机数 N 的 4 B 分量；c_0—c_3 为 4 B 随机数；*counter* 为 4 B 计时器。

利用 ChaCha20 算法对 $\boldsymbol{S}_1$ 进行 20 轮混合运算得到状态矩阵 $\boldsymbol{S}_2$，将状态矩阵 $\boldsymbol{S}_1$ 与 $\boldsymbol{S}_2$ 相加得到最终状态矩阵 $\boldsymbol{S}_3$，见式（3）。

$$\boldsymbol{S}_3[i,j]=\left(\boldsymbol{S}_1[i,j]+\boldsymbol{S}_2[i,j]\right)\bmod 2^{32} \tag{3}$$

式中：i=0, 1, 2, 3; j=0, 1, 2, 3。

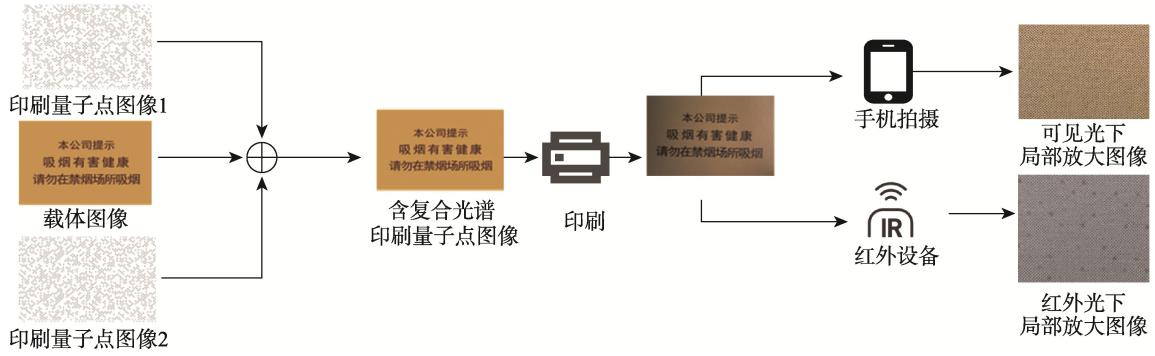


图 1　含复合光谱印刷量子点图像印刷与拍摄

Fig.1 Printing and photographing of images containing composite spectral printed quantum dots

表 1 不同卷积码的性能参数
Tab.1 Performance parameters of different convolutional codes

性能参数	(561, 753)	(331, 225, 367)	(463, 535, 733, 745)
编码效率	1/2	1/3	1/4
最大自由距离	12	16	24
编码时间/s	0.05	0.10	0.2
译码时间/s	0.02	0.03	0.1

将 $\boldsymbol{S}_3$ 按行输出，最终生成一组 64 B 的密钥流块 *block*，将其转化为二进制序列，根据 *h* 截取此二进制序列与明文二进制码组 *B* 进行异或运算，生成密文信息 *C*。

3）根据式（4）填充密文信息 *C* 后，输入 SHA-256 哈希函数生成 256 b 的哈希值 *H*，截取 16 b 的 *H* 作为数字摘要填充到 *C* 后组成编码输入信息 *M*。

$$H=\begin{cases} C=C\|1\|0^k\|len(C) \\ k=448-\left[len(C)+1\right]\bmod 512 \\ SHA(C) \end{cases} \tag{4}$$

式中：‖为二进制序列拼接；*len*(*C*)为密文信息 *C* 的原始长度；*SHA*( )为 SHA-256 哈希函数。

4）构造(331, 225, 367)卷积码编码器结构，如图 2 所示。

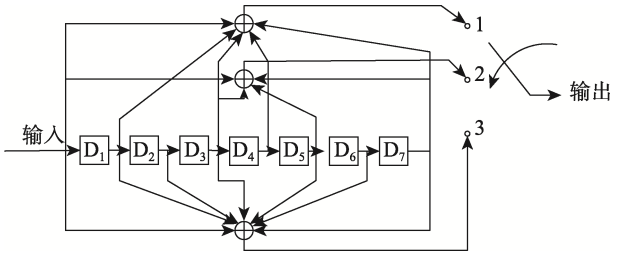


图 2 (331, 225, 367)卷积编码器
Fig.2 (331, 225, 367) convolutional encoder

将 *M* 作为输入，某个特定时刻 *t* 传输的数据为 *M*(*t*)，移位寄存器 D_i 中存留的数据为 *t*-*i* 时刻传输的数据 *M*(*t*-*i*)，寄存器初始状和最终状态均为 0，寄存器之间进行模 2 运算，得到 3 个码组序列 $e_t^{(1)}$、$e_t^{(2)}$ 和 $e_t^{(3)}$，3 个码组组合生成编码数据 *E*，见式（5）。

$$E=\left(e_t^{(1)},\ e_t^{(2)},\ e_t^{(3)}\right)=$$
$$\begin{cases} e_t^{(1)}=\left(M_t+M_{t-1}+M_{t-3}+M_{t-4}+M_{t-7}\right)\bmod 2 \\ e_t^{(2)}=\left(M_t+M_{t-3}+M_{t-5}+M_{t-6}\right)\bmod 2 \\ e_t^{(3)}=\left(M_t+M_{t-1}+M_{t-2}+M_{t-3}+M_{t-4}+M_{t-5}+\right. \\ \qquad \left.M_{t-6}+M_{t-7}\right)\bmod 2 \end{cases} \tag{5}$$

5）编码数据 *E* 根据式（6）计算最大交织深度 *n*，根据式（7）计算对 *E* 填充的数据段长度 l_z。

$$n=\left\lfloor\sqrt{\frac{len(E)}{2}}\right\rfloor \tag{6}$$

$$l_z=\begin{cases} 0 & len(E)\bmod n=0 \\ n-len(E)\bmod n & \text{otherwise} \end{cases} \tag{7}$$

式中：*len*(*E*)为编码数据 *E* 的长度。

根据 l_z 对 *E* 填充数据 0、1 后输入交织编码器得到交织数据 *E*′，*E*′进行串并变换得到本原矩阵 $\boldsymbol{X}$。交织编码器结构如图 3 所示。

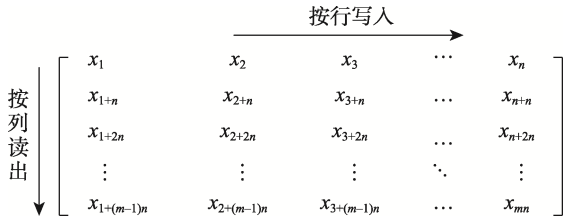


图 3 交织编码器
Fig.3 Interleaved encoder

6）定义一个位置序列 *P*，将 $\boldsymbol{S}_P$ 分散插入 $\boldsymbol{X}$ 得到 $\boldsymbol{X}'$，见式（8）。

$$\boldsymbol{X}'=\text{Dispersed\_insertion}\left(\boldsymbol{X},\boldsymbol{S}_P,P\right) \tag{8}$$

式中：Dispersed_insertion( )为分散插入函数；$P=\{(P_{1,1}, P_{1,2}), (P_{2,1}, P_{2,2}), \ldots, (P_{k,1}, P_{k,2})\}$。

为保证复制拼接印刷量子点图像不会出现干涉条纹漏洞和大面积黑白堆积的问题，同时可通过相邻数据快速解码，定义伪随机同步信息 $\boldsymbol{S}_P$ 和掩膜矩阵信息 $\boldsymbol{M}_{\text{ask}}$ 之间的对应关系，见式（9）。

$$\boldsymbol{M}_{\text{ask},i}=\min\left(\max\left(\left\lceil\frac{S_{P,j}-1}{4}\right\rceil,1\right),4\right) \tag{9}$$

式中：*i*=1, 2, 3, 4; *j*=1, 2, 3, …, 16。

利用式（9）得到的 $\boldsymbol{M}_{\text{ask}}$ 与 $\boldsymbol{X}'$进行异或运算得到伪本原矩阵 $\boldsymbol{G}$，见式（10）。

$$\boldsymbol{G}=XOR\left(\boldsymbol{M}_{\text{ask}},\boldsymbol{X}'\right) \tag{10}$$

7）利用式（11）对伪本原矩阵 $\boldsymbol{G}$ 进行扩散映射，生成具有分散稀疏特性的印刷量子点图像 *W*，其中秘密信息数据 0 用黑块表示，1 用白块表示。

$$W=Map\left(\boldsymbol{G},\theta,\Delta\right) \tag{11}$$

式中：*Map*( )为扩散映射函数；θ 为排列角度参数；Δ 为间隔参数。

2.1.2 信息调制

读取一幅 C_{MYK} 灰色值载体图像 *I*，将 2 组秘密信息 str_1 和 str_2 输入印刷量子点图像生成算法，生成与 *I* 匹配的 2 幅印刷量子图像 W_1 和 W_2，分别代表可见光谱秘密信息和红外光谱秘密信息。将 W_1、W_2 和 *I* 输入 Metamerism_Adjustment( )函数，即复合光谱信息调制算法，得到 3 组数值 $C_{\text{MYK},1}$、$C_{\text{MYK},2}$ 和 $C_{\text{MYK},3}$，$C_{\text{MYK},1}$ 中 K=0，$200\leqslant Y\leqslant 255$；$C_{\text{MYK},2}$ 中 $1\leqslant K\leqslant 15$；

$C_{MYK,3}$ 中 $1 \leqslant K \leqslant 15$。分别对应不同 W_1、W_2 对 I 进行幅度调制后得到 C_{MYK}'，见表 2。

表 2　幅度调制对应
Tab.2 Amplitude modulation correspondence

W_1	W_2	C_{MYK}'
0	1	$C_{MYK,1}$
0	0	$C_{MYK,2}$
1	0	$C_{MYK,3}$
1	1	C_{MYK}

通过印刷量子点图像生成算法和信息调制算法，将 2 组秘密信息生成的印刷量子点图像嵌入载体图像，在可见光和红外光下显示不同的印刷量子点图像，实现复合光谱印刷量子点信息防伪与增值服务。算法伪代码如下。

输入：明文信息 str_1 和 str_2，载体图像 I，插入位置序列 P，伪随机同步信息码组 $\boldsymbol{S}_P$，密钥 K，随机数 N，排列角度参数 θ，间隔参数 Δ；

输出：含复合光谱印刷量子点图像 I'；

将 str_1 转换为二进制序列 B；

将 B 输入 ChaCha20 算法得到二进制密钥流块 *block*；

将 *block* 转换为二进制序列与 B 异或得到密文 C；

根据式（4）得到 16 b 哈希值 H，填充到 C 后得到编码输入信息 M；

将 M 输入（331, 225, 367）卷积码编码器，得到编码数据 E；

利用式（6）计算交织深度 n，构造交织编码器；

根据式（7）对 E 进行填充后输入交织编码器，得到交织数据 E'；

E'串并变换得到本原矩阵 $\boldsymbol{X}$；

根据式（8）将 $\boldsymbol{S}_P$ 插入 $\boldsymbol{X}$ 得到 $\boldsymbol{X}'$；

根据式（9）得到掩膜矩阵 $\boldsymbol{M}_{ask}$；

$\boldsymbol{M}_{ask}$ 与 $\boldsymbol{X}'$进行异或得到伪本原矩阵 $\boldsymbol{G}$；

根据式（11）对 $\boldsymbol{G}$ 进行扩散映射生成印刷量子点图像 W_1；

str_2 重复上述算法流程生成印刷量子点图像 W_2；

将 I、W_1 和 W_2 输入 Metamerism_Adjustment( ) 函数得到 $C_{MYK,1}$、$C_{MYK,2}$ 和 $C_{MYK,3}$。

```
for i=1 to l do
  for j=1 to l do
      if W1==0&&W2==1
        I=C_MYK,1;
      elseif W1==0&&W2==0
        I=C_MYK,2;
      elseif W1==1&&W2==0
        I=C_MYK,3;
      end if
    end for
  end for
  return I'
```

2.2　印刷量子点信息识读算法

由于在印刷量子点中插入伪随机同步信息 $\boldsymbol{S}_P$，并且掩膜矩阵 $\boldsymbol{M}_{ask}$ 与 $\boldsymbol{S}_P$ 之间存在对应关系，本研究对印刷量子点的识读为可通过相邻数据联合解算的任意区域识读算法。假设编码伪随机同步信息码组为 $\boldsymbol{S}=\{\boldsymbol{S}_1, \boldsymbol{S}_2, \boldsymbol{S}_3, \ldots, \boldsymbol{S}_P\}$，插入位置序列为 $P=\{P_1, P_2, P_3, \ldots, P_k\}$，密钥为 K，随机数为 N，生成印刷量子点图像尺寸为 $D\times D$。在可见光或红外光下拍摄含印刷量子点的图像，在其任意区域采集尺寸为 $D\times D$ 的印刷量子点矩阵 $\boldsymbol{A}$，识读主要步骤如下。

1）将矩阵 $\boldsymbol{A}$ 分割为$(D/2+1)^2$ 个子矩阵块，遍历子矩阵块，根据位置序列 P 提取子矩阵块中的伪随机同步信息 $\boldsymbol{S}'$，$\boldsymbol{S}'$与 $\boldsymbol{S}$ 进行异或运算得到汉明距离 h_ρ 和索引 ρ，见式（12）。

$$\begin{cases} \boldsymbol{S}' = \left\{ \boldsymbol{A}_{P_1}, \boldsymbol{A}_{P_2}, \cdots, \boldsymbol{A}_{P_k} \right\} \\ h_\rho = \min\left(\boldsymbol{S} \oplus \boldsymbol{S}' \right) \\ \rho = \arg\min_i h_i \end{cases} \tag{12}$$

2）根据 ρ 得到掩膜矩阵信息 γ 和区域定位因子 α，见式（8）和式（13）。

$$\alpha = \left[(\rho - 1) \bmod 4 \right] + 1 \tag{13}$$

3）通过子矩阵块坐标 i、j 及 α 获得区域分割因子 β，见表 3。

表 3　区域分割因子查找
Tab.3 Search of region segmentation factor

i	j	α	β
D	D	1、2、3、4	0
∀	D	1、2	
D	∀	1、3	
∀	∀	1	
D	1	1、2、3、4	1
∀	1	1、2	
D	∀	2、4	
∀	∀	2	
1	D	1、2、3、4	2
∀	D	3、4	
1	∀	1、3	
∀	∀	3	
1	1	1、2、3、4	3
∀	1	3、4	
1	∀	2、4	
∀	∀	4	

4）更新区域分割坐标 $O(r, z)$，将 $\boldsymbol{A}$ 划分为碎片矩阵 $\boldsymbol{A}_1$、$\boldsymbol{A}_2$、$\boldsymbol{A}_3$、$\boldsymbol{A}_4$，见式（14）~（15）。

$$(r,\ z)=(i,\ j)+D\left(\left\lfloor\frac{\beta}{4}\right\rfloor \bmod 2,\ \left\lfloor\frac{\beta}{2}\right\rfloor \bmod 2\right) \tag{14}$$

$$\begin{cases} \boldsymbol{A}_1=\{f(i,j)\ \ i\in r_1, j=z_1\} \\ \boldsymbol{A}_2=\{f(i,j)\ \ i\in r_1, j=z_2\} \\ \boldsymbol{A}_3=\{f(i,j)\ \ i\in r_2, j=z_1\} \\ \boldsymbol{A}_4=\{f(i,j)\ \ i\in r_2, j=z_2\} \end{cases} \tag{15}$$

式中：$f(i,j)$为矩阵 $\boldsymbol{A}$ 在第 i 行和第 j 列上的元素，r_1={1, 2, 3, …, r-1}，z_1={1, 2, 3, …, z-1}，r_2={r, r+1, r+2, …, D}，z_2={z, z+1, z+2, …, D}。

5）通过模板信息 ω 得到掩膜矩阵 $\boldsymbol{M}_1$、$\boldsymbol{M}_2$、$\boldsymbol{M}_3$、$\boldsymbol{M}_4$，与 $\boldsymbol{A}_1$、$\boldsymbol{A}_2$、$\boldsymbol{A}_3$、$\boldsymbol{A}_4$ 进行异或运算得到矩阵 $\boldsymbol{A}_n'$，见式（16）。

$$\boldsymbol{A}_n'(i,j)=\boldsymbol{A}_n(i,j)\oplus\boldsymbol{M}_n(i,j) \tag{16}$$

6）子矩阵块以 D/2 步长移位获得相邻矩阵，通过式（8）得到认证掩膜信息 γ_1、γ_2、γ_3，查找表 4 得到重构子矩阵 $\boldsymbol{R}_1$、$\boldsymbol{R}_2$、$\boldsymbol{R}_2$、$\boldsymbol{R}_4$。

表 4 重构矩阵关系

Tab.4 Reconstructed matrix relationship

i	j	$\gamma, \gamma_1, \gamma_2, \gamma_3$	$\boldsymbol{R}_1$	$\boldsymbol{R}_2$	$\boldsymbol{R}_3$	$\boldsymbol{R}_4$
i=1 或 i=D	j=1 或 j=D	$\gamma=\gamma_1=\gamma_2=\gamma_3$	$\boldsymbol{A}_1$'	$\boldsymbol{A}_2$'	$\boldsymbol{A}_3$'	$\boldsymbol{A}_4$'
		$\gamma=\gamma_2$，$\gamma_1=\gamma_3$	$\boldsymbol{A}_2$'	$\boldsymbol{A}_1$'	$\boldsymbol{A}_4$'	$\boldsymbol{A}_3$'
		$\gamma=\gamma_1$，$\gamma_2=\gamma_3$	$\boldsymbol{A}_3$'	$\boldsymbol{A}_4$'	$\boldsymbol{A}_2$'	$\boldsymbol{A}_1$'
		$\gamma\neq\gamma_1\neq\gamma_2\neq\gamma_3$	$\boldsymbol{A}_4$'	$\boldsymbol{A}_3$'	$\boldsymbol{A}_2$'	$\boldsymbol{A}_1$'
i≠1 或 i≠D	j=1 或 j=D	$\gamma=\gamma_1$	$\boldsymbol{A}_3$'	$\boldsymbol{A}_4$'	$\boldsymbol{A}_1$'	$\boldsymbol{A}_2$'
		$\gamma\neq\gamma_1$	$\boldsymbol{A}_4$'	$\boldsymbol{A}_3$'	$\boldsymbol{A}_2$'	$\boldsymbol{A}_1$'
i=1 或 i=D	j≠1 或 j≠D	$\gamma=\gamma_2$	$\boldsymbol{A}_2$'	$\boldsymbol{A}_1$'	$\boldsymbol{A}_4$'	$\boldsymbol{A}_3$'
		$\gamma\neq\gamma_2$	$\boldsymbol{A}_2$'	$\boldsymbol{A}_1$'	$\boldsymbol{A}_4$'	$\boldsymbol{A}_3$'
∀	∀	∀	$\boldsymbol{A}_4$'	$\boldsymbol{A}_3$'	$\boldsymbol{A}_2$'	$\boldsymbol{A}_1$'

7）根据式（17）得到重组可译码矩阵 $\boldsymbol{A}'$，将 $\boldsymbol{A}'$ 并串变换得到待解交织数据序列 s，将 s 输入交织编码器得到待译码数据 s'，根据式（1）进行维特比译码得到译码数据 y。

$$\boldsymbol{A}'=\begin{bmatrix}\boldsymbol{R}_1 & \boldsymbol{R}_2\\ \boldsymbol{R}_3 & \boldsymbol{R}_4\end{bmatrix} \tag{17}$$

8）y 去掉尾部 16 b，根据式（4）得到验证哈希值 H'，将 y 尾部 16 b 数据与 H'截取的 16 b 数据进行对比验证。若一致，则证明数据正确，对 y 去掉尾部 16 b 得到待解密数据 y'，根据式（3）对密钥 K 和随机数 N 获取最终状态矩阵，按行输出得到密钥流块，生成二进制序列，与 y'异或得到明文二进制数据 str'，对其进行格式转换得到明文信息 str。算法实现伪代码如下。

输入：印刷量子点矩阵 $\boldsymbol{A}$，插入位置序列 P，伪随机同步信息码组 $\boldsymbol{S}_P$，密钥 K，随机数 N；

输出：明文信息 str；

```
for i=1 to D/2 do
    for i=1 to D/2 do
        遍历子矩阵块；
        使用式（12）检测伪随机同步信息并获取汉明距离 hρ 和索引 ρ；
        if hρ≤2 then
            使用式（8）和式（13）更新掩膜信息 γ 和区域定位因子 α；
            查找表 3 得到区域分割因子 β；
            使用式（14）更新区域分割坐标 O；
            使用式（15）获得 4 组矩阵碎片 An；
            使用式(16)对 4 组矩阵碎片进行解掩膜；
            子矩阵块以 D/2 部长移位，使用式（8）得到认证掩膜信息 γ′；
            查找表 4 得到重构子矩阵 Rn；
            使用式（17）得到重构矩阵 A′；
            对 A′并串变换输入交织编码器得到解交织数据 s；
            使用式（1）对 s 进行维特比译码得到译码数据 y；
            使用式（4）得到验证哈希值 H′；
            if H′(1∶16) == y(end-15∶end) then
                对 y 去掉后 16 b；
                使用式(3)进行 ChaCha20 解密得到 str′；
                对 str′进行格式转换；
                return 明文信息 str；
            else
                移动到下一位；
            end if
        else
            移动到下一位；
    end if
    end for
end for
```

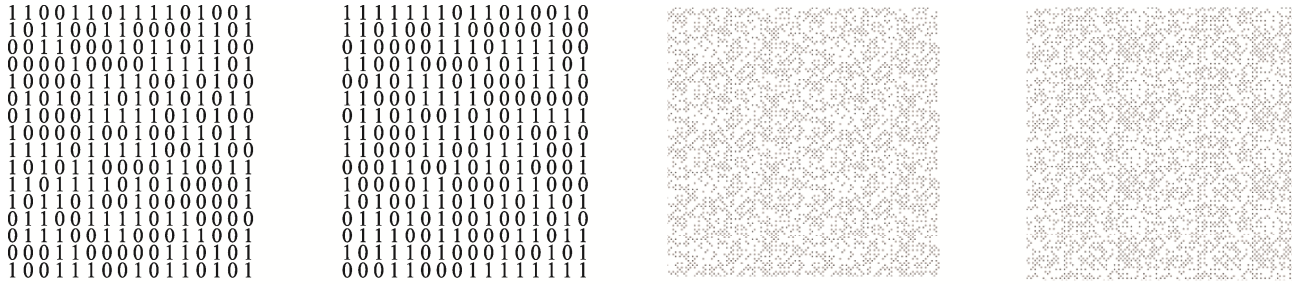
3 实验结果与分析

本研究在 MATLAB R2021a 上进行仿真实验，机身环境为 Xeon(R) Silver 4210 处理器、32 G 内存、64 位 Windows11 操作系统。

3.1 印刷量子点图像生成、植入与识读

选择 2 组 12 位随机数字序列号作为秘密信息生成印刷量子点图像，密钥和随机数相同，扩散映射的角度均为 45°，间隔参数均为 19。2 组秘密信息先后经过规范化处理、ChaCha20 加密、SHA-256 数字签名、卷积编码、交织编码、插入伪随机同步信息和多掩膜置乱，生成 2 组多置乱伪本原矩阵，其中 2 种见图 4a~b；对 2 组多置乱伪本原矩阵进行拼接后扩散映射生成 2 幅印刷量子点图像，见图 4c~d。

为验证本算法的可靠性，对 12 位数字 202 408 056 854 生成的单幅印刷量子点图像进行仿真实验，通过黑白块颜色反转反映数据错误，模拟打印与扫描过程遇到的随机和突发污损情况。用误码率（Bit Error Rate，BER）代表不同程度的污损情况，见表 5~6，可见该算法生成的印刷量子点图像可以抵抗一定程度的噪声攻击。



a 第1组伪本原矩阵　b 第2组伪本原矩阵　c 第1组印刷量子点图像　d 第2组印刷量子点图像

图 4　伪本原矩阵和印刷量子点图像

Fig.4 Pseudo primitive matrix and printed quantum dot images

表 5　不同程度随机污损后信息识读结果

Tab.5 Information literacy results after different levels of random defacement

BER/%	原量子点图像	污损后图像	识读情况
5			误码率：5% 提取信息：202 408 056 584 历时：0.095 694 s
10			误码率：10% 提取信息：202 408 056 584 历时：0.085 389 s
15			误码率：15% 提取信息：202 408 056 584 历时：0.086 180 s
20			误码率：20% 提取信息：202 408 056 584 历时：0.106 254 s

表 6　不同程度突发污损后信息识读结果

Tab.6 Information recognition results after different levels of sudden defacement

BER/%	原量子点图像	污损后图像	识读情况
5			误码率：5% 提取信息：202 408 056 584 历时：0.098 786 s
10			误码率：10% 提取信息：202 408 056 584 历时：0.097 333 s
15			误码率：15% 提取信息：202 408 056 584 历时：0.087 169 s
20			误码率：20% 提取信息：202 408 056 584 历时：0.096 793 s

3.2 实验分析

3.2.1 隐蔽性分析

信息隐藏效果采用峰值信噪比（Peak Signal To Noise Ratio，PSNR）和结构相似性（Structural Similarity Index，SSIM）来评价，计算见式（18）~（19）。

$$P_{\mathrm{SNR}}\left(p(i,j),p'(i,j)\right)=10\lg\frac{m\times n\times 256^2}{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(p(i,j)-p'(i,j)\right)^2} \tag{18}$$

式中：$p(i,j)$为原始图像；$p'(i,j)$为加密图像；m、n 分别为 2 个图像的宽度和高度。

$$S_{\mathrm{SIM}}(x,y)=\frac{\left(2u(x)u(y)+C_1\right)\left(2Cov(x,y)+C_2\right)}{\left(u(x)^2+u(y)^2+C_1\right)\left(s^2(x)+s^2(y)+C_2\right)} \tag{19}$$

式中：x 为原始图像；y 为加密图像；$u(x)$、$u(y)$为均值；$Cov(x,\ y)$为协方差；$s^2(x)$、$s^2(y)$为方差；C_1=0.01×256^2，C_2=0.03×256^2。

3.1 节生成的含复合光谱印刷量子点图像，嵌入率(Embedding Rate)为 2 bpp，计算得到的 PSNR 为 40.77 dB，说明含复合光谱印刷量子点图像的不可见性满足客观评价要求；SSIM 为 0.97，说明含复合光谱印刷量子点图像的质量损失较小，与原始载体图像之间的相似性较大。

3.2.2 算法鲁棒性对比

与文献[16]~[18]以及(7, 4)汉明码进行对比实验，测试不同算法可以正确译码的最大 BER，见表 7。实验对比结果表明，本算法采用的(331, 225, 367)卷积码加块交织编码方案，相比随机交织具有更强的结构化特性，能够提供更加稳定的抗干扰性和鲁棒性。同时，(331, 225, 367)卷积码的编码率相对较高，错误恢复能力较强，在 BER 达到 20%时，生成的印刷量子点图像仍能被准确识别，证明该算法在图像打印过程中具备更强的抗污损和正确识读能力。

表 7 不同 BER 下不同算法译码情况

Tab.7 Decoding by different algorithms at different BER

噪声类型	BER/%	是否正确译码(Yes/No)				
		文献[16]	文献[17]	文献[18]	(7, 4)汉明码	本算法
随机噪声	≤2.5	Yes	Yes	Yes	Yes	Yes
	(2.5, 7.5]	No	Yes	Yes	Yes	Yes
	(7.5, 10.0]	No	Yes	Yes	No	Yes
	(10.0, 12.0]	No	Yes	No	No	Yes
	(12.0, 20.0]	No	No	No	No	Yes
	>20.0	No	No	No	No	No
突发噪声	≤7.0	Yes	Yes	Yes	Yes	Yes
	(7.0, 12.0]	No	Yes	Yes	No	Yes
	(12.0, 16.0]	No	Yes	No	No	Yes
	(16.0, 20.0]	No	No	No	No	Yes
	>20.0	No	No	No	No	No

3.2.3 算法效率性对比

针对截取的不同尺寸印刷量子点图像，测试不同算法的解码时间，见表 8。实验结果表明，本文采用的伪随机同步信息分散插入方式，通过相邻数据联合解算，相较于文献[16-18]中采用的遍历查询同步信息的方案，在面对噪声干扰时具有显著优势，能够提高译码速度，并且对于高噪声环境下的同步和数据恢复具有更好的鲁棒性，对不同尺寸下图像的识读时间保持在 0.2 s 以内，能够在实际应用中为用户提供更优的体验。

表 8 不同算法的印刷量子点信息解码时间

Tab.8 Decoding time of printed quantum dot information by different algorithms

像素尺寸	识读时间/s				
	文献[16]	文献[17]	文献[18]	(7, 4)汉明码	本算法
87×87	0.57			0.84	0.08
90×90	0.78		0.45		0.09
111×111	1.86	1.46	1.42		0.09
120×120	3.12	1.47	2.48	3.32	0.10
135×135	5.72	1.47	4.70	5.86	0.10
180×180	18.70	1.51	16.33	19.06	0.12

4　结语

利用 SHA-256 哈希算法生成的哈希函数验证比特数据，确保数据被篡改时能够得到有效验证，同时加入 ChaCha20 加密算法，使得未经密钥的用户无法读取数据内容，从而确保机密性。通过交织编码将突发噪声转换为随机噪声干扰，利用(331, 225, 367)卷积码对随机噪声的纠错能力，进一步增强印刷量子点图像的鲁棒性；伪随机同步信息分散插入，使得相邻数据之间互相提供先验信息，保证任意截取一块印刷量子图像即可解码，极大地提高解码速度。通过同色异谱技术，用 2 幅印刷量子点图像对载体图像进行信息调制，使得可见光和红外光下显示不同的印刷量子点图像，提高信息嵌入容量。实验表明，本算法生成的印刷量子点图像 BER 可以达到 20%，识读时间在 0.1 s 左右；含复合光谱印刷量子点图像嵌入率为 2 bpp，与原始载体图像的 PSNR 约为 40 dB，SSIM 约为 0.97。

参考文献：

[1] LIN Y H, ZHANG H K, FENG J Y, et al. Unclonable Micro-Texture with Clonable Micro-Shape towards Rapid, Convenient, and Low-Cost Fluorescent Anti-Counterfeiting Labels[J]. Small, 2021, 17(30): 2100244.

[2] WANG T Y, ZHENG H, YOU C H, et al. A Texture-Hidden Anti-Counterfeiting QR Code and Authentication Method[J]. Sensors, 2023, 23(2): 795.

[3] WANG T Y, ZHENG H, GUO Z Y, et al. Anti-Counterfeiting Textured Pattern[J]. The Visual Computer, 2024, 40(3): 2139-2160.

[4] DING S, LYU X, XIA Y, et al. Fluorescent Materials Based on Spiropyran for Advanced Anti-Counterfeiting and Information Encryption[J]. Molecules, 2024, 29(11): 2536.

[5] GAO D L, GAO J, GAO F, et al. Quintuple-Mode Dynamic Anti-Counterfeiting Using Multi-Mode Persistent Phosphors[J]. Journal of Materials Chemistry C, 2021, 9(46): 16634-16644.

[6] LI Y J, GAO P F. Emerging Luminescent Materials for Information Encryption and Anti-Counterfeiting: Stimulus-Response AIEgens and Room-Temperature Phosphorescent Materials[J]. Chemosensors, 2023, 11(9): 21.

[7] DATTA K, JANA B, SINGH P K, et al. Robust Data Hiding Scheme for Highly Compressed Image Exploiting BTC with Hamming Code[J]. Multimedia Tools and Applications, 2024, 83(3): 8591-8628.

[8] LI L, CHANG C C, LIN C C. Reversible Data Hiding in Encrypted Image Based on (7, 4) Hamming Code and UnitSmooth Detection[J]. Entropy, 2021, 23(7): 790.

[9] KIM C, YANG C N, ZHOU Z L, et al. Dual Efficient Reversible Data Hiding Using Hamming Code and OPAP[J]. Journal of Information Security and Applications, 2023, 76: 103544.

[10] LIEN B K, CHEN S K, WANG W S, et al. Dispersed Data Hiding Using Hamming Code with Recovery Capability[C]// International Conference on Genetic and Evolutionary Computing, 2015: 179-187.

[11] WU X T, YANG C N, LIU Y W. A General Framework for Partial Reversible Data Hiding Using Hamming Code[J]. Signal Processing, 2020, 175: 107657.

[12] NGUYEN T D, LE H D. A Reversible Data Hiding Scheme Based on (5, 3) Hamming Code Using Extra Information on Overlapped Pixel Blocks of Grayscale Images[J]. Multimedia Tools and Applications, 2021, 80(9): 13099-13120.

[13] WANG C Y, LI C. A Steganography Approach for Printed Image Based on Image Complexity and Template Matching[J]. The Open Automation and Control Systems Journal, 2014, 6(1): 84-97.

[14] VINOTH K C, NATARAJAN V, NIRMALA K, et al. Encrypted Separable Reversible Watermarking with Authentication and Error Correction[J]. Multimedia Tools and Applications, 2019, 78(6): 7005-7027.

[15] ZHU J L, CAO P, WANG X, et al. Research on Printing Quantum Dot Anti-Counterfeiting Image Generation and Recognition Technology[C]// the 4th International Conference, 2018: 91-95.

[16] 王育军，曹鹏. 基于印刷量子点的多重组合信息可靠性编解码算法[J]. 包装工程, 2021, 42(19): 192-203.
WANG Y J, CAO P. Reliability Encoding and Decoding Algorithm of Multiple Combination Information Based on Printed Quantum Dots[J]. Packaging Engineering, 2021, 42(19): 192-203.

[17] 王育军，曹鹏，王明飞，等. 基于 Turbo 码的印刷量子

点信息隐藏算法研究[J]. 数字印刷, 2022(4): 195-206.
WANG Y J, CAO P, WANG M F, et al. Research on Information Hiding Algorithm for Printing-Quantum-Dots Based on Turbo Codes[J]. Digital Printing, 2022(4): 195-206.

[18] 邱英英, 曹鹏. 印刷量子点点阵信息可靠性编解码算法[J]. 计算机科学与应用, 2023, 13(3): 617-625.
QIU Y Y, CAO P. Reliability Codec Algorithm for Printed Quantum Dot Lattice Information[J]. Computer Science and Applications, 2023, 13(3): 617-625.

[19] LYU G W, CAO P, HUANG Y. Maximum Dynamic Range of GCR Based on Metamerism and Application[J]. International Journal of Scientific & Technology, 2021, 10(8): 152-158.

[20] KUZNETSOV Y V. High-Definition Halftone Printing[J]. Principles of Image Printing Technology, 2021: 331-352.

[21] WYSZECKI G, STILES W S. Color Science: Concepts and Methods, Quantitative Data and Formulae[M]. 2nd ed. New York: Wiley, 1982.

[22] LIN S, COSTELLO D J. Error Control Coding[M]. New Jersey: Prentice Hall, 2004.

[23] LIEB J, PINTO R, ROSENTHAL J. Convolutional Codes[M]. Florida: CRC Press, 2021: 197-226.

[24] VITERBI A. Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm[J]. IEEE Transactions on Information Theory, 1967, 13(2): 260-269.

[25] KEBANDE V R. Extended-Chacha20 Stream Cipher with Enhanced Quarter Round Function[J]. IEEE Access, 2023, 11: 114220-114237.

[26] WANG J, LIU G, CHEN Y Q, et al. Construction and Analysis of SHA-256 Compression Function Based on Chaos S-Box[J]. IEEE Access, 2021, 9: 61768-61777.