文章编号：2095-2163(2024)01-0162-06 中图分类号：TP309.7 文献标志码：A

基于 QR 码和信息隐藏的秘密图像安全分享方案

刘鑫淇，王洪君，孙 蕾
（吉林师范大学 数学与计算机学院，吉林 四平 136000）

摘 要：随着数字化时代的到来，防止数据和信息的泄露问题是现如今持久关注的问题。在视觉密码加密过程中，人们侧重于原始秘密信息的保护，而忽视了对共享份保护以及信息传输过程中发送者与参与者的验证。因此，本文在 (k,n) 像素不扩展的视觉密码方案下，基于 QR 码的纠错容错功能，对现存的隐藏方法进行改进，提出了一种保护秘密共享份的安全分享方案。针对 QR 码在重要信息的传输时，易被窃取者任意读取篡改这一现实问题，利用 RSA 非对称加密算法对 QR 码的发送传输进行验证保护。实验结果表明，本文方案减少了共享份在加密和发送过程中受到的攻击性，实现了对发送者和参与者的验证，保证了 QR 码编码内容的真实性和传播过程中的可靠性。

关键词：QR 码；信息隐藏；视觉密码；RSA 算法

A secret image-sharing scheme based on QR code and steganography

LIU Xinqi, WANG Hongjun, SUN Lei
(College of Mathematics and Computer Science, Jilin Normal University, Siping Jilin 136000, China)

Abstract: With the advent of the digital era, the problem of preventing data and information leakage is an enduring concern nowadays. In the visual cipher encryption process, people focus on the protection of the original secret information, while neglecting the protection of the shared copy and the verification of the sender and the participants in the information transmission process. Therefore, in this paper, we propose a secure sharing scheme to protect the secret shared copies under the (k,n) - pixel unexpanded visual cipher scheme, based on the error-correction and fault-tolerance function of QR codes, and improving the existing hiding methods. Aiming at the real problem that QR codes are easy to be read and tampered arbitrarily by eavesdroppers during the transmission of important information, the RSA asymmetric encryption algorithm is utilized to verify and protect the sending transmission of QR codes. The experimental results show that the scheme in this paper reduces the aggressiveness of the shared share in the encryption and sending process, realizes the verification of the sender and the participants, and ensures the authenticity of the encoded content of the QR code and the reliability of the transmission process.

Key words: QR code; steganography; visual cryptography; RSA algorithm

0 引 言

数字化时代给文本和图像内容的产生和发展创造了便捷，但与此同时防止信息的窃取、盗用和错误传播变得尤为重要。信息隐藏能够将秘密信息嵌入在透明的载体中，来传递秘密信息和保证数据完整性[1]。主要是载体图像中隐藏的秘密信息不被篡改或删除，从而在必要时提供有效证明信息。

快速响应码（Quick Response code，QR）是由日本 Denso 公司研制的一种二维条码[2]。QR 码作为信息存储和传递的重要技术载体，在许多领域都起着至关重要的作用，具有便携、信息密度大等特点，广泛应用于身份验证和物流行业等诸多领域[3]。但是，传统的 QR 码存在易于被攻击者篡改，盗取信息的缺点，具有安全隐患。

针对上述问题，学者们对 QR 码与信息隐藏相结合加密方式的研究已成为当前的研究热点。Zhang[4] 等人提出了一种基于像素对平均预测的可逆信息隐藏算法，将 QR 码作为可见水印载到载体图像选定位置上进行传递；LIN[5] 等人提出使用信息隐藏方法，依据秘密长短来改变隐藏块数量，但该方法存在大量的矩阵运算，计算复杂度高；Wang[6] 等人基于 QR 码模块和编码区域，对秘密信息进行 LSB 空间域信息隐藏；Zheng[7] 等人通过密钥直接得

作者简介：刘鑫淇（1999-），女，硕士研究生，主要研究方向：信息安全、密码学、视觉密码。
通讯作者：王洪君（1965-），男，博士，教授，硕士生导师，主要研究方向：密码学、信息安全、网络体系结构。Email：jlnuwhj@ sina.com

收稿日期：2023-01-11

到位置信息序列，再通过得到的序列直接嵌入秘密信息，算法中主要依赖随机位置序列；M. Alajmi[8] 等人提出了一种利用容器隐藏有效载荷的隐写系统，它不仅可以隐藏有效载荷，而且还可以给攻击者提供误导信息。该系统生成的 QR 码除了可以携带有效载荷外，还可以携带普通信息。RJ Mstafa[9] 等人提出一种基于离散小波变换（DWT）和快速响应码的可逆视频隐写解决方案，为了提高所提方法的安全级别，提出了一种增强的 ElGamal 密码系统。Fauzia Yasmeen[10] 等人提出一种算法，在 NSCT 域中应用了 QR 分解和奇异值分解（SVD）。该算法首先使用 Arnold 变换对秘密图像进行加扰，将载波和加扰的隐藏图像分解为系数子带；其次，将 QR 分解和 SVD 分别用于载波和加扰秘密图像的特定系数；最后，将修改后的秘密镜像插入到载波镜像中进行通信。

综上分析研究，本文在前人 QR 码与信息隐藏相结合的方案基础上，对信息隐藏方法进行改进，提出了一种对视觉密码加密生成的共享份的保护方案。同时由于 QR 码在扫描内容时是公开透明的，传递的重要信息容易被任意读取，采用非对称加密方法，对 QR 码自身进行加密，并将加密后的信息进行数字签名验证。该方案既保证 QR 码信息的真实性和完整性，又减少了攻击者对视觉密码产生的无意义共享份的注意，避免其进行攻击。

1　相关知识

1.1　视觉密码方案

视觉密码（Visual Cryptography Scheme，VCS）由 Naor 和 Shamir 于 1994 年提出。在 (k,n) 视觉密码方案中，将秘密图像加密成 n 张共享份，只有大于或等于 k 张共享份参与才能够将其解密，小于 k 张共享份不会显现出任何秘密信息[11]。按照加密方式的不同，视觉密码可以划分为确定型、概率型和随机网格视觉密码[12]。本文采用像素不扩展的基于随机网格的视觉图像秘密共享方案，将一幅秘密的二值图像加密成两个随机颜色的网格[13]。每个网格的平均透光率为 0.5。像素不扩展 VCS 方案的加密规则见表 1。

使用像素不扩展的（2,2）视觉密码方案得出的实验结果如图 1 所示。将原图像进行加密得到 2 个无意义的共享份，从任一共享份中无法得到秘密信息，只有将两个共享份叠加才能得到秘密图像。

表 1　像素不扩展 VCS 方案加密规则

Table 1　Encryption rules of the VCS scheme without pixel extension

秘密像素	共享份 1	共享份 2	叠加结果
□	□	□	□
	■	■	□
■	□	■	■
	■	□	■

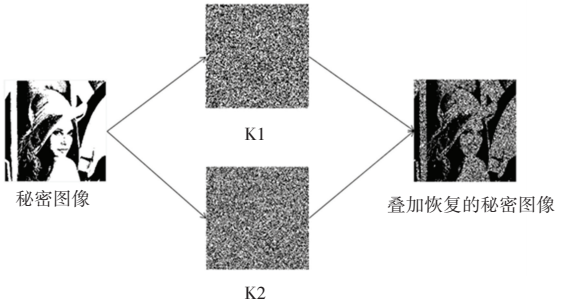

图 1　（2,2）—VCS 实验结果

Fig. 1　（2,2）-Results of the VCS experiment

1.2　QR 码理论基础

QR 码属于矩阵式二维码[14-15]的一种，每个 QR 码可以分为功能区和编码区两部分。功能区由定位标志、定时标志和校正标志组成，3 个回字形的定位标志用于确定 QR 码的正确方向。QR 码版本的不同，决定校正标志的不同，会出现一个或者多个标志模块。定时标志则是黑白模块相间的部分，用于进一步网格化校验。编码区包含版本信息、格式信息和数据及纠错容错密钥。图 2 为 QR 码版本 7 的结构图。

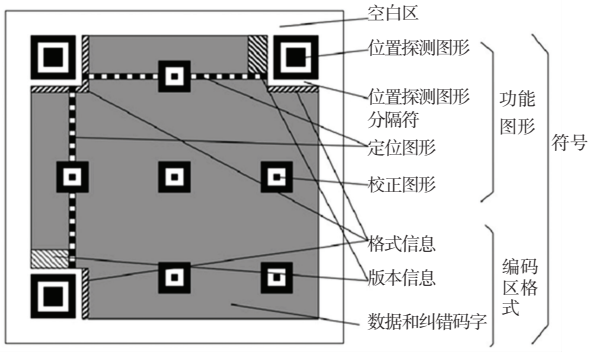

图 2　QR 码结构图

Fig. 2　QR code structure diagram

QR 码有 40 个版本，版本大小决定容量大小。版本 1 由 21×21 个模块组成，目前最高版本的模块数达到 177×177 个[16]。生成 QR 码图像时，需要根据实际的嵌入数据来选择不同的版本号。

QR 码有 4 个不同的纠错等级。表 2 为 QR 码纠错等级表。

表 2 QR 码纠错等级表

Table 2 QR code error correction grade table

QR 码纠错等级	
L(Low)	7%的字码可被修正
M(Medium)	15%的字码可被修正
Q(Quartile)	25%的字码可被修正
H(High)	30%的字码可被修正

1.3 信息隐藏方案

信息隐藏又称隐写术,通过透明载体传输秘密,展现的是内容和传输过程的隐蔽性。信息隐藏的基本框架模型如图 3 所示,主要包括嵌入和提取两部分。其中,秘密信息是在发送过程中需要保密的信息,只有指定的接收方才可以获取其内容;载体信息是在公开透明的信道传播的信息,是可被任意第三方查看的;信息隐藏一般都会带有密钥,用于确定嵌入位置;嵌入算法和提取算法用于秘密信息的隐藏和提取。

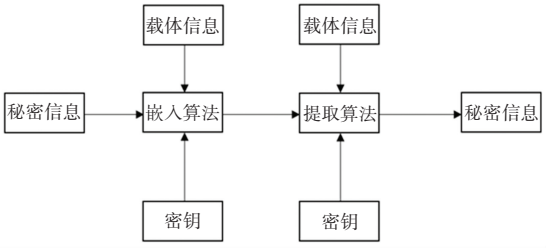

图 3 信息隐藏基本框架结构

Fig. 3 The basic framework of steganography

本文使用一种改进的直接 4 bit 法来隐藏信息。算法原理为载体图像低 4 位改为秘密图像高 4 位,优势在于隐藏秘密信息的容量非常大。由于人眼对于 RGB 的敏感性各不相同,绿色敏感性最大,红色次之,蓝色最小,所以改进方案将 4 bit 进行分块,嵌入在载体的 R 层和 B 层,即秘密图像较高的 2 bit 隐藏在 R 层中,另外 2 bit 隐藏在 B 层中。传统隐藏方案仅在其一层嵌入,像素色彩沿着某一坐标方向变化,而改进后像素色彩在 RGB 空间整体偏移。这样前、后颜色坐标点之间的间距在一个分量上改变较小,对载体图像的影响会更少。

1.4 基于 QR 码和信息隐藏的视觉密码方案

针对视觉密码方案生成的无意义噪声图像容易受到攻击者注意,QR 码在传输过程中容易被复制和篡改,以及无法验证发送者真伪等问题,提出了一种将生成的秘密共享份嵌入到 QR 码中的安全方案。在发送过程中,使用 RSA 加密和数字签名算法来解决以上问题。方案流程如图 4 所示。

使用像素不扩展的(3,3)-VCS 方案对秘密图像进行加密,生成 3 张与秘密图像大小相同的无意义共享份。由于 QR 码自身具有容错和纠错功能,将共享份通过双线性插值法进行缩小,分别嵌入到 3 个 QR 码的中心容错区域部分,最后通过矩阵赋值生成载有秘密信息的 3 个 QR 码。载有秘密共享份的 QR 码和原秘密图像相比,人眼几乎看不出任何差别。

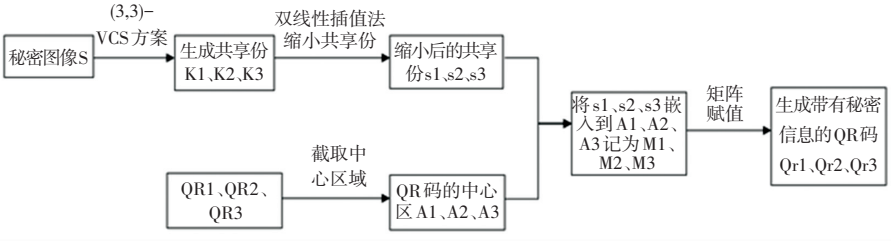

图 4 方案示意图

Fig. 4 Schematic of the scheme

2 RSA 非对称加密算法

RSA 是传统非对称加密算法的一种,是由 RIRivest 等人[17-18]于 1977 年在 MIT 上提出的,具有良好的安全性。RSA 算法是用于数字加密和数字签名的算法,主要包括素数的生成、密钥的生成、明文和密文[19-20]。用于上述信息隐藏后,在避免 QR 码传输过程被攻击者攻击的同时,保证了共享份的完整性和真实性。

2.1 RSA 加密算法

2.1.1 密钥的产生

(1)生成两个随机素数 p 和 q,并且满足 $p \neq q$;

(2)计算 $n = p * q$,欧拉方程:$\varphi(n) = (p - 1) * (q - 1)$;

(3)随机生成正整数 e,满足 $1 < e < \varphi(n)$,且 e 与 $\varphi(n)$ 互质;

(4)计算 e 对于 $\varphi(n)$ 的模反元素 d,得到 $d \equiv e^{-1} \bmod(n)$;

(5)得到密钥对:公钥为(e,n),私钥为(d,n)。

2.1.2 加密

计算公式为

$$C = M^e \bmod(n) \tag{1}$$

式中:C 为传送的密文,M 为需要加密的明文或信

息，(e,n) 为公钥对。

2.1.3　解密

计算公式为

$$M = C^d \bmod (n) \tag{2}$$

式中：M 为解密的数据，C 为传送的密文，(d,n) 为私钥对。

2.2　RSA 数字签名算法

传统的 RSA 数字签名存在攻击者可以任意伪造信息，加密长文件时存在算法效率低等缺点。本文采用的 RSA 算法利用单项函数，先使用 Hash 函数对签名消息做 Hash 变换，得到报文摘要，再对变换后的消息进行数字签名。数字签名验证过程如图 5 所示。

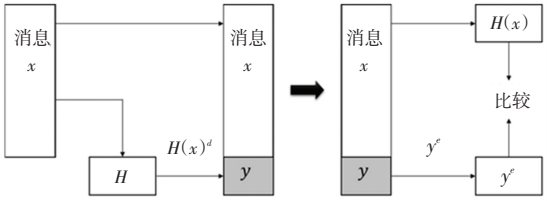

图 5　数字签名验证过程

Fig. 5　Digital signature verification process

2.2.1　签名过程

用户 A 对消息 X 进行签名，计算公式为

$$S = Sig(H(X)) = H(X)^d \bmod n \tag{3}$$

将 S 作为用户 A 对消息 X 的数字签名与消息 X 共同发送给用户 B。式中 $H(X)$ 表示对消息使用 Hash 算法，Hash 函数可以抵御伪造的攻击。

2.2.2　验证过程

用户 B 验证用户 A 对消息 X 的数字签名 S，计算公式为

$$H(X)' = S^e \bmod n \tag{4}$$

判断报文摘要 $H(X)$ 与 $H(X)'$ 是否相等，若二者相等，则可以证明签名 S 的确来源于用户 A；否则签名 S 有可能是被伪造的。同时，参与者再对接收到的消息 M 使用哈希函数算法，将得到的结果与上一步得到的报文摘要进行对比，如果两者一致则证明消息从未被修改过。

3　实验结果

本文以 (3,3)－VCS 密码方案对本方案进行验证，相关测试用图见表 3。

表 3　相关测试图例

Table 3　Related test legends

序号	QR 码	QR 码的扫描结果	双线性插值法缩小的共享份	截取 QR 码的中心区域
1				
2				
3				

按照上述改进后的直接 4 bit 法信息隐藏方法，利用 QR 码自身具有的容错和纠错功能，将双线性插值法缩小的共享份嵌入到 QR 码的中心区域中，人眼几乎无法察觉到 QR 码的变化，即使 QR 码受到攻击，攻击者首先会对 QR 码的校正、定位模块等区域进行攻击，保证共享份的安全。秘密共享份被安全隐藏后，发送方将 3 张 QR 码分别使用 RSA 得到加密后的 QR 码密文，再将密文进行 RSA 数字签名，保证 QR 码的真实性和有效传输。参与者在接收到密文和签名后，首先使用 RSA 数字签名验证算法，利用 Hash 函数对比，确保秘密传输方为发送者，并且在传输过程中信息没有被篡改，再对得到的 QR 码密文进行解密，最终得到载有秘密共享份的 QR 码图像，如图 6 所示。

结果显示，共享份嵌入到 QR 码后，QR 码可以被准确扫描，前后扫描结果一致，并且解密后的共享份可以完整的恢复出秘密图像。

(a) 秘密图像S (b) 带有隐藏信息的QR1 (c) 带有隐藏信息的QR2 (d) 带有隐藏信息的QR3

(e) QR1扫描结果 (f) QR2扫描结果 (g) QR3扫描结果 (h) 共享份T1⊕共享份T2

(i) 共享份T1 (j) 共享份T2 (k) 共享份T3 (l) 恢复图像

图 6 实验结果

Fig. 6 Experimental results

为验证本文方案的有效性,通过与其它相关方案进行计算复杂度、是否具有验证能力、是否抵抗恶意篡改以及嵌入容量等 4 个方面比较。以版本号 4 与纠错等级 H 的 QR 码作为载体, h 为 QR 码中的总块数; E 表示纠错码的数量,每 2 个纠错码可以纠正 1 个数据,所以纠错冗余为 $\lfloor E/2 \rfloor$, 比较结果见表 4。

表 4 相关方案比较

Table 4 Comparison of related schemes

方案	计算复杂度	是否具有验证能力	是否抵抗恶意篡改	嵌入容量
文献[6]	中	是	否	小于 $h \times \lfloor E/2 \rfloor$ bits
文献[21]	高	否	否	$h \times \lfloor E/2 \rfloor$ bits
文献[22]	高	否	否	$8 \times R - \sum_{j=1}^{m} (4 + B_j + C) - D$ bits
本文方案	低	是	是	$w \times h \times \lfloor E/2 \rfloor$ bits

由表 4 可见,文献[7]中为了实现验证能力,需要将一部分嵌入容量进行分配,所以实际容量小于 $h \times \lfloor E/2 \rfloor$;文献[22] 的秘密信息嵌入到补齐区域中,为了使版本号与信息相匹配,减少被攻击性,实际最大嵌入量为 $8 \times R - \sum_{j=1}^{m} (4 + B_j + C) - D$ bits ;本文方案以 QR 码的纠错容错功能为载体,直接利用 QR 码的纠错和容错块的数量,秘密的长短并不影响安全性,由于本文生成的秘密份额使用双线性插值法变换为 $1/w$ 实现嵌入,所以本文方案的嵌入容量为 $w \times h \times \lfloor E/2 \rfloor$ bits。同时 RSA 数字加密和数字签名算法,可以有效预防 QR 码遭受恶意破坏和篡改,解决了隐藏信息后的 QR 码无法被识别及发送者身份无法辨认等问题。

4 结束语

本文在像素不扩展的 (k,n) 视觉密码方案下,提出了一种基于 QR 码的纠错和容错功能与改进后的信息隐藏方案的秘密图像安全分享方案。本文在传输过程中,利用 RSA 的非对称加密算法进行加密和数字签名验证,有效的保证了载有秘密共享份的 QR 码在传输过程中不被任意读取、篡改等,减少攻击者的注意可能性,同时又保证了信息发送和接收双方的真实性和有效性,提高了参与者接受信息的安全性。

根据对现存方案的分析验证,后续工作将针对验证能力弱等缺点进行改进和创新,进一步提升方案的可靠性。

参考文献

[1] 徐明杰,杨婉霞,周蓓蓓,等. 文本信息隐藏技术分析与综述[J]. 软件导刊,2022,21(8):213-220.

[2] LIU T, YAN B, PAN J S. Color visual secret sharing for QR code with perfect module reconstruction[J]. Applied Sciences, 2019, 9(21): 4670.

[3] 燕雨薇,余粟. 二维码技术及其应用综述[J]. 智能计算机与应用,2019,9(5):194-197.

[4] 章佳佳. 结合 QR 码应用的可逆信息隐藏技术研究[D]. 合肥:合肥工业大学,2014.

[5] LIN P Y. Distributed secret sharing approach with cheater prevention based on QR code[J]. IEEE Transactions on Industrial Informatics,2016,12(1):384-392.

[6] 王斯琴. 结合 QR 码应用的多信息隐藏技术研究[D]. 南昌:南昌大学,2017.

[7] 郑东,杨舜同,赵庆兰. 基于 QR 码低复杂度信息隐藏方案[J]. 西安邮电大学学报,2019,24(3):64-70.

[8] ALAJMI M, ELASHRY I, EL-SAYED H S, et al. Steganography of encrypted messages inside valid QR codes[J]. IEEE Access, 2020, 8: 27861-27873.

[9] MSTAFA R. Reversible video steganography using quick response codes and modified elgamal cryptosystem [J]. Computers, Materials and Continua, CMC, 2022, 72(2):000.

[10] YASMEEN F, UDDIN M S. An efficient image steganography approach based on QR factorization and singular value decomposition in non-subsampled contourlet transform domain [J]. Security and Privacy, 2022, 5(4): e229.

[11] 郭松鸽,吕东辉,戴玉静,等. 基于异或解密的(k,n)视觉密码方案[J]. 上海大学学报(自然科学版),2020,26(1):21-32.

[12] 赵永康. 两类视觉密码方案的研究[D]. 天津:南开大学,2022.

[13] KAFRI O, KEREN E. Encryption of pictures and shapes by random grids[J]. Optics Letters, 1987,12(6):377-379.

[14] 燕雨薇,余粟. 二维码技术及其应用综述[J]. 智能计算机与应用,2019,9(5):194-197.

[15] 张兴华. 矩阵式快速 QR 码的研究和应用[D]. 成都:电子科技大学,2009.

[16] 俞吉儿. QR 码的安全认证研究及应用[D]. 杭州:杭州电子科技大学,2019.

[17] 刘孟栋. 数据加密技术在计算机网络安全中的应用价值评价[J]. 现代工业经济和信息化,2022,12(9):82-84.

[18] 赵杰峰. 基于 RSA 算法的网络信息加密方法[J]. 电脑知识与技术,2022,18(10):38-39.

[19] 杨雨,宋可鑫,王宇涵,等. RSA 加密算法和 DES 加密算法的论述及改进[J]. 海峡科技与产业,2022,35(1):78-82.

[20] 张键红,肖晗,王继林. 高效的基于身份 RSA 多重数字签名[J]. 小型微型计算机系统,2018,39(9):1978-1981.

[21] CHOW Y W, SUSILO W, YANG G, et al. Exploiting the error correction mechanism in QR codes for secret sharing [C]// Information Security and Privacy: 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part I 21. Springer International Publishing, 2016: 409-425.

[22] TAN L, LU Y, YAN X, et al. XOR-ed visual secret sharing scheme with robust and meaningful shadows based on QR codes [J]. Multimedia Tools and Applications, 2020, 79: 5719-5741.

(上接第 161 页)

[2] CAI X, GIALLORENZO M, SARABANDI K. Machine learning-based target classification for MMW radar in autonomous driving [J]. IEEE Transactions on Intelligent Vehicles, 2021, 6(4): 678-689.

[3] HE J, TERASHIMA S, YAMADA H, et al. Diffraction signal-based human recognition in non-line-of-sight (NLOS) situation for millimeter wave radar[J]. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 2021, 14: 4370-4380.

[4] MEIER D, ZECH C, BAUMANN B, et al. Millimeter-wave radar sensor for automated tomographic imaging of composite materials in a manufacturing environment [J]. IEEE Sensors Letters, 2021, 5(3): 1-4.

[5] FÖLSTER F, ROHLING H. Signal processing structure for automotive radar[J]. Frequenz, 2006, 60(1-2): 20-24.

[6] VENON A, DUPUIS Y, VASSEUR P, et al. Millimeter wave FMCW radars for perception, recognition and localization in automotive applications: A survey [J]. IEEE Transactions on Intelligent Vehicles, 2022, 7(3): 533-555.

[7] ESTER M, KRIEGEL H P, SANDER J, et al. A density-based algorithm for discovering clusters in large spatial databases with noise[C]//kdd. 1996, 96(34): 226-231.

[8] SUN D, LI B, QIAN Z. Research of vehicle counting based on DBSCAN in video analysis [C]//2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing. IEEE, 2013: 1523-1527.

[9] LIM S, LEE S, KIM S C. Clustering of detected targets using DBSCAN in automotive radar systems [C]//2018 19th international radar symposium (IRS). IEEE, 2018: 1-7.

[10] WAGNER T, FEGER R, STELZER A. Modification of DBSCAN and application to range/Doppler/DoA measurements for pedestrian recognition with an automotive radar system[C]//2015 European Radar Conference (EuRAD). IEEE, 2015: 269-272.

[11] 郑晶月, 吴佩仑, 陈家辉,等. 车载毫米波雷达多径假目标分析与消除方法[J/OL]. 系统工程与技术:1-11[2023-05-26]. http://kns.cnki.net/kcms/detail/11.2422.TN.20230111.0727.004.html.

[12] ESTER M, KRIEGEL H P, SANDER J, et al. A density-based algorithm for discovering clusters in large spatial databases with noise[C]//kdd. 1996, 96(34): 226-231.