基于路径规划和像素翻转的鲁棒二维码隐写算法

李红棒[1],董理[1],王让定[1],严迪群[1],李元满[2],廖鑫[3]
(1.宁波大学信息科学与工程学院,浙江 宁波 315211;2.深圳大学电子与信息工程学院,广东 深圳 518000;
3.湖南大学信息科学与工程学院,湖南 长沙 410000)

摘 要: 二维码作为一种高效的信息存储和传输方式,广泛应用于支付、广告和物流等领域。然而,现有二维码隐写技术在噪声和干扰环境下的鲁棒性和隐蔽性尚存不足,难以满足高安全性信息传输的需求。为此,提出一种基于路径规划和像素翻转的鲁棒二维码隐写算法。该算法通过将二维码视为迷宫,结合路径规划算法选择像素进行翻转,确保在不影响二维码正常识别的前提下增强秘密信息的抗干扰能力。在技术实现上,首先设计了路径规划算法用于选择最优像素点,以减少信息嵌入对二维码图像质量的影响;其次,结合像素翻转技术实现秘密信息的嵌入,并分析其在不同噪声条件下的表现。采用噪声攻击、图像扰动、物理失真等典型干扰场景对算法进行测试,并以嵌入容量、图像质量,以及信息恢复率为评价指标。实验结果表明,该算法在提高二维码隐写的鲁棒性和隐蔽性方面具有显著优势,适用于信息安全需求较高的场景,同时为二维码隐写技术的进一步发展提供了新的思路。

关键词: 二维码隐写;图像隐写术;电脑鼠;路径规划;数字水印;鲁棒隐写
中图分类号: TP309.2 **文献标志码:** A **DOI:** 10.19678/j.issn.1000-3428.0252005

Robust QR Code Steganography Algorithm Based on Path Planning and Pixel Flipping

LI Hongbang[1], DONG Li[1], WANG Rangding[1], YAN Diqun[1], LI Yuanman[2], LIAO Xin[3]
(1.Faculty of Electrical Engineering and Computer Science, Ningbo University, Ningbo 315211, Zhejiang, China;
2.College of Electronics and Information Engineering, Shenzhen University, Shenzhen 518000, Guangdong, China;
3.College of Computer Science and Electronic Engineering, Hunan University, Changsha 410000, Hunan, China)

【Abstract】 As an efficient information storage and transmission method, QR codes are widely used in payment, advertising, and logistics. However, the robustness and steganography of existing QR code steganography techniques in noisy and disturbed environments are insufficient to meet the needs of high-security information transmission. Therefore, a robust QR code steganography algorithm based on path planning and pixel flipping is proposed. The algorithm ensures that the anti-jamming ability of the secret information is enhanced without affecting the normal recognition of the QR code by treating the QR code as a labyrinth and selecting pixels to be flipped in combination with the path planning algorithm. In terms of technical implementation, first, a path planning algorithm is designed for selecting the optimal pixel points to reduce the impact of information embedding on the image quality of the QR code; second, the embedding of the secret information is realized by applying the pixel flipping technique and analyzing its performance under different noise conditions. The algorithm is tested via experiments using typical interference scenarios such as noise attack, image perturbation, and physical distortion; the embedding capacity, image quality, and information recovery rate are used as evaluation indexes. The results show that the algorithm has significant advantages in improving the robustness and steganography of QR code steganography and is suitable for scenarios with high information security requirements. Moreover, the proposed algorithm opens avenues for further development of QR code steganography techniques.

【Key words】 QR code steganography; image steganography; MicroMouse; path planning; digital watermarking; robust steganography

0 引言

二维码(QR code)作为一种高效、便捷的信息存储和传输方式,被广泛应用于支付、广告、物流领域,随着二维码应用的日益普及,人们对其在信息安全方面的关注也在不断增加[1]。图像隐写术作为

基金项目: 国家自然科学基金(62171244);浙江省自然科学基金(LY23F020011)。
作者简介: 李红棒(CCF 学生会员),男,硕士研究生,主研方向为多媒体安全;董理(通信作者),副教授、博士;王让定,教授、博士;严迪群,副教授、博士;李元满,助理教授、博士;廖鑫,教授、博士。
收稿日期: 2025-01-06 **修回日期:** 2025-03-26 **E-mail:** dongli@nbu.edu.cn

一种在不引起注意的情况下隐藏信息的方法，能够在数字图像中嵌入秘密信息，从而实现信息的隐蔽传输[2]。随着二维码应用场景的拓展，如何在公开的二维码中隐藏秘密信息成为了学术界和产业界关注的焦点。

传统的二维码隐写方法主要分为误差容忍嵌入法[3]、颜色编码法[4]、空白区域嵌入法[5]、数据加密嵌入[6]、图像隐写术结合[7]和扩展二维码标准[8]等。其中误差容忍嵌入法利用二维码的容错能力，通过改变或微调二维码中特定位置的点来隐藏信息。颜色编码法在传统黑白二维码的基础上，使用不同颜色编码信息，在增加数据容量的同时嵌入秘密信息。空白区域嵌入法则在二维码的周围或空白区域添加秘密信息，这些信息可通过专门的解码设备或软件读取，而普通扫描器会忽略这些区域。数据加密嵌入方法将秘密信息加密后嵌入二维码的数据部分，只有拥有加密密钥的一方才能解码。图像隐写术结合的方法将二维码嵌入到一张图像中，进一步增强秘密信息的隐蔽性。扩展二维码标准使用高密度版本的二维码，在更小空间内嵌入更多信息。

尽管以上方法能够实现信息的隐蔽传输，但由于二维码在实际应用场景中，难以避免需要经过打印扫描或者显示扫描这个过程，因此打印失真、扫描失真等干扰[9-10]难以避免。而上述方法在此种场景下面对噪声和干扰时的鲁棒性仍有待提高。此外，由于二维码图像仅由黑白像素组成，任何对二维码图像纯净度的破坏都极易被肉眼察觉，从而降低隐写的安全性。因此，研究一种既能保持二维码图像纯净，又具备更强鲁棒性的隐写算法具有重要的理论意义和实际价值。

本文受电脑鼠路径规划算法的启发[11]，提出一种基于路径规划和像素翻转的鲁棒二维码隐写算法。对于构造和起点位置、终点位置相同的迷宫，使用不同的路径规划算法会导致电脑鼠走出不同的路径。使用同一种路径规划算法在构造和起点位置、终点位置相同的迷宫中行走，电脑鼠也会走出不同的路径。借鉴这一思想，本文设计一种路径规划算法和二维码像素翻转策略，通过控制起点位置、终点位置、二维码构造和路径规划策略，从而控制电脑鼠在二维码中的行走路径，并将秘密信息编码进其中。本算法在不影响二维码识别性能的前提下，可以显著增强秘密信息的抗干扰能力。本文的主要贡献如下：

1）将路径规划算法引入二维码隐写，通过将二维码视为迷宫，设计路径规划算法选择像素进行翻转，提升秘密信息嵌入的精准性和灵活性。

2）根据二维码容错率高的特点，通过修改特定的像素块，具有较强的鲁棒性。

3）详细讨论路径规划与像素翻转技术对二维码图像质量的影响，确保隐写信息与二维码性能之间的优化平衡，为二维码隐写算法的设计提供新思路。

1 相关工作

在研究鲁棒二维码隐写技术之前，本文首先回顾与此相关的几个重要领域的研究，包括数字图像水印、二维码水印与隐写、路径规划算法和鲁棒数字图像水印。这些领域的研究为本文提供了理论基础和技术支持。

1.1 数字图像水印

数字图像水印是一种基于内容的非加密计算机信息隐藏技术[12]，能够将标识信息直接嵌入到数字载体中，同时不影响原载体的使用价值，并具备难以被察觉和修改的特点，从而实现版权保护和信息隐藏的功能。该技术通常包括嵌入、提取和验证三个主要过程，研究者通过像素值修改、频域变换或空域嵌入等方法完成水印信息的隐藏[13]。数字水印的性能评估主要集中在隐蔽性和鲁棒性两方面。水印信息的长度、嵌入强度以及载体的规格均会对这两项性能产生影响。一般而言，水印信息长度越长、嵌入强度越大，水印的鲁棒性越强，但隐蔽性会有所下降。根据特性，数字图像水印可分为鲁棒水印和脆弱水印。现有技术在图像完整性和鲁棒性方面已取得显著进展，为鲁棒二维码隐写技术的研究提供了重要的参考和启发[14]。

1.2 电脑鼠

电脑鼠[15]是一种由嵌入式微控制器、传感器[16]和机电运动部件构成的智能行走装置，电脑鼠可以在不同“迷宫”中自动记忆和选择路径，采用相应的路径规划算法，快速地达到所设定的目的地。国际电工和电子工程学会每年都举办一次国际性的电脑鼠走迷宫竞赛，这项竞赛目前在美国、英国、日本、韩国、新加坡、台湾等地区颇为盛行。自 1979 年在纽约举行了第一届电脑鼠走迷宫竞赛以来，该竞赛已经风靡全球 40 余年。电脑鼠走迷宫是一项多学科、多技术的融合体，主要涉及电子信息、程序设计、机械工程、自动控制、人工智能、传感与测试技术等多项技术知识。近年来，研究人员致力于提出和优化搜索未知迷宫并找到最短路径的算法[17-18]。二维码是由黑白块组成的二维图案，如图 1 所示（彩色效果见《计算机工程》官网 HTML 版，下同），若把

黑块视为阻碍，白块视为通道，则二维码可以看作是一个迷宫。

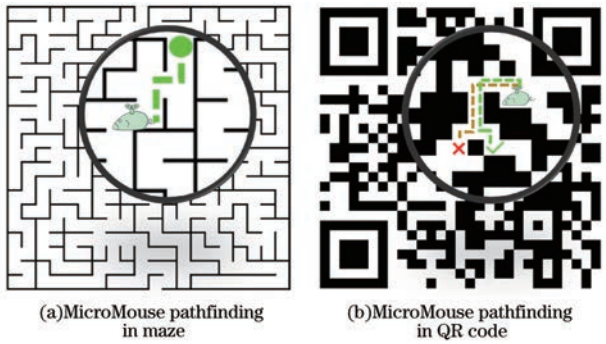

图 1 电脑鼠寻道示意图

Fig. 1 Schematic diagram of MicroMouse pathfinding

1.3 基于二维码的信息隐藏

二维码具有高容错率、大数据容量等特点，通过采用里德-所罗门纠错算法，即使部分二维码被损坏或污损，仍能通过纠错恢复原始数据。利用二维码这一特点设计信息隐藏方案可以取得良好鲁棒性和隐蔽性的效果。HUANG 等[3]利用二维码的纠错能力，提出一种有效的秘密隐藏机制来保护二维码中的敏感信息。秘密信息将被嵌入到基于(8，4)汉明码的载体二维码中。TKACHENKO 等[8]采用特定的纹理模式将二维码替换成黑色模块来构建私有层，设计出了双层二维码，既可以用于私有消息共享，也可以用于身份验证场景。WU 等[19]利用图像处理技术对二维码模块形状进行调整，提出一种基于二维码图像的隐蔽通信数据隐藏方法，在可读性、抗噪声攻击，以及数据嵌入率等方面具有一定优势。LIU 等[20]利用汉明码的特性和二维码的纠错机制，提出一种新型的三层信息丰富的二维码来保护秘密信息，具有信息嵌入效率高、抗常见图像后处理攻击的鲁棒性强等优点。CHEN 等[21]只针对二维码防伪解决方案无法解决物理非法复制的问题，设计一种随机水印嵌入系统，通过调制两个精心选择变换系数之间的关系来嵌入水印位，最终生成的水印以白点图案的形式出现在二维码的黑色模块中。

1.4 路径规划算法研究

路径规划算法[22]是机器人领域的重要研究内容，旨在使机器人从起点到达目标点时有效避开障碍物并优化路径，它包括自由空间建模、路径搜索算法、动态规划、多机器人路径协调，以及智能算法应用。研究者提出了各种路径规划算法[23-24]，包括基于图搜索、启发式搜索、遗传算法。经典的路径搜索算法如 A*和 Dijkstra 在已知环境中表现出色，而快速探索随机树(RRT)和概率路图法(PRM)等算法在复杂和动态环境中更有效。动态规划算法如 D*能够在环境变化时实时调整路径。路径规划技术广泛应用于自动驾驶、仓储物流、无人机送货和医疗机器人等领域，提高了机器人系统的自主性和智能性，为本文算法设计提供了一定的借鉴。

1.5 鲁棒数字图像水印

鲁棒数字图像水印技术是指将水印信息嵌入到数字图像中，能够对一定程度的攻击保持稳定性的技术[25]。通常对原始图像进行一系列变换，将水印嵌入变换后的系数中，例如小波变换[26]、离散余弦变换[27]等。因为变换域系数较为稳定，因此水印图像是鲁棒的，可以抵抗常见的攻击。此外，近些年，许多研究者使用深度学习的方法进行水印算法的设计。TANCIK 等[28]提出的学习型隐写算法 StegaStamp 对图像扰动具有鲁棒性，近似于真实打印和摄影造成的失真空间。FANG 等[29]提出一种基于流的鲁棒数字水印框架，该框架采用可逆噪声层来抵御黑盒失真。在数字图像、音频和视频领域，研究者提出各种鲁棒水印算法，以应对压缩、旋转、噪声等各种攻击。将这些鲁棒水印技术应用于二维码隐写中[30]，可以提高二维码对各种攻击的鲁棒性，保障秘密信息的安全传输和存储。

2 所提方案

2.1 算法框架

本文提出一种在二维码中进行秘密信息隐写的算法，整体系统框架如图 2 所示，主要分为秘密信息嵌入模块和秘密信息提取模块。其中秘密信息嵌入模块包含原始二维码生成、二进制秘密序列生成、隐写二维码及密钥生成等步骤。秘密信息提取包含二维码重建、二进制秘密序列提取、秘密校验解密等步骤。

2.2 路径规划

路径规划算法可根据需要自行设计，为表示方便，在本文中，基于从起点向终点的路径方向上，左转表示“1”，右转表示“0”，采用广度优先搜索[31](BFS)算法作为示例进行路径规划。BFS 算法作为一种经典的图搜索算法，在解决二维码矩阵中的路径规划问题时具有良好的性能和可靠性。

具体而言，本文将二维码矩阵抽象为 1 个图，其中每个像素点对应图中的 1 个节点，节点之间的相邻关系由像素点的 8 个方向(上、下、左、右、左上、右上、左下、右下)确定。BFS 算法通过从起点开始，逐层地搜索其相邻节点，直到找到终点为止。在搜索过程中，本文使用 1 个集合 V 来记录已经访问过的节点，以避免重复访问。

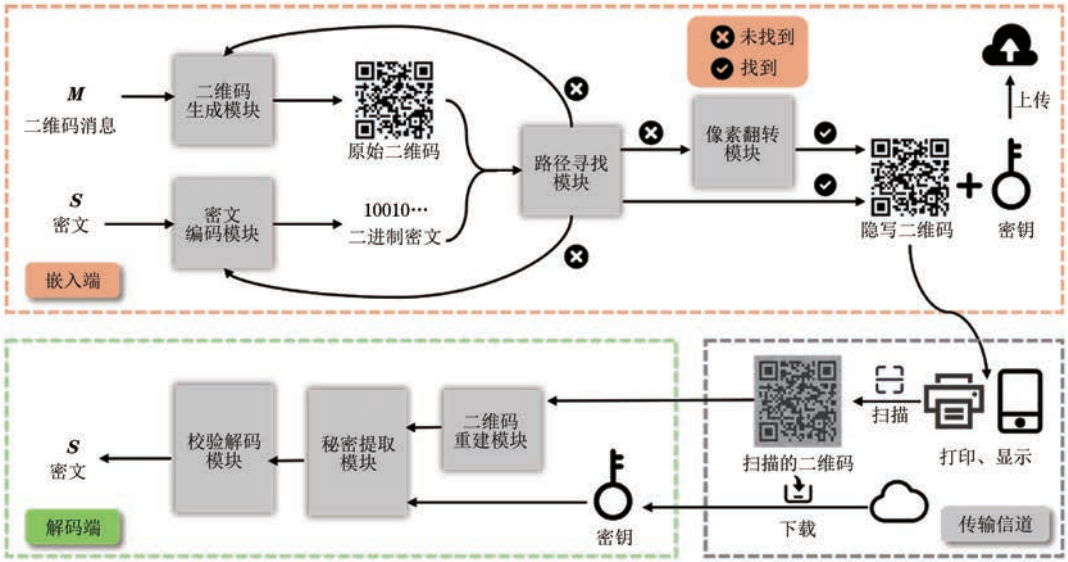

图 2 系统框架

Fig. 2 System framework

具体实现中，首先初始化一个队列 Q，将起点及其路径加入队列中；然后不断从队列中取出节点，并对其相邻节点进行扩展。如果相邻节点尚未访问过且是有效移动位置，则将其加入队列，并更新路径。最终，当找到终点时，算法返回从起点到终点的路径，此路径能够表示秘密信息，其伪代码如算法 1 所示。

算法 1 路径规划算法

输入 二维码像素矩阵 matrix、起点坐标 start、终点坐标 end、二进制秘密序列 W

输出 路径 path

```
1. path=[],V=set(),directions = [(1, 0), (0, 1), (−1, 0), (0, −1), (−1, −1), (−1, 1), (1, −1), (1, 1)] //初始化
2. Q=[(start, [start])];//将起点及其路径加入队列
3. while Q 不为空 do
4.     node, path = Q.popleft() //取出一个节点及其//路径
5.     V.add(node)//将该节点标记为已访问
6.     if node == end do
7.         return path//若当前节点是终点，则返回当前路径
8.     w = W[len(path) % len(W)]//获取下一个秘密//信息
9.     for 每个方向 (dx, dy) in directions do
10.        if w =='0' do
11.            new_x = node[0] + dx
12.            new_y = node[1] + dy
13.        if w == '1' do
14.            new_x = node[0] + dy
15.            new_y = node[1] + dx
16.        new_node = (new_x, new_y)
17.        if 新节点是有效移动位置 and 新节点未被访问 and 新节点为可修改的二维码元素 do
18.            Q.append(new_node,path+ [new_node])//将新节点及其路径加入队列中，并更新路径
19.            V.add(new_node)//将新节点标记为已访问
20. return []//若未找到路径，则返回空路径
```

2.3 隐写嵌入算法

嵌入流程如图 3 所示，主要分为 3 个步骤：

1）生成原始二维码 Q_{org}，这一步涉及明文信息 M 以及在秘密信息嵌入过程中根据自动调整得到的二维码版本 v 和容错率 e。

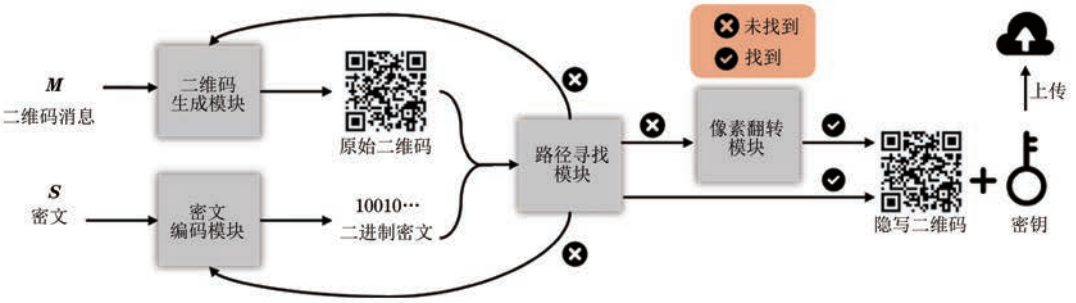

图 3 嵌入流程图

Fig. 3 Embedding flowchart

2)将密文信息 $\boldsymbol{S}$ 通过编码模式 m_c 及添加循环冗余校验(CRC)码得到二进制秘密序列 $\boldsymbol{W}$。

3)将二进制秘密序列按照路径规划模式 m_r 嵌入到生成的二维码中。

在这个过程中,若找到合适的路径,则输出隐写二维码图片 $\boldsymbol{Q}_s$ 以及密钥 key,若无法找到合适的路径,则会依次修改二维码版本、二维码容错率、密文编码模式。在均尝试过所有组合依旧无法找到合适的路径之后,开始对二维码进行修改,翻转指定区域内的若干像素块。若成功找到合适路径,则输出隐写二维码图片 $\boldsymbol{Q}_s$ 以及密钥 key 并将密钥上传至云端,若对像素块的修改达到指定数量仍未找到合适路径,则秘密信息嵌入失败。

2.3.1 二进制秘密序列生成

根据秘密消息 $\boldsymbol{S}$,使用编码模式 m_c 生成二进制秘密序列,然后对生成的二进制秘密序列进行 CRC,添加校验码得到待嵌入的二进制秘密序列 $\boldsymbol{W}$。EC(·)表示二进制秘密序列生成算法,编码模式和二进制秘密序列生成算法可以根据需要自行设计,在设计二进制秘密序列生成算法时,应尽量避免生成的二进制秘密序列存在过多连续的"1"或"0",其数量应控制在 3 以下。二进制秘密序列 $\boldsymbol{W}$ 的表达式如下:

$$\boldsymbol{W}=\mathrm{CRC}(\mathrm{EC}(\boldsymbol{S},m_c)) \tag{1}$$

2.3.2 原始二维码生成

根据消息 $\boldsymbol{M}$,生成版本为 v、容错率为 e 的二维码图片 $\boldsymbol{Q}_{\mathrm{org}}$,其中二维码版本 v 的取值范围是 3～10,容错率 e 包含"M""Q""H"3 个级别,$G(\cdot)$表示二维码生成算法,本文使用 OpenCV 实现。为了优化嵌入效率,二维码版本 v 和容错率 e 的初始值,根据二进制秘密序列的长度动态调整。二维码图片 $\boldsymbol{Q}_{\mathrm{org}}$ 的表达式如下:

$$\boldsymbol{Q}_{\mathrm{org}}=G(\boldsymbol{M},v,e) \tag{2}$$

2.3.3 隐写二维码及密钥生成

根据生成的二维码图片 $\boldsymbol{Q}_{\mathrm{org}}$、二进制秘密序列 $\boldsymbol{W}$,使用路径规划模式 m_r 寻找合适的路径。若寻找成功,则会输出隐写二维码图像 $\boldsymbol{Q}_s$ 以及含有起点位置信息、终点位置信息、编码模式、路径规划模式的密钥 key。若寻找失败,则会依次调整二维码版本、二维码容错率、密文编码模式。若尝试过所有组合均失败,则开始对二维码进行像素翻转,直到翻转的像素数目达到指定个数仍未找到合适的路径,则秘密信息嵌入失败。EM(·)表示隐写二维码及密钥生成算法。

$$\boldsymbol{Q}_s,\mathrm{key}=\mathrm{EM}(\boldsymbol{Q}_{\mathrm{org}},\boldsymbol{W},m_c,m_r) \tag{3}$$

2.4 隐写提取算法

提取流程如图 4 所示,主要分为 3 个步骤:首先对捕获的二维码图像 $\boldsymbol{C}$ 进行重建,得到高质量的二维码图像;然后使用从云端获取的密钥 key 对秘密信息进行解码,提取得到二进制秘密序列 $\boldsymbol{W}'$;最后使用 CRC 对二进制信息进行校验,根据密钥对其进行解码,得到密文消息 $\boldsymbol{S}$。

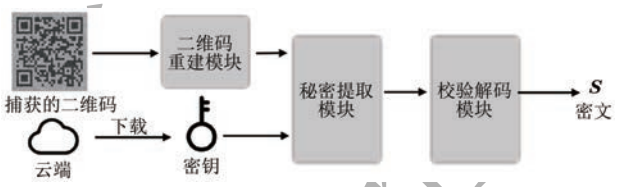

图 4 提取流程图

Fig. 4 Extraction flowchart

2.4.1 二维码重建

捕获的二维码图像 $\boldsymbol{C}$ 受到各种因素的影响会失真,对二维码进行重建可以提高二维码图像的质量,以便后续处理。RS(·)表示二维码重建算法,本文使用 OpenCV 实现对二维码检测与矫正。此外,根据捕获二维码的具体受损程度,可以使用包括但不限于以下算法中的一种或几种:对比度亮度调整、滤波降噪、反二值化、腐蚀膨胀处理、Canny 边缘检测、Hough 算子拟合直线、图像超分辨率重建等。重建的二维码图像表达式如下:

$$\boldsymbol{Q}'=\mathrm{RS}(\boldsymbol{C}) \tag{4}$$

2.4.2 二进制秘密序列提取

使用密钥 key,使用二进制秘密序列提取算法 DC(·)对重建的二维码图像 $\boldsymbol{Q}'$ 进行解码,提取出二进制秘密序列 $\boldsymbol{W}'$。具体来说,根据密钥中的起点位置信息、终点位置信息、路径规划模式 m_r,找到一条连接起点和终点的路径。基于本文从起点向终点的路径方向上,左转表示"1",右转表示"0"的设定,还原二进制秘密序列 $\boldsymbol{W}'$,如式(5)所示:

$$\boldsymbol{W}'=\mathrm{DC}(\boldsymbol{Q}',\mathrm{key}) \tag{5}$$

2.4.3 秘密校验解密

对提取的二进制秘密序列 $\boldsymbol{W}'$ 进行循环冗余校验,校验通过后使用密钥通过秘密校验解密算法 EX(·)对其进行解码,得到秘密信息明文 $\boldsymbol{S}'$。具体来说,本文使用 CRC8 对二进制秘密序列进行校验,校验通过后根据密钥中的编码模式 m_c 还原秘密信息。秘密信息明文 $\boldsymbol{S}'$ 如式(6)所示:

$$\boldsymbol{S}'=\mathrm{EX}(\mathrm{CRC}(\boldsymbol{W}'),\mathrm{key}) \tag{6}$$

2.5 像素翻转

在讨论二维码像素翻转之前,本文先给出其基本的解释和定义,然后讨论其理论基础、翻转区域与翻转策略。

定义 1 二维码像素翻转是指将二维码中指定位置的若干个像素块进行翻转，由于二维码的像素块只有黑色和白色两种，因此把黑色像素块变为白色或把白色像素块变为黑色。假设二维码原始像素值为 $\theta\in\{0,1\}$，像素翻转后的像素值为 $1-\theta$。

像素翻转的理论基础是二维码的容错机制。二维码使用了纠错码，这些纠错码能够检测和纠正一定数量的错误。设二维码纠错码允许的最大错误像素块数量为 n，通过翻转不超过 n 个像素块嵌入秘密信息，二维码的正常解码不会受到影响。这意味着即使有一定数量的像素块被翻转，二维码的纠错码也能自动纠正这些错误，确保二维码的完整性和可读性。

像素翻转可以取得较好的鲁棒性及隐蔽性的原因是像素翻转前后二维码的信息熵变化较小。信息熵 $H(x)$是度量信息随机性的一个指标。对于二维码图像而言，其信息熵可以反映其像素分布的随机性。假设二维码像素分布的概率密度函数为 $p(x)$，则信息熵可以表示为：

$$H(x)=-\sum_{x}p(x)\log_a p(x) \tag{7}$$

通过翻转像素嵌入秘密信息，假设翻转的像素块数量为 t，如果 t 相对整个二维码的像素块总数 N 来说很小(即 $t\ll N$)，那么嵌入秘密信息后的信息熵变化也会很小，这意味着嵌入秘密信息对二维码整体信息分布的影响不大，从而在视觉上和统计上难以察觉。假设嵌入水印前后像素的概率分布分别为 $p(x)$和 $p'(x)$，由于 $t\ll N$，则 $p(x)\approx p'(x)$。信息熵变化近似为：

$$\Delta H=H(x')-H(x)\approx 0 \tag{8}$$

这表明嵌入秘密信息前后信息熵变化很小，秘密信息在整体上难以察觉。综上，本文利用二维码的容错设计，采取像素翻转的方法嵌入秘密信息，可以取得较强的鲁棒性以及较好的隐蔽性。

对于像素翻转区域，由于二维码由多个不同的组成部分构成[32]，每块区域都包含特定的信息，这些区域包括定位图案、对齐图案、计时模式、格式信息、编码数据、版本信息。为了保证二维码的可识读性以及信息隐藏的隐蔽性，像素翻转的区域限制为数据和纠错码字区域。

为了快速寻找能表示待嵌入二进制串的路径，降低像素翻转过程的算法复杂度，节省时间和计算资源。本文在无法搜索到合适的能够表示秘密信息的路径时，优先寻找能表示其最长子串的路径，并在其尾端附近进行随机像素翻转。

$$\begin{cases}\theta=\theta, & \text{像素不在当前路径附近或禁止翻转区域}\\ \theta=1-\theta, & \text{像素在当前路径附近且允许翻转区域}\end{cases} \tag{9}$$

3 实验与分析

3.1 测试环境及设置

为了验证本文算法的有效性和鲁棒性，在实验部分重点针对所提算法进行性能测试，并对所提算法的信息容量及安全性进行分析。

本文算法在 Python 中实现，使用 OpenCV 库实现二维码的编码和解码。本文针对多个包含不同编码信息及秘密信息的二维码进行了多次实验，实验结果均验证了本文方法的鲁棒性。为了更直观地展示受攻击后的二维码图像，本节实验中二维码的编码信息 $\boldsymbol{M}$ 统一设置为“Ningbo University”，秘密信息 $\boldsymbol{S}$ 设置为“1986”，将其编码成 16 bits 长度的二进制流，二维码版本为“3”，纠错等级为“L”。在打印扫描实验中，使用打印机型号为 Brother MFC-T4500DW，纸张为普通 A4 纸，打印质量设置为标准，打印图像尺寸为 4 cm×4 cm，扫描设备为 iPhone 15。在显示扫描实验中，显示设备为 iPhone XR，扫描设备为 iPhone 15。

3.2 隐写隐蔽性

隐写隐蔽性是衡量隐写算法性能的重要标准之一，主要指信息嵌入后对载体数据的视觉或统计特性影响程度。对于二维码图像，由于其像素仅由黑白两种颜色构成，因此任何影响图像纯净度的改动都极易被肉眼察觉。因此，在设计隐写算法时，必须尽可能减少对二维码结构的干扰，以确保隐写后的图像仍然保持其原有的视觉特性和可读性。

本实验针对不同隐写方法的隐蔽性进行对比分析，选取了多种图像领域经典隐写算法，包括最低有效位(LSB)[33]、离散小波变换(DWT)-奇异值分解(SVD)[34]、StegaStamp[28]，以及文献[8,21]所提的两种二维码隐写算法与本文算法进行比较，以全面评估各算法在视觉隐匿性方面的表现。其中 LSB 是一种经典的图像隐写算法，通过替换图像像素的最低有效位来嵌入信息。DWT-SVD 将信息嵌入到图像的频域部分。StegaStamp 是一种基于深度学习的隐写算法，使用神经网络自动学习嵌入和提取信息的过程。文献[8,21]所提的算法通过对二维码的黑色像素块进行特定的修改用于隐藏秘密信息。

多种水印算法效果对比如图 5 所示。如图 5(a)和图 5(b)所示，文献[8,21]所提算法在二维

码的黑色像素块上进行了修改，使得其变化程度达到肉眼可见的水平。对于其余四种算法而言，除StegaStamp 在局部区域存在轻微的残影之外，其余三种算法均能保持二维码图像的纯净度，未引入明显可见的视觉伪影。鉴于实际隐写应用对隐蔽性具有较高要求，为避免信息嵌入对二维码的完整性和可读性造成影响，本文后续不再考虑文献[8，21]所提的算法。

图 5 多种水印算法效果对比

Fig.5 Comparison of the effect of various watermarking algorithms

3.3 隐写鲁棒性

数字图像在网络或者是现实场景中都很容易受到各种各样的攻击，比如典型的噪声攻击、压缩攻击、旋转攻击等。隐写鲁棒性用于衡量隐写方案抗攻击性的能力。为评价所提算法的鲁棒性，本文选取 LSB、DWT-SVD、StegaStamp 3 种算法进行对比，这 3 种算法都应用于数字图像隐写，广泛用于需要隐藏信息的领域，如数字水印、版权保护、数据保密和信息安全等。

1）噪声环境下鲁棒性实验。

在实际应用中，二维码图像可能会受拍摄条件、传输过程或存储环境的影响而受到各种噪声的干扰。这些噪声会导致图像质量下降，影响在图像中嵌入秘密信息的完整性和可检测性。因此，为了验证本文算法在噪声干扰下的鲁棒性，本节设计并进行了抗噪声攻击实验。

在本实验中，通过对嵌入秘密信息的二维码图像添加不同类型和强度的噪声，包括椒盐噪声[35]和高斯噪声[36]，评估秘密信息的恢复情况和完整性。噪声攻击模拟了图像在实际应用场景中可能遇到的各种干扰，通过分析秘密信息在各种噪声条件下的恢复效果，可以验证隐写算法的可靠性和稳健性。

噪声攻击的实验结果如表 1 所示，随着攻击强度的增加，图像质量不断下降，但是本文算法仍能正确提取秘密信息。实验结果表明，本文算法可以有效抵抗噪声攻击，能够正确重建受噪声攻击后的二维码图像，并且正确提取出秘密信息。

表 1 噪声攻击实验结果

Table 1 Results of the noise attack experiments

算法	椒盐噪声			高斯噪声		
	$d=0.1$	$d=0.2$	$d=0.3$	$V=0.1$	$V=0.2$	$V=0.3$
						
LSB	否	否	否	否	否	否
DWT-SVD	否	否	否	否	否	否
StegaStamp	否	否	否	是	否	否
本文算法	是	是	是	是	是	是

2）图像扰动攻击实验。

在实际应用中，二维码图像可能会受到各种噪声和失真的影响，例如拍摄时的振动或环境光线变化。为了评估高斯模糊对本文算法的影响，本节设计并进行了高斯模糊攻击实验。二维码图像在实际应用中常常会因各种原因受到损坏或污损，例如裁剪、折叠、撕裂等，这些操作可能导致嵌入其中的秘密信息丢失或无法识别。为了验证所提算法在面对这些实际应用场景时的鲁棒性，本节设计并进行了裁剪攻击实验。此外，二维码图像常常需要进行压缩处理以便于存储和传输，而 JPEG 压缩[37]作为一种广泛使用的有损压缩算法，会引入压缩噪声，可能导致嵌入在图像中的秘密信息丢失或难以识别。为了验证所提算法在 JPEG 压缩处理下的鲁棒性，本节设计并进行了抗 JPEG 压缩实验。最后，二维码图像可能会因拍摄角度或使用环境的

变化而发生旋转，这些操作可能影响嵌入在图像中秘密信息的完整性和可检测性。为了验证所提算法在旋转操作下的鲁棒性，本节设计并进行了旋转攻击实验。

图像扰动攻击实验结果如表 2 和表 3 所示。在多种类型及强度的攻击下，秘密信息仍能被正确提取。这说明本文算法可以有效抵抗图像扰动攻击，具有较强的鲁棒性。

表 2 图像扰动攻击实验结果 1

Table 2 Experimental results 1 of image perturbation attack

算法	高斯模糊			裁剪攻击		
	$\sigma=2$	$\sigma=3$	$\sigma=4$	$R=0.1$	$R=0.2$	$R=0.3$
						
LSB	否	否	否	否	否	否
DWT-SVD	否	否	否	是	是	是
StegaStamp	是	是	是	是	是	是
本文算法	是	是	是	是	是	是

表 3 图像扰动攻击实验结果 2

Table 3 Experimental results 2 of image perturbation attack

算法	JPEG 压缩			旋转攻击		
	$p=0.3$	$p=0.6$	$p=0.9$	$\theta=30°$	$\theta=45°$	$\theta=60°$
						
LSB	否	否	否	否	否	否
DWT-SVD	否	否	否	否	否	否
StegaStamp	是	是	是	是	是	否
本文算法	是	是	是	是	是	是

3）物理失真场景实验。

在实际应用中，二维码图像可能会经历物理失真过程，例如打印扫描、屏幕显示扫描等操作，这些操作可能会导致图像质量下降，影响嵌入在图像中秘密信息的完整性和可检测性。因此，为了验证本文算法在物理失真场景下的鲁棒性，本节设计并进行了物理失真场景实验，包括打印扫描实验和屏幕显示扫描实验，通过控制隐写二维码图像与扫码设备之间的距离，测试本文算法的鲁棒性。

在打印扫描实验中，将嵌入秘密信息的二维码图像进行打印，再通过扫描设备提取其中秘密信息[38]。在打印和扫描过程中可能引入噪声、失真和分辨率变化，这些因素可能影响秘密信息的可检测性。通过评估秘密信息在经过打印和扫描后的恢复情况，可以验证隐写算法在物理打印和扫描场景中的可靠性和稳健性。在屏幕显示扫描实验中[39-40]，将嵌入秘密信息的二维码图像在电子屏幕上显示，并使用手机进行扫描。屏幕显示和扫描过程可能引入光照变化、反射、失真和分辨率变化等因素，这些因素可能影响秘密信息的可检测性。通过评估秘密信息在经过屏幕显示和扫描后的恢复情况，可以验证本文算法在显示扫描场景中的可靠性和稳健性。

实验结果如表 4 所示，随着显示设备与扫描设备之间距离的增加，图像质量不断下降，在距离达到 120 cm 后，秘密信息仍能被正确提取。实验结果证明，本文算法能有效抵抗打印扫描场景及显示扫描场景下的失真。

3.4 隐写分析

隐写分析是一种通过分析载体的统计特性来判断其中是否隐藏额外信息，甚至估计信息嵌入量或提取隐藏信息内容的技术。为了验证本文算法的抗隐写分析能力，本节使用广泛应用的开源工具 StegExpose[41] 对本文算法生成的载密二维码图像进行隐写分析测试。实验中，随机生成 2 000 张无隐写信息图像和 2 000 张嵌入隐写信息的二维码图

表 4 物理失真场景实验结果

Table 4 Results of physical distortion scenario experiments

算法	打印扫描			显示扫描		
	d=60 cm	d=90 cm	d=120 cm	d=60 cm	d=90 cm	d=120 cm
LSB	否	否	否	否	否	否
DWT-SVD	否	否	否	否	否	否
StegaStamp	是	是	否	是	是	否
本文算法	是	是	是	是	是	是

像，其中二维码编码信息为 16 bit 随机英文字母，秘密信息为 4 bit 随机数字编码成的 16 bit 二进制流。二维码版本设定为“3”，纠错等级为“L”。

对隐写分析结果进行统计分析后绘制的 ROC 曲线如图 6 所示，曲线下的面积为 0.49。这表明 StegExpose 的检测性能接近随机猜测，说明本文方法能够有效规避标准隐写分析工具的检测，满足隐写的不可检测性要求。

近年来，深度学习技术与图像隐写及其检测的结合已成为研究热点。为评估所提方法在隐写分析网络下的安全性，本文采用 SRNet 模型[42]进行隐写分析。SRNet 在空域和频域隐写算法的检测方面均表现出较优的性能。通常，检测精度越接近 50%，表明隐写图像中的秘密信息越难以被识别，从而提升隐写安全性。实验结果表明，本文方法的检测准确率为 53%，表明其能够有效抵抗隐写分析工具的检测，具有较强的安全性。

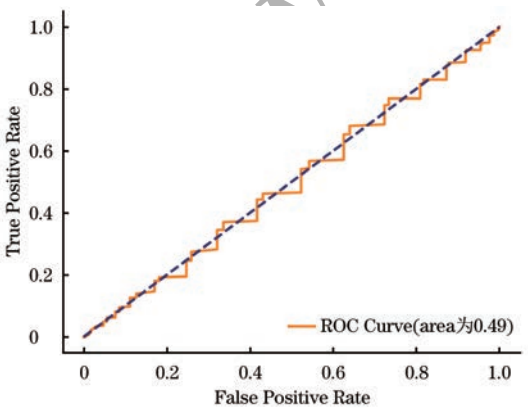

图 6 StegExpose 隐写分析结果 ROC 图

Fig. 6 ROC plot of StegExpose steganalysis results

3.5 路径规划算法选择

不同的路径规划算法基于不同的原理，使用不同的路径规划算法会带来不同的时间消耗。目前路径规划算法存在的主要问题为环境建模困难、算法收敛速度慢、容易陷入局部最优解。常用的路径规划算法包括 BFS 算法[43]、DFS 算法[44]、Dijkstra 算法[45]、A*算法[46]等。

BFS 算法是一种在无权图或网格图中寻找最短路径的有效算法。它能按层次逐渐扩展节点，因此能发现最短路径，且实现简单，适用于实时性要求较高的场景。相对于其他算法，BFS 算法的空间复杂度较低，缺点是它只能处理无权图，无法应对带权图。此外，BFS 算法的时间复杂度较高，在处理大规模图时，性能会受到限制。而且在复杂图结构下，BFS 算法的空间开销也较大。

相比之下，DFS 算法空间复杂度较低，特别适用于路径深度较大的问题。由于 DFS 算法采用栈结构进行深度遍历，其空间复杂度为 $O(h)$，其中 h 为树的最大深度。因此，它在树形结构或深度优先搜索时非常高效。然而，DFS 的缺点是无法保证找到最短路径，可能会陷入较深的分支，在不理想的路径上浪费时间。此外，DFS 算法也无法处理带权图，因此在路径规划任务中，它的应用场景较为有限。

Dijkstra 算法是最经典的带权图最短路径算法，适用于加权图中的路径规划问题，它能够计算出边权不同图中的最短路径，特别是当图的边权不一致时，Dijkstra 算法展现了其优势。但该算法的时间复杂度较高，在使用邻接矩阵时，其时间复杂度为 $O(V^2)$，即使使用堆优化，也只能降低为 $O((V+E)\log_a V)$。此外，Dijkstra 算法的空间复杂度较高，这使得它在处理大型图时效率较低。

A*算法结合了启发式函数，能够引导搜索方向，通常比 Dijkstra 算法更高效，尤其是在需要快速路径搜索的大规模图中。A*算法通过启发式函数能够更智能地缩小搜索范围，从而在带权图中快速找到最优路径。然而，A*算法的性能高度依赖于启

发式函数的选择，如果启发式不合适，可能会导致性能下降，甚至表现不如 Dijkstra 算法。此外，A*算法的计算复杂度较高，尤其在启发式函数不准确时，计算开销也较大。

综上所述，对于本文实时性要求较强且图结构相对简单的场景使用 BFS 算法是合适的。相较于 Dijkstra 算法和 A*算法，BFS 算法的实现更加简单，且能够有效避免不必要的复杂计算。虽然 DFS 算法在空间复杂度上具有优势，但在路径规划中，由于其不能保证找到最短路径，且在深度较大的问题中可能陷入死循环或无效路径，BFS 算法仍然是更合适的选择。

下面对于各算法在寻找路径过程中的效率进行实验。对于同一个二维码，使用不同的路径规划算法，记录其在寻找相同长度的所有路径所用的平均时间。实验结果如图 7 所示，从图 7 可以看出，在隐写长度小于 18 bits 时，BFS 算法表现最好，在隐写长度达到 20 bits 时，表现最好的是 A*算法。考虑到 BFS 算法非常直观和简单，只需要一个队列就可以实现，它不需要复杂的启发式函数或额外的代价计算。相比一些复杂的启发式搜索算法（如 A*），BFS 算法的实现更加直接，不需要额外存储启发式信息或代价估算等优点。综上，本文选择采用 BFS 算法作为路径规划算法。

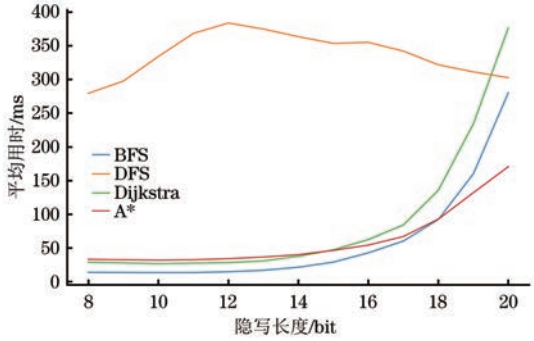

图 7 不同路径规划算法效率对比

Fig. 7 Comparison of the efficiency among different path planning algorithms

3.6 隐写容量

隐写容量与二维码版本、二维码容错率及路径规划算法直接相关。在本实验中，固定使用 BFS 作为路径规划算法，二维码容错率设置为业内常用的“H”水平进行实验。实验结果如表 5 所示，本文算法的隐写容量较小。使用常用的版本为“3”，纠错等级为“H”的二维码，最多隐藏 20 bit 长度的信息，在提高二维码版本的情况下，隐写容量增加有限，在二维码的版本达到“10”，隐写容量增加至 56 bit。

表 5 不同版本二维码的隐写容量

Table 5 Steganographic capacity of different versions of QR codes

二维码版本	二维码图像	数据容量/Byte	隐写容量/bit
3		53	20
4		78	26
5		106	32
6		134	36
7		154	39
8		192	42
9		230	48
10		271	56

3.7 算法复杂度分析

算法复杂度分析是对算法性能的客观评估，涉及到对算法执行时间和空间消耗的量化分析，本节对所提算法的复杂度进行了详细的分析。

1）秘密信息嵌入。

首先，本文采用了 BFS 算法作为路径规划算法。该算法的时间复杂度为 $O(V+E)$、空间复杂度为 $O(V)$，其中 V 是顶点数量，E 是边数量。由于本文算法主要基于图的搜索，因此时间复杂度与图的大小和连通性直接相关。

其次，在修改矩阵和处理最短路径时，本文算法的时间复杂度较低。对于修改矩阵的过程，时间复

杂度为 $O(N)$，其中 N 是要修改的元素数量。而在最短路径的处理和图形绘制过程中，时间复杂度主要取决于矩阵中的非零元素数量 V，因此时间复杂度为 $O(V)$。

总体而言，本文算法在时间方面都表现出了较高的效率。在应用中，它能够有效地处理二维码图像，并且具有较低的资源消耗。

2)秘密信息提取。

解码端的算法复杂度分析旨在评估解码过程中的时间和空间资源消耗。该部分主要包括最短路径搜索和路径方向获取等关键步骤。

首先，在最短路径搜索阶段，本文应用了 BFS 算法，其时间复杂度取决于图的规模和复杂度。在最坏情况下，搜索整个图的时间复杂度为 $O(V+E)$，其中 V 是顶点数量，E 是边的数量。在空间方面，搜索过程中需要维护一个队列，因此空间复杂度为 $O(V)$，其中 V 是图中顶点的数量。

其次，在获取二进制秘密的过程中，根据最短路径的结果，获取路径的方向信息，将其还原为二进制秘密。这一过程的时间复杂度是 $O(K)$，其中 K 是路径的长度。在空间方面，获取路径方向的过程中没有消耗额外的空间，空间复杂度为 $O(1)$。

综上所述，解码端的算法复杂度主要受最短路径搜索过程的影响，其时间复杂度为 $O(V+E)$，空间复杂度为 $O(V)$，其中 V 是图中顶点的数量，E 是边的数量。其他步骤的复杂度较低，都是 $O(n)$ 或 $O(1)$级别。

3.8 比较与分析

本节选取 LSB、DWT-SVD、StegaStamp 3 种算法进行对比，主要对比算法的隐蔽性、鲁棒性、复杂度等指标。

首先，从隐蔽性上看，StegaStamp 隐蔽性最差，其余 3 种算法隐蔽性良好，均保持了二维码图像的纯净。LSB 算法和 DWT-SVD 算法未对二维码像素进行改动，本文算法对二维码像素进行了翻转，4 种算法均不影响二维码的识别。

其次，从鲁棒性上看，LSB 算法的鲁棒性最差，稍微的图像处理(如压缩、噪声、滤波等)都可能破坏嵌入的信息。其次是 DWT-SVD，对常见的图像处理操作(如压缩、噪声、滤波等)有较好的抵抗力。再次是 StegaStamp，深度学习模型能够学习到抵抗各种图像处理操作(如压缩、噪声、滤波等)的特征。在训练过程中，可以通过加入各种扰动和变换增强模型的鲁棒性，使得嵌入的信息在各种情况下都能有效提取。由于本文算法直接对二维码像素进行修改，因此具有较强的鲁棒性。

最后，对于算法复杂度，LSB 算法时间复杂度为 $O(n)$，空间复杂度为 $O(1)$，其中 n 是图像像素的数量。DWT-SVD 算法的时间复杂度为 $O(n\log_a n)$(DWT 分解和重建)$+O(m^3)$(SVD 分解和重建)，其中 n 是图像像素的数量，m 是子带矩阵的维度。空间复杂度为 $O(n)$，需要存储 DWT 子带和 SVD 的矩阵。StegaStamp 训练阶段的时间复杂度为 $O(T\times n\times p)$，其中 T 是训练轮数，n 是训练样本数量，p 是神经网络的参数数量。推理阶段的时间复杂度为 $O(p)$，在推理阶段，只需一次前向传播，空间复杂度为 $O(p)$。本文算法复杂度高于 LSB 算法和 DWT-SVD 算法，远小于 StegaStamp。综上，本文算法在具有良好隐蔽性以及较低算法复杂度的基础上，可以取得较强的鲁棒性。

4 结束语

本文受电脑鼠的启发，根据二维码容错率高的特点，提出一种基于路径规划和像素翻转的鲁棒二维码隐写算法。本文设计一种路径规划算法、二维码像素翻转策略，控制起点位置、终点位置、二维码构造和路径规划策略，从而控制电脑鼠在二维码中的行走路径，并将秘密信息编码进其中。实验结果表明，本文所提算法可以有效实现二维码鲁棒隐写，具有鲁棒性强、隐蔽性好、安全性高的特点，但存在隐写容量较低的问题，未来工作将致力于提升隐写容量。

参考文献

[1] SHANKAR B P, RAJKUMAR N, VIJI C, et al. Approach to identifying counterfeit products with QR codes and computational algorithms[C]// Proceedings of the 5th International Conference on Smart Electronics and Communication (ICOSEC). Washington D.C., USA: IEEE Press, 2024: 1203-1209.

[2] SUBRAMANIAN N, ELHARROUSS O, AL-MAADEED S, et al. Image steganography: a review of the recent advances[J]. IEEE Access, 2021, 9: 23409-23423.

[3] HUANG P C, CHANG C C, LI Y H, et al. Efficient QR code secret embedding mechanism based on hamming code[J]. IEEE Access, 2020, 8: 86706-86714.

[4] TAN L D, LIU K S, YAN X H, et al. Visual secret sharing scheme for color QR code[C]//Proceedings of the IEEE 3rd International Conference on Image, Vision and Computing (ICIVC). Chongqing, China: IEEE Press, 2018: 961-965.

[5] WAHSHEH H A M, LUCCIO F L. Security and privacy of QR code applications: a comprehensive study, general guidelines and solutions[J]. Information, 2020, 11(4): 217.

[6] LOU S T, SHEN W Q, SHEN G Q, et al. QR code anti-counterfeiting technique with lattice-based cryptography[C]// Proceedings of the International Conference on Cyber Security, Artificial Intelligence, and Digital Economy

(CSAIDE 2023). Nanjing, China: SPIE, 2023: 25.
[7] 宋梦丽. 基于二维码图像的信息隐写算法研究[D]. 武汉: 华中师范大学, 2022.
SONG M L. Research on information steganography algorithm based on QR code image[D]. Wuhan: Central China Normal University, 2022. (in Chinese)
[8] TKACHENKO I, PUECH W, DESTRUEL C, et al. Two-level QR code for private message sharing and document authentication[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(3): 571-583.
[9] BOUJERFAOUI S, DOUZI H, HARBA R. Print-CAM image distortion correction for robust image watermarking[C]// Proceedings of the 26th International Conference on Digital Signal Processing and its Applications (DSPA). Washington D.C., USA: IEEE Press, 2024: 1-6.
[10] EVSUTIN O, MELMAN A, MESHCHERYAKOV R. Digital steganography and watermarking for digital images: a review of current research directions[J]. IEEE Access, 2020, 8: 166589-166611.
[11] RATHNAYAKE O, WIJESEKARA G, SAMARANAYAKE L. A path planning technique to reduce the travel time of a micromouse[C]//Proceedings of the IEEE 17th International Conference on Industrial and Information Systems (ICIIS). Washington D.C., USA: IEEE Press, 2023: 519-523.
[12] BEGUM M, UDDIN M S. Digital image watermarking techniques: a review[J]. Information, 2020, 11(2): 110.
[13] WAN W B, WANG J, ZHANG Y M, et al. A comprehensive survey on robust image watermarking[J]. Neurocomputing, 2022, 488: 226-247.
[14] 温万钦. 数字图像水印算法的研究与应用[D]. 大连: 大连交通大学, 2022.
WEN W Q. Research and application of digital image watermarking algorithm[D]. Dalian: Dalian Jiaotong University, 2022. (in Chinese)
[15] LU L, LIU X X, YOU P Y, et al. Research on micromouse maze search algorithm based on centripetal algorithm[C]// Proceedings of the 7th International Conference on Computing, Control and Industrial Engineering. Berlin, Germany: Springer, 2023: 937-947.
[16] 陈志萌,黄昌清. 基于保偏光纤与少模光纤的激光温度传感器[J]. 光电工程,2024,51(11): 240185.
CHEN Z M, HUANG C Q. Laser temperature sensor based on polarization maintaining fiber and few mode fiber[J]. Opto-Electronic Engineering, 2024, 51(11): 240185. (in Chinese)
[17] BOSE A, BRUNO J, DAMES P, et al. Time constraint finite-horizon path planning solution for micromouse extreme problem[C]//Proceedings of the 2022 19th International Conference on Mobile Ad Hoc and Smart Systems. Washington D.C., USA: IEEE Press, 2022: 325-331.
[18] PAME Y G, KOTTAWAR V G, MAHAJAN Y V. A novel approach to maze solving algorithm[C]//Proceedings of the International Conference on Emerging Smart Computing and Informatics (ESCI). Washington D.C., USA: IEEE Press, 2023: 1-6.
[19] WU D C, WU Y M. Covert communication via the QR code image by a data hiding technique based on module shape adjustments[J]. IEEE Open Journal of the Computer Society, 2020, 1: 12-34.
[20] LIU S J, FU Z X, YU B. Rich QR codes with three-layer information using hamming code[J]. IEEE Access, 2019, 7: 78640-78651.
[21] CHEN J L, DONG L, WANG R D, et al, Physical anti-copying semi-robust random watermarking for QR code[C]// Proceedings of International Workshop on Digital-forensics and Watermarking (IWDW 2022). Berlin, Germany: Springer, 2022: 131-146.
[22] ZULFIQAR M I, ABDULLAH I, AKRAM A, et al. An efficient autonomous maze solving robot based on microcontroller by avoiding obstacles using a decision-making algorithm[C]//Proceedings of the International Conference on IT and Industrial Technologies (ICIT). Washington D.C., USA: IEEE Press, 2023: 1-6.
[23] SÁNCHEZ-IBÁÑEZ J R, PÉREZ-DEL-PULGAR C J, GARCÍA-CEREZO A. Path planning for autonomous mobile robots: a review[J]. Sensors, 2021, 21(23): 7898.
[24] WAHAB M N A, NEFTI-MEZIANI S, ATYABI A. A comparative review on mobile robot path planning: classical or meta-heuristic methods?[J]. Annual Reviews in Control, 2020, 50: 233-252.
[25] WAN W B, WANG J, ZHANG Y M, et al. A comprehensive survey on robust image watermarking[J]. Neurocomputing, 2022, 488: 226-247.
[26] BEGUM M, FERDUSH J, UDDIN M S. A hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transform, and singular value decomposition[J]. Journal of King Saud University-Computer and Information Sciences, 2022, 34(8): 5856-5867.
[27] 王文冰. 基于变换域的数字图像鲁棒水印算法研究[D]. 郑州: 战略支援部队信息工程大学, 2021.
WANG W B. Research of digital image robust watermarking algorithm based on transform domain[D]. Zhengzhou: Information Engineering University, 2021. (in Chinese)
[28] TANCIK M, MILDENHALL B, NG R. StegaStamp: invisible hyperlinks in physical photographs[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Washington D.C., USA: IEEE Press, 2020: 2114-2123.
[29] FANG H, QIU Y P, CHEN K J, et al. Flow-based robust watermarking with invertible noise layer for black-box distortions[C]//Proceedings of the AAAI Conference on Artificial Intelligence. New York, USA: AAAI Press, 2023: 5054-5061.
[30] LIU J N, HAN J, FU K, et al. Application of QR code watermarking and encryption in the protection of data privacy of intelligent mouth-opening trainer[J]. IEEE Internet of Things Journal, 2023, 10(12): 10510-10518.
[31] LINA T N, RUMETNA M S. Comparison analysis of breadth first search and depth limited search algorithms in sudoku game[J]. Bulletin of Computer Science and Electrical Engineering, 2021, 2(2): 74-83.
[32] 郑秋梅, 赵丹, 牛薇薇, 等. 基于多通道的彩色图像多重水印算法[J]. 计算机工程, 2024, 50(9): 246-254.
ZHENG Q M, ZHAO D, NIU W W, et al. Multiple watermarking algorithm for color images based on multi-channel[J]. Computer Engineering, 2024, 50(9): 246-254. (in Chinese)
[33] RACHAEL O, MISRA S, AHUJA R, et al. Image steganography and steganalysis based on Least Significant Bit (LSB)[C]//Proceedings of ICETIT 2019. Berlin, Germany: Springer, 2019: 1100-1111.
[34] ZERMI N, KHALDI A, KAFI R, et al. A DWT-SVD based robust digital watermarking for medical image security[J]. Forensic Science International, 2021, 320: 110691.
[35] ZAINI H, ALQADI Z. High salt and pepper noise ratio reduction[J]. International Journal of Computer Science and Mobile Computing, 2021, 10(9): 88-97.
[36] DENG J Y, YAN M T, WANG X Y, et al. Image denoising algorithm based on Gaussian-pepper noise[C]//Proceedings of the 4th International Conference on Machine Learning and Intelligent Systems Engineering (MLISE). Washington D.C., USA: IEEE Press, 2024: 16-19.
[37] CHEN B J, WU Y Q, COATRIEUX G, et al. JSNet: a simulation network of JPEG lossy compression and

restoration for robust image watermarking against JPEG attack[J]. Computer Vision and Image Understanding, 2020, 197: 103015.
[38] QIN C, LI X M, ZHANG Z Y, et al. Print-camera resistant image watermarking with deep noise simulation and constrained learning[J]. IEEE Transactions on Multimedia, 2024, 26: 2164-2177.
[39] FANG H, ZHANG W M, ZHOU H, et al. Screen-shooting resilient watermarking[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(6): 1403-1418.
[40] FANG H, CHEN D D, WANG F, et al. TERA: screen-to-camera image code with transparency, efficiency, robustness and adaptability[J]. IEEE Transactions on Multimedia, 2022, 24: 955-967.
[41] BOEHM B. StegExpose-a tool for detecting LSB steganography[EB/OL]. [2024-12-01]. https://arxiv.org/abs/1410.6656.
[42] BOROUMAND M, CHEN M, FRIDRICH J. Deep residual network for steganalysis of digital images[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(5): 1181-1193.
[43] SIHOTANG J. Analysis of shortest path determination by utilizing breadth first search algorithm[J]. Jurnal Info Sains: Informatika dan Sains, 2020, 10(2): 1-5.
[44] ALIYAN M, HASAN M Z, QAYOOM H, et al. Analysis and performance evaluation of various shortest path algorithms[C]// Proceedings of the 3rd International Conference for Innovation in Technology. Washington D.C., USA: IEEE Press, 2024: 1-16.
[45] LUO M, HOU X R, YANG J. Surface optimal path planning using an extended Dijkstra algorithm[J]. IEEE Access, 2020, 8: 147827-147838.
[46] TANG G, TANG C Q, CLARAMUNT C, et al. Geometric A-* algorithm: an improved A-* algorithm for AGV path planning in a port environment[J]. IEEE Access, 2021, 9: 59196-59210.

文字编辑 薛晋栋
栏目编辑 赖玉玲