

文章编号: 1002-1582(2026)02-0211-07

基于QR码迭代相位恢复的光学加密算法 在交通图像的应用研究

刘俊龙, 程思, 杨利霞*, 智慧

(安徽大学 电子信息工程学院, 安徽 合肥 230601)

摘 要: 在智能交通系统中, 未加保护的图像数据传输面临着严重的安全威胁, 现有加密方法常受限于图像类型、抗噪能力弱或加密容量有限等问题。为此, 文章提出了一种基于二维 (QR) 码迭代相位恢复的光学加密算法, 并用于交通图像加密中。首先将原始图像转换成QR码, 再使用随机生成的二进制明文掩码和QR码进行异或运算生成多个密文, 这里的明文掩码作为第一个加密密钥。然后利用迭代相位恢复模块将这些密文编码为傅里叶域中的纯相位函数 (即第二个加密密钥) 并相互调制成最终密文。实验结果表明该方法不仅能够恢复出高质量图像, 还具有较好的抗攻击能力。此外, 方法在理论上通过QR码的强容错性与相位调制的多重加密机制, 提升了系统的安全性与鲁棒性。

关 键 词: 交通图像加密; 光学加密; 二维码; 异或运算; 迭代相位恢复

中图分类号: TP394.1; TH691.9

文献标识码: A

Application of QR Code-based iterative phase recovery in optical encryption for traffic image processing

LIU Junlong, CHENG Si, YANG Lixia*, ZHI Hui

(School of Electronic and Information Engineering, Anhui University, Hefei 230601, China)

Abstract: In intelligent transportation systems, unprotected image data transmission faces serious security threats, and existing encryption methods are often limited by image types, weak anti-noise capabilities, or limited encryption capacity. Therefore, An optical encryption algorithm based on two-dimensional (Quick Response) (QR) code is proposed, which is used in traffic image encryption. First, the original image is converted into a QR code, and then a randomly generated binary plaintext mask and QR code are used to generate multiple ciphertexts by XOR operation, where the plaintext mask is used as the first encryption key. Then, the iterative phase recovery module is used to encode these ciphertexts into a pure phase function (i.e., the second encryption key) in the Fourier domain and modulate each other into the final ciphertext. Through a series of experiments, it is proved that the proposed method can not only recover high-quality images, but also have good anti-attack ability. In addition, this method theoretically improves the security and robustness of the system through the strong fault tolerance of QR code and the multiple encryption mechanism of phase modulation.

Keywords: traffic image encryption; optical encryption; code; XOR operations; Iterative phase recovery

收稿日期: 2025-11-17; 收到修改稿日期: 2026-02-16

基金项目: 安徽省研究生质量工程项目 (2023qygz005)

作者简介: 刘俊龙 (1986—), 男, 博士研究生, 从事新一代电子信息技术研究。117343987@qq.com

杨利霞 (1975—), 男, 教授、博/硕士生导师, 从事电磁散射与逆散射、无线通信系统中的电波传播及天线理论与设计、计算电磁学等研究。

* 通讯作者: lixiayang@yeah.net

0 引 言

随着信息技术和网络的普及、应用与进步,我国交通运输行业的信息化建设得到了飞速发展,智能交通系统应运而生^[1,2]。智能交通系统中的大部分数据是以各种图像的形式进行采集、传输和处理的,交通图像是交通系统全流程信息化的数据基础^[3],为交通管理部门提供科学决策的重要手段,交通图像处理的典型应用场景包括高速公路视频联网监控、ETC 门架系统、城市道路交通监控、停车场出入口等。交通图像中包含了大量的个人隐私信息^[4],如车辆号牌、驾驶员人脸等信息,在公共信道传输过程中,采集到的图像极易受到黑客攻击,从而导致信息丢失、泄露和被篡改等。因此,设计有效的图像加密方法来保障交通图像的安全传输,对于维护公共安全、提升交通管理效率、促进智能交通发展以及保护隐私与数据安全等方面都具有极其重要的意义。

为了保护图像信息的安全,图像加密技术采用编码方法将待加密的图像转换成难以识别的噪声图像^[5,6],以保护其内容不被未经授权的用户访问。基于光学理论与方法,光学图像加密技术以其高速处理、高并行性能以及大密钥空间等优势而备受关注。

一些研究者们利用相位恢复算法(Phase Retrieve Algorithm, PRA)来进行光学加密。利用 PRA 可以为每幅图像生成不同的相位掩模,同时利用这些相位掩模可以进一步降低串扰噪声。1972 年,Gerchberg 和 Saxton 提出了一种可应用于显微成像的相位恢复算法,该算法被称为 GS 算法^[7]。在 2009 年,Hwang 等^[8]提出了一种结合 4F 系统和级联相位恢复算法(Cascaded Phase Retrieval algorithm, CPRA)的加密方法。这种方法通过其独特的结构,既提升了加密图像的容量,又有效消除了串扰噪声。2012 年,Zhao 和 Deng 提出了一种基于相位恢复的图像加密方法^[9],这种方法突破了以往加密系统中用户间相互依赖的局限,实现了几乎无限数量的图像在无串扰噪声的环境下的安全加密。哈尔滨工程大学的单明广等在 2021 年基于三维相位恢复算法提出了一种安全增强的级联相位编码方案,该方法不仅消除了传统加密系统的线性关系,而且密钥的安全性得到了提高^[10]。2023 年,Mehra 等提出了一种光学非对称指纹图像加密技术^[11]。该技术将指纹图像与 Gerchberg-Saxton 相位恢复算法生成的相位掩模相结合,并通过它生成不同的密钥。密钥的不对称使得系统

可以免受暴力破解、已知明文攻击和特殊攻击等攻击。然而,上述方法在实际交通场景应用中仍面临挑战:首先,交通监控系统采集的图像多为彩色(如车辆颜色、交通信号灯),而现有相位恢复加密方法大多针对灰度图像设计,适应性不足;其次,交通图像在传输中易受各类噪声(如传感器噪声、信道干扰)和局部遮挡(如树木遮挡摄像头)影响,而传统相位恢复方法的抗噪与抗遮挡能力有限。

为了扩大加密方法可作用对象的范围并提升鲁棒性,近年来,不少研究员将 QR 码引入图像预处理阶段。QR 码具有标准化、强纠错能力以及对输入内容(文本、链接、图像二进制流)格式无特定要求等优点,恰好能应对交通图像加密的前述挑战:将任意格式的交通图像编码为 QR 码,可统一处理尺度,摆脱对图像色彩模式的依赖;其内嵌的纠错机制能天然抵抗一定程度的噪声和污损,为后续加密过程提供了基础防护。并且鉴于 QR 码自身的抗噪性,加密方法的抗噪声攻击能力也有所提升。2014 年,Barrera 等提出了第一个使用 QR 码的加密技术^[12]。紧接着,Kumar 等在 2018 年提出了一种基于 QR 码的非线性图像加密方法^[13]。在 2020 年,Mustafa 等提出了基于 QR 码和混沌映射的虹膜图像加密方法,该方法的主要思想是利用卷积从 QR 码中提取特征用于密钥生成^[14]。2024 年,Allarakha 等使用 QR 码编码光束进行二进制图像加密^[15]。该加密方法中使用的加密光束仅包含有关对象的部分信息,从而阻止在没有适当密钥信息的情况下检索完整的信息。然而,这些基于 QR 码的加密方案多侧重于单幅图像或有限数量图像的加密,在需要同时加密海量交通监控视频流或图像序列时,其加密容量和处理效率仍显不足。

综上所述,现有研究在面向交通图像加密时,往往在“图像类型适应性”、“抗干扰鲁棒性”和“多图像加密容量”三者间难以兼顾。为了解决上述问题,本文提出一种基于 QR 码迭代相位恢复的光学加密算法,并用于交通图像加密中。该方法旨在结合 QR 码的格式通用性与强纠错能力,以及迭代相位恢复算法的多图像无串扰编码优势,从而构建一种更适用于复杂交通环境的、安全高效的图像加密解决方案。

1 算法描述

为了保障交通图像的安全传输,提出了基于 QR 码的迭代相位恢复光学加密算法。

1.1 加密过程

本算法设计基于QR码的容错机制与相位恢复算法的多重加密特性,通过两级密钥(二进制掩码与纯相位函数)实现信息的分层保护。QR码预处理不仅扩展了图像类型适应性,其固有的纠错能力也为后续相位调制提供了抗干扰基础。相位恢复模块则利用傅里叶域的能量集中特性,实现多图像无串扰编码,从而在理论上支持近乎无限的加密容量。该算法的加密过程如图1所示。

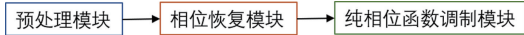


图1 算法加密过程框图

1.1.1 预处理模块

该加密方法首先将原始图像转换为QR码,这一步将图像的明文信息转化为易于处理的二进制格式。并且,该加密方法直接作用于QR码,这使得该方法在原始图像的色彩、形状和大小等方面没有使用限制。

在上述基础上,该方法生成一个随机的二进制明文掩码 E ,这个掩码作为第一个加密密钥。掩码 E 与QR码进行异或(Exclusive OR, XOR)运算,从而产生加密后的二进制数据。XOR运算不仅能提升加密方法的复杂性,还因为XOR运算具备可逆性和恒等性的特点保证了解的可行性。这一加密数据保证了原始图像信息的安全性,同时随机掩码还充当解密时所需的密钥。值得注意的是,相同的随机掩码可以加密多个QR码,从而创建一系列加密的二进制密文。由于每个加密的QR码都能够通过同一个解密密钥精确恢复,因此输入的随机二进制掩码极大地提升了系统的加密效率,能够安全地处理大量图像。此加密方案不仅高效,而且由于其二进制操作的本质,也易于计算机执行。

本文使用的随机二进制掩码 E 由下式定义

$$\begin{cases} E = \text{rand}(N, N) \\ E(E \geq 0.5) = 1 \\ E(E < 0.5) = 0 \end{cases} \quad (1)$$

式中 $\text{rand}()$ 表示随机分布矩阵; N 是随机分布矩阵的大小。公式表明矩阵中元素大于等于0.5时取值为1,小于0.5时取值为0。该矩阵在使用后需要记录并保存下来作为解密第二步的密钥。

用随机二进制掩码 E 与用 QR_n 表示的不同QR码进行异或运算,则可以生成多个二进制密文,表示为

$$f_n(x, y) = (E) \text{ xor } (QR_n) \quad (2)$$

式中, xor 表示XOR运算; $f_n(x, y)$ 表示不同的二进制密文。

1.1.2 相位恢复模块

在预处理模块之后,利用相位恢复模块将密文 $f(x, y)$ 编码为傅里叶域中的纯相位函数。

首先对 $f(x, y)$ 进行傅里叶变换,得到一个中间相函数 $\exp[j\varphi(u, v)]$ 。然后对 $\exp[j\varphi(u, v)]$ 进行傅里叶反变换,其振幅可以视为单位1,得到 $\hat{f}(x, y)$,相函数为 $\exp[j\theta(x, y)]$ 。然后用相函数 $\exp[j\theta(x, y)]$ 来更新算法输入的相位部分,得到的结果再一次进行傅里叶变换。重复上述过程,直到达到阈值,即相关系数达到一定程度或者迭代到一定次数。位于傅里叶平面收敛的相函数 $\exp[j\varphi(u, v)]$,作为对应于密文 $f(x, y)$ 的纯相位函数。编码过程其流程图如图2所示。

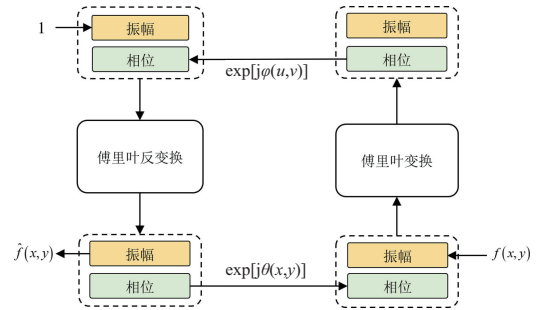


图2 相位恢复模块

在上述迭代相位恢复算法的帮助下,将每个单独的明文 $f_n(x, y)$ 编码为其相应的纯相位函数 $\exp[j\varphi_n(u, v)]$ 。也就是说,每个纯相位函数 $\exp[j\varphi_n(u, v)]$ 应满足以下表达式

$$FT^{-1}\{\exp[j\varphi_n(u, v)]\} = \hat{f}_n(x, y) \exp[j\theta_n(x, y)] \quad (3)$$

式中 $\exp[j\theta_n(x, y)]$ 是伴随的相位项。

1.1.3 纯相位函数调制模块

获得每个单独明文相应的纯相位函数(Phase-only Function, POF)后,在傅里叶平面上调制POF,从而获得最终的密文 $g(x, y)$ 。这里我们使用的纯相位掩码 $e_n(u, v)$ 作为第二个加密密钥,表示为

$$e_n(u, v) = \exp\left[j \sum_{k \neq n}^N \varphi_k(u, v)\right], (n, k) \in [1, N] \quad (4)$$

因此,调制后的结果可以表示为

$$G(u, v) = \exp\left[j \sum_{k=1}^N \varphi_k(u, v)\right] \quad (5)$$

通过对 $G(u, v)$ 进行傅里叶反变换,可以得到最终的密文 $g(x, y)$ 。

从式 (5) 可以看出, 每个要调制的纯相位函数 $\exp[j\varphi_n(u,v)]$ 与对应的加密密钥 $e_n(u,v)$ 相对于 $G(u,v)$ 来说是互补的, 即每个明文对应的最终密文是相同的, 并且包含了所有明文的加密信息。所有明文都可以从密文中提取出来, 没有任何串扰, 加密容量几乎是无限的。

纯相位函数调制过程如图 3 所示, 其中 FT^{-1} 表示傅里叶反变换, $\otimes$ 代表乘法运算。

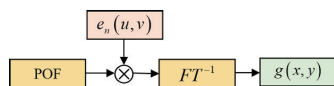


图 3 纯相位函数调制模块

1.2 解密过程

对接收方而言, 解密过程分为两个主要步骤。在第一步中, 必须逆转第二阶段的加密操作, 即纯相位函数调制模块。首先使用加密密钥 $e_n(u,v)$ 对应的解密密钥 $e_n^*(u,v)$, 让接收方从密文 $g(x,y)$ 中提取近似为 $f_n(x,y)$ 的 $\hat{f}_n(x,y)$, 再进行提取绝对值的操作。

整个解密第一步过程可以表示为

$$|\hat{f}_n(x,y)| = |FT^{-1}\{FT[g(x,y)]e_n^*(u,v)\}| \quad (6)$$

式中 FT^{-1} 和 FT 分别表示傅里叶反变换和傅里叶变换, 符号 $*$ 表示共轭运算。

在解密过程中, 未恢复的图像被解密密钥抵消, 当使用相应的解密密钥时, 可以从密文 $g(x,y)$ 中近似提取出所有明文, 而不会产生任何串扰。

解密第一步如图 4 所示, $\otimes$ 代表乘法运算。

虽然这一过程可能导致图像质量略有下降, 但关键在于它不会妨碍随后的 XOR 运算, 这是解密第一阶段密文所必需的。此外, 虽然加密过程是相互依赖的, 但解密过程是相互独立的, 任何明文的解密偏差都不会影响到其他明文。

在完成第一阶段的解密后, 将二进制密文 $\hat{f}_n$ 与最初加密时设置的随机二进制掩码 E 进行 XOR 运

算。这一步骤是解密流程的关键, 因为它利用了 XOR 运算的性质, 恢复出了原始的二维码图像, 从而使得接收方能够迅速而准确地访问到嵌入在 QR_n 码中的数据

$$QR_n = (E) \text{ xor } (\hat{f}_n) \quad (7)$$

最后直接扫描 QR 码能够直接得到高质量的恢复结果。

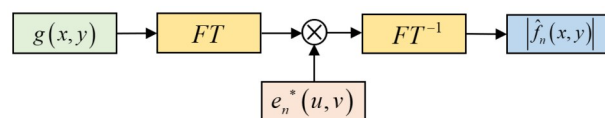


图 4 解密第一步

2 实验结果与分析

2.1 多图像无噪实验分析

该部分实验采用了 3 幅像素数为 1600×1200 的监控拍摄图像 (“Car1”、“Car2”、“Car3”) 作为要加密的原始图像, 仿真结果如图 5 所示。

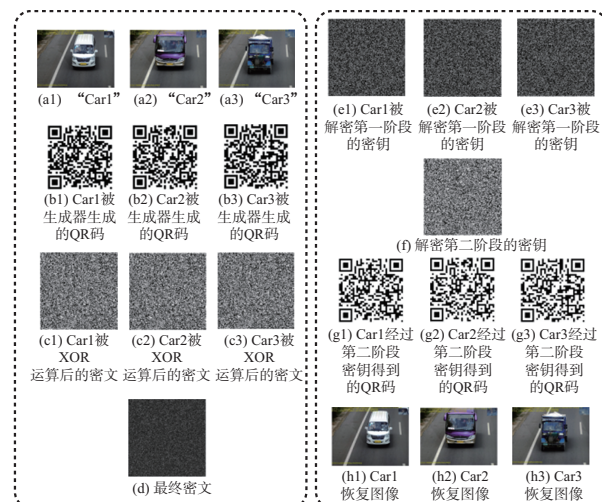


图 5 多图像无噪实验结果

选择相关系数 (Correlation coefficient, CC) 作为评估函数来定量评估解密的 QR 码的质量可以通过以下方式计算

$$CC = \frac{\left| \sum_{x=1}^M \sum_{y=1}^N [A(x,y) - \bar{A}] [B(x,y) - \bar{B}] \right|}{\sqrt{\left[\sum_{x=1}^M \sum_{y=1}^N (A(x,y) - \bar{A})^2 \right] \left[\sum_{x=1}^M \sum_{y=1}^N (B(x,y) - \bar{B})^2 \right]}} \quad (8)$$

式中, $A(x,y)$ 是解密的 QR 码第 x 行、第 y 列的灰度值, $B(x,y)$ 是原始 QR 码第 x 行、第 y 列的灰度值; $M \times N$ 是图像的分辨率; $\bar{A}$ 是解密图像的平均灰度值, $\bar{B}$ 是原始图像的平均灰度值。当解密的 QR 码和原始 QR 码之间的 CC 值越接近 1, 说明两码之间的相关性越强。

为定量评价解密图像的质量, 广泛采用的一个指标是峰值信噪比 (Peak Signal to Noise Ratio, PSNR)。对于大小为 $m \times n$ 的原始图像 I 和重建图像 R , 由式 (9) 先定义均方误差 (Mean Squared Error, MSE)

$$MSE = \frac{1}{m \times n} \sum_{i=1}^m \sum_{j=1}^n [R(i,j) - I(i,j)]^2 \quad (9)$$

PSNR 定义为

$$\text{PSNR} = 10 \log_{10} \left(\frac{(MAX - 1)^2}{MSE} \right) \quad (10)$$

式中，MAX 表示图像的最大像素值。一般认为：30~40dB 表明图像质量较好（有失真但可以接受），20~30dB 说明图像质量较差，低于 20dB 则不可接受。

表 1 解密得到的图像和原始图像之间的 CC 值

原始图像	CC 值
Car1	0.9971
Car2	0.9953
Car3	0.9955

表 2 解密得到的图像和原始图像之间的 PSNR 值

原始图像	PSNR 值
Car1	36.4156
Car2	36.2307
Car3	36.3441

图 5 (b1) - (b3) 展示了由 QR 码生成器制作的 QR 码。这些 QR 码接着与一个随机生成的二进制明文进行异或操作，该明文同样充当了解密第二阶段的密钥，并且可以由接收方提前传递给发送方。异或操作之后得到的图像分别为图 5 (c1) - (c3)。随后，这三幅经过异或运算后的图像分别经由迭代相位恢复算法进行加密处理，得到最终密文，如图 5 (d) 所示。图 5 (e1) - (e4) 是相位恢复加密步骤中产生的解密第一阶段的密钥。在实现第一阶段解密后，将得到的密文与解密第二阶段的密钥 5 (f) 进行异或操作，成功恢复出原始的 QR 码，具体如图 5 (g1) - (g3) 所示。图 5 (h1) - (h3) 分别是扫描恢复的 QR 码后得到的图像。从整个过程的结果来看，所有图像都被高质量恢复。

2.2 遮挡攻击实验分析

该部分实验为了验证加密方法的抗遮挡攻击性能，对密文在同一位置进行不同程度的裁剪，实验结果如图 6 所示。

结合图 6、表 3 和表 4 可以看出，随着密文遮挡面积的增加，解密得到的 QR 码清晰程度在逐步下降。当遮挡程度达到 20% 时，解密得到的 QR 码存在非常多的杂质，但是仍可扫描出 QR 码的信息，说明该方法能够较好地抵抗遮挡攻击。综上所述，本文提出的加密方法在抵御噪声攻击和遮挡攻击方面表现出良好的鲁棒性。

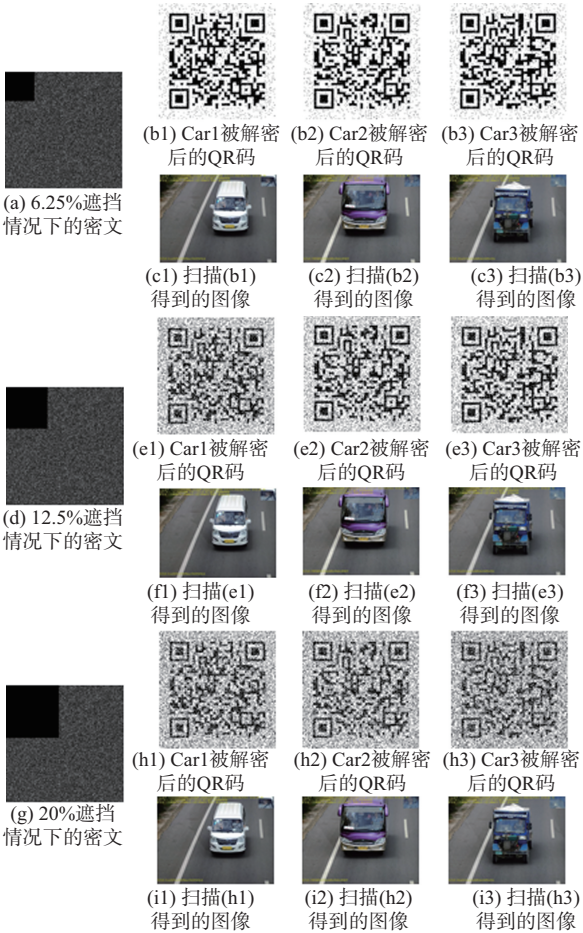


图 6 遮挡攻击实验结果

表 3 解密得到的图像和原始图像之间的 CC 值

原始图像	遮挡 6.25%	遮挡 12.5%	遮挡 20%
Car1	0.9971	0.9971	0.9971
Car2	0.9953	0.9953	0.9953
Car3	0.9955	0.9955	0.9955

表 4 解密得到的图像和原始图像之间的 PSNR 值

原始图像	遮挡 6.25%	遮挡 12.5%	遮挡 20%
Car1	36.4156	36.4156	36.4156
Car2	36.2307	36.2307	36.2307
Car3	36.3441	36.3441	36.3441

2.3 噪声攻击实验分析

在真实交通图像传输场景中，系统常受到各类低强度随机噪声（如传感器热噪声或信道扰动）的干扰，可能影响加密数据完整性。为验证算法在此类环境下的稳定性，模拟了不同波动程度的低强度高斯噪声攻击。采用了噪声强度恒定、标准差值不同的零均值高斯噪声，噪声强度为 1，标准差 σ_{noise} 分别为 0、0.1、0.5。以系统评估噪声波动对解密性能的影响。

被一定强度的零均值高斯噪声污染的密文可以表示为

$$C'(x,y)=C(x,y)[1+bG(x,y)] \quad (11)$$

式中， $C(x,y)$ 表示原始图像， $C'(x,y)$ 表示受污染图

像, $G(x,y)$ 表示零均值高斯噪声, b 表示噪声强度。
实验结果如图 7 所示。



图 7 噪声攻击实验结果

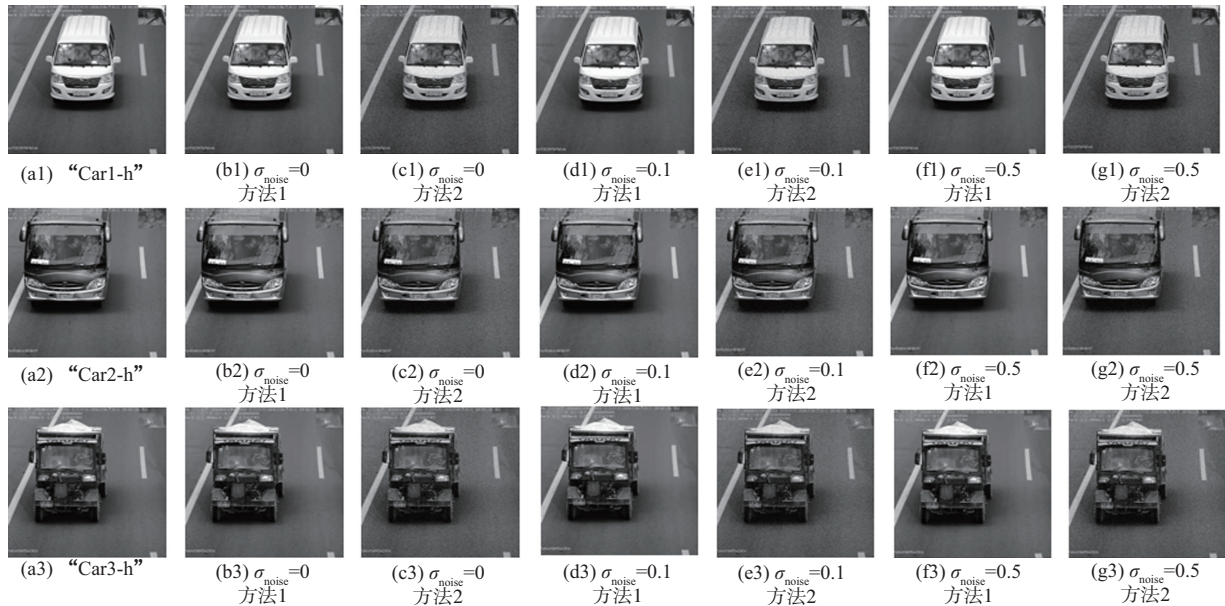


图 8 对比实验结果(不同 σ 不同方法恢复得到图像)

从图 7 可以看出, 即使在 $\sigma=0.5$ 的噪声干扰下, 解密恢复的 QR 码结构仍保持完整, 可被正确识别; 恢复图像在视觉上也与原始图像高度一致。定量数据(表 5-6)显示, 不同 σ 下解密图像的 CC 值均高于 0.995, PSNR 均大于 36 dB, 且数值稳定。这表明算法对低强度高斯噪声具有良好的鲁棒性, 其抗噪能力主要得益于 QR 码的强纠错能力和相位恢复过程对噪声的扩散效应。

表 5 解密得到的图像和原始图像之间的 CC 值

原始图像	$\sigma_{\text{noise}} = 0$	$\sigma_{\text{noise}} = 0.1$	$\sigma_{\text{noise}} = 0.5$
Car1	0.9971	0.9971	0.9971
Car2	0.9953	0.9953	0.9953
Car3	0.9955	0.9955	0.9955

表 6 解密得到的图像和原始图像之间的 PSNR 值

原始图像	$\sigma_{\text{noise}} = 0$	$\sigma_{\text{noise}} = 0.1$	$\sigma_{\text{noise}} = 0.5$
Car1	36.4156	36.4156	36.4156
Car2	36.2307	36.2307	36.2307
Car3	36.3441	36.3441	36.3441

为了进一步体现本文方法的抗噪能力, 将该方法和基于相位检索互调的多图像加密方法^[5]进行对比。由于该方法作用对象的局限性, 将“Car1”、“Car2”、“Car3”转换成 3 幅像素数为 256×256 的灰度图 (“Car1-h”、“Car2-h”、“Car3-h”) 作为要加密的原始图像, 采用的零均值高斯噪声强度为 1, 标准差 σ_{noise} 分别为 0、0.1、0.5。实验结果如图 8, 表 7、8 所示。其中方法 1 用来代指本文所提算法, 方法 2 代指基于相位检索互调的多图像加密方法^[5]。

由表 7 可知, 本文所提方法恢复得出的图像质量与原始图像之间的 CC 值高于基于相位检索互调

的多图像加密方法^[5]。由表8可知,本文所提方法恢复得出的图像质量与原始图像之间的PSNR值体现出恢复得出的图像质量很高,基于相位检索互调的多图像加密方法^[5]恢复得出的图像质量与原始图像之间的PSNR值低于可接受阈值。由此可见,本文所提方法的抗噪性能强于使用相位检索互调的多图像加密方法^[5]。

表7 两种方法解密分别得到的图像和原始图像之间的CC值

原始图像(方法)	$\sigma_{\text{noise}} = 0$	$\sigma_{\text{noise}} = 0.1$	$\sigma_{\text{noise}} = 0.5$
Car1-h(方法1)	0.9979	0.9979	0.9979
Car1-h(方法2)	0.9866	0.9866	0.9866
Car2-h(方法1)	0.9962	0.9962	0.9962
Car2-h(方法2)	0.9814	0.9812	0.9810
Car3-h(方法1)	0.9965	0.9965	0.9965
Car3-h(方法2)	0.9828	0.9825	0.9825

表8 两种方法解密分别得到的图像和原始图像之间的PSNR值

原始图像(方法)	$\sigma_{\text{noise}} = 0$	$\sigma_{\text{noise}} = 0.1$	$\sigma_{\text{noise}} = 0.5$
Car1-h(方法1)	37.5278	37.5278	37.5278
Car1-h(方法2)	7.6529	7.9674	10.4636
Car2-h(方法1)	37.3133	37.3133	37.3133
Car2-h(方法2)	8.0971	8.5079	11.6316
Car3-h(方法1)	37.3969	37.3969	37.3969
Car3-h(方法2)	8.1367	8.5465	11.5492

3 结 论

为了更好地保护智能交通系统中的图像数据免受黑客的攻击,本文提出了一种基于QR码和迭代相位恢复的多图像加密方法,并运用在交通上。此方法先采用QR码和随机二进制明文进行XOR操作,生成二进制解密密钥和多个密文,利用迭代相位恢复算法将这些密文编码为POF,这些POF相互作为加密密钥调制成最终密文。最后通过逆向操作得到和原始明文一样的图像。本文通过一系列实验证明所提的加密方法抗噪性能优于使用相位检索互调的多图像加密方法^[5],在抵御噪声攻击和遮挡攻击方面表现出良好的鲁棒性。

本文提出的加密方法兼顾了QR码的广泛适用性以及相位检索互调作用下容量无限的优点。此外,在预处理上添加的异或(Exclusive OR, XOR)运算提升了加密方法的复杂性,并且XOR运算具备的可逆性和恒等性保证了解密的可行性。该方法不仅能实现多图像加密高质量恢复,对于常见的光学和计算攻击还表现出了一定的防御能力。

参考文献:

- [1] Shuai Ling, Shurui Jin, Qing Wang, et al. Can smart transportation reduce carbon emission intensity? -an empirical study from macro and micro perspectives in china[J]. Journal of Management Science and Engineering, 2024, 9(4): 490—509.
- [2] Singh A K, Pamula R, Akhter N, et al. Intelligent transportation system for automated medical services during pandemic[J]. Future Generation Computer Systems, 2024, 163: 107515.
- [3] Mrudula S T, Ritonga M, Sivakumar S, et al. Internet of things and optimized knn based intelligent transportation system for traffic flow prediction in smart cities[J]. Measurement: Sensors, 2024, 35: 101297.
- [4] Driessen T, Dodou D, Basilinskyy P, et al. Putting ChatGPT vision (GPT-4V) to the test: risk perception in traffic images [J]. Royal Society Open Science, 2024, 11(5): 231676.
- [5] Tong X, Liu X, Zhang M, et al. A high-quality visual image encryption algorithm utilizing the conservative chaotic system and adaptive embedding[J]. Chaos, Solitons & Fractals, 2024, 188: 115581.
- [6] Guang Y, Ding Q. Dynamics analysis of a novel parametrically controllable symmetric multi-scroll chaotic system and FPGA design of an image encryption system[J]. Chaos, Solitons & Fractals, 2024, 188: 115572.
- [7] Gerchberg R. A practical algorithm for the determination of phase from image and diffraction plane pictures[J]. Optik, 1972, 35: 237.
- [8] Hwang H E, Chang H T, Lie W N. Multiple-image encryption and multiplexing using a modified Gerchberg-Saxton algorithm and phase modulation in Fresnel-transform domain[J]. Optics Letters, 2009, 34(24): 3917—3919.
- [9] Deng X, Zhao D. Multiple-image encryption using phase retrieval algorithm and intermodulation in Fourier domain[J]. Optics & Laser Technology, 2012, 44(2): 374—377.
- [10] Shan M, Liu L, Liu B, et al. Security enhanced cascaded phase encoding based on a 3D phase retrieval algorithm[J]. Optics and Lasers in Engineering, 2021, 145: 106662.
- [11] Mehra I, Nishchal N K. Fingerprint image encryption using phase retrieval algorithm in gyrator wavelet transform domain using QR decomposition[J]. Optics Communications, 2023, 533: 129265.
- [12] Barrera J F, Vélez A, Torroba R. Experimental scrambling and noise reduction applied to the optical encryption of QR codes[J]. Optics Express, 2014, 22(17): 20268—20277.
- [13] Kumar R, Bhaduri B, Hennelly B. QR code-based non-linear image encryption using Shearlet transform and spiral phase transform[J]. Journal of Modern Optics, 2018, 65(3): 321—330.
- [14] Mustafa R A, Maryoosh A A, George D N, et al. Iris images encryption based on QR code and chaotic map[J]. Telecommunication Computing Electronics and Control, 2020, 18(1): 289—300.
- [15] Shikder A, Rao S K, Kumar P, et al. Binary image encryption with a QR code-encoded optical beam having an array of vortices[J]. JOSA A, 2024, 41(3): A73—A82.