基于机器学习的犯罪预测研究进展

张耀峰[1,2,3]，姚金伶[2,4*]，徐 旭[1,3]，王 睿[1,2]

[1]湖北经济学院新财经交叉学科研究院 湖北武汉
[2]湖北经济学院湖北数字政府建设研究中心 湖北武汉
[3]湖北经济学院湖北数据与分析中心 湖北武汉
[4]湖北经济学院金融学院 湖北武汉

【摘要】犯罪预测是预防犯罪的一项技术方法。近年来，随着大数据技术和人工智能的兴起，机器学习方法被引入到犯罪预测的研究中，取得了丰富的研究成果。本文系统梳理了基于机器学习的犯罪预测研究进展，从环境犯罪学理论出发总结了犯罪预测的理论基础与方法演进，阐述了机器学习模型在犯罪预测中的主要技术路径。研究从预测对象和预测场景两个维度，重点分析了机器学习方法在犯罪趋势预测、犯罪热点预测、犯罪时空预测、犯罪类型识别以及犯罪嫌疑人预测及其落脚点预测等方面的应用，并归纳其在侵财、凶杀、金融及网络犯罪等典型领域的研究成果。结果表明，机器学习方法能够有效提升犯罪预测的准确性与实时性，为社会治安防控提供新思路。然而，当前研究仍面临数据稀疏性、时空相关性处理、区域划分合理性、模型可解释性、预测效果评价、伦理与隐私保护等方面的挑战。

【关键词】机器学习；犯罪预测；时空预测；犯罪场景
【基金项目】国家社科基金重点项目，项目编号 23ATJ005
【收稿日期】2025 年 9 月 19 日 【出刊日期】2025 年 10 月 13 日 【DOI】10.12208/j.sdr.20250235

Research progress of crime prediction based on machine learning

Yaofeng Zhang[1,2,3], Jinling Yao[2,4], Xu Xu[1,3], Rui Wang[1,2]*

[1]Interdisciplinary Research Institute in New Finance and Economics, Hubei University of Economics, Wuhan, Hubei
[2]Hubei Research Center for Digital Government Construction, Hubei University of Economics, Wuhan, Hubei
[3]Hubei Centre for Data and Analysis, Hubei University of Economics, Wuhan, Hubei
[4]School of Finance, Hubei University of Economics, Wuhan, Hubei

【**Abstract**】Crime prediction serves as a technical approach to crime prevention. In recent years, with the rapid development of big data and artificial intelligence, machine learning methods have been increasingly applied to crime prediction, yielding substantial research progress. This paper provides a systematic review of research advancements in crime prediction based on machine learning. Grounded in environmental criminology, it summarizes the theoretical foundations and methodological evolution of crime prediction, and outlines the main technical pathways of machine learning models in this field. From the dual perspectives of prediction targets and prediction scenarios, this study focuses on the applications of machine learning in crime trend prediction, crime hotspot detection, spatiotemporal crime forecasting, crime type identification, as well as suspect and offender location prediction. It further synthesizes representative findings across major crime categories, including property crimes, homicides, financial crimes, and cybercrimes. The results indicate that machine learning approaches can significantly enhance the accuracy and timeliness of crime prediction, offering new insights for social security and crime prevention. Nevertheless, current research still faces challenges in data sparsity, spatiotemporal correlation processing, regional partitioning rationality,

作者简介：张耀峰（1979-）男，博士，教授，研究方向：机器学习、数字政府、数字经济等；徐旭（1984-）男，博士，讲师，研究方向：机器学习、数字经济；王睿（1997-）女，博士，讲师，研究方向：机器学习、数字经济；
*通讯作者：姚金伶（1998-）女，硕士研究生，研究方向：机器学习、数字经济。

model interpretability, prediction performance evaluation, as well as ethical and privacy protection issues.

【**Keywords**】Machine learning; Crime prediction; Spatio-temporal prediction; Crime scene

犯罪问题影响着社会的和谐发展，威胁着公民的生命与财产安全。打击犯罪、降低犯罪发生率是历届政府关注的重点问题之一。对公安而言降低犯罪发生率的重要手段可以归纳为“打、防、管、控”。其中，“防”指的是预防犯罪，而预防犯罪的前提是对可能实施的犯罪行为进行预测。及时、准确的犯罪预测可以提前预知犯罪信息，有针对性地提出合理的布控、排查与巡逻方案，将犯罪预防从被动响应转为主动防范，是一种降低犯罪发生率的理想手段。但是，由于早期警务系统信息化程度低、数据获取难，警察仅能根据经验或直觉对可能的犯罪进行判断，存在的少量犯罪预测研究也仅以理论研究[1-7]和定性分析[8-10]为主。随着统计学方法的兴起，核密度估计[11-14]、风险地形建模[15-16]和自激点模型[17-20]等各种犯罪预测方法相继被提出，并取得了丰富的研究成果。

随着信息时代的发展，大数据已成为国家战略的重要组成部分，数字政府、“互联网+”放管服等一系列改革极大地促进了政府部门大数据的管理与应用。在此背景下，公安系统率先迈出了数字化转型的步伐，启动了数字警务和智慧警务的建设，警务大数据由此迎来发展的春天。警务大数据不仅提高了工作效率与质量，还为犯罪预测提供了广泛而坚实的数据基础。然而，警务大数据普遍具有数据量大、高维度、多源异构等特点，传统犯罪预测方法难以发挥优势。随着大数据与人工智能技术的不断发展，机器学习逐渐成为解决这一问题的重要工具。近年来，基于机器学习的犯罪预测研究逐渐兴起，将犯罪预测研究推向新的高潮。机器学习技术不仅能够深入挖掘警务大数据中的潜在信息，还具备强大的适应性，能够应对复杂数据特征，从而显著提升犯罪预测的精度与效率，推动警务工作的进一步创新。

本文旨在对基于机器学习的犯罪预测研究进行系统综述。首先，梳理犯罪预测研究的理论依据，为后续分析奠定理论基础。接着，从预测对象和预测场景两个维度对现有研究进行分类与总结，全面揭示研究现状和主要方向。最后，分析当前研究存在的不足，并探讨未来研究的发展方向，为相关领域的研究人员提供参考与借鉴。

1 犯罪预测的基础理论与方法

在讨论基于机器学习的犯罪预测之前，我们先来探讨这样一个问题，即犯罪是可预测的吗，犯罪预测的理论依据是什么？显然，这是基于机器学习方法进行犯罪预测的前提。众所周知，利用机器学习进行犯罪预测是近些年才逐渐兴起的新方法，那么在此之前学者是如何进行犯罪预测的，犯罪预测的方法是如何演化的？为了更好的回答这些问题，本部分先对犯罪预测的基础理论和方法演化进行综述。

1.1 犯罪预测理论基础

环境犯罪学（Environmental Criminology）被普遍认为起源于美国犯罪学家 Jeffery 在 1971 年提出的“通过环境设计预防犯罪”（Crime Prevention Through Environmental Design, CPTED）理论[1]。该理论核心在于通过改变犯罪发生的物理环境条件来预防犯罪行为，强调犯罪是犯罪者与环境之间互动的结果，而非完全随机的事件。这一视角促使犯罪学研究从关注犯罪者的心理和社会特征转向关注犯罪行为的时空分布规律。

基于环境犯罪学，研究者进一步提出了一系列经典理论，包括理性选择理论[2]、日常活动理论[3]、犯罪模式理论[4-5]等。这些理论从犯罪原因与特点的不同角度出发，共同揭示了犯罪行为的外部条件及其发生规律，并揭示犯罪者、犯罪目标与时空环境之间的相互作用，研究犯罪行为的空间聚集性和时空分布特征。这些理论奠定了犯罪预测的理论基础，推动了基于数据驱动的方法对犯罪时空风险动态特征的研究。犯罪预测因此可以理解为，通过分析犯罪主体、时空环境及案件要素的交互关系，构建预测模型以评估未来犯罪风险。

在上述理论的基础上，重复受害理论[6]和临近重复现象[7]随即被提出。重复受害理论由 Farrell 于 1993 年提出，其观点是曾经受害的个体或地区更容易再次成为犯罪目标[6]，这为基于历史数据进行犯罪风险评估提供了理论依据。由重复受害理论进一步延伸，形成临近重复现象理论，该理论指出某地发生犯罪后，其周边地区在短时间内的犯罪风险显

著上升[7]。临近重复现象的实证发现来自英国伦敦大学学院 Jill Dando 犯罪科学研究所在 2004 年对入室盗窃的研究[21]。此后，研究者们对美国、澳大利亚、中国等 15 个不同城市进行实证研究，结果表明犯罪的传播具有显著的时间和空间特征，例如入室盗窃的时空传播范围分别为两周和周围 400 米，不同城市之间在风险尺度上存在一定差别[22]。从理论关系来看，重复受害理论与临近重复现象是对犯罪模式理论的细化和补充。犯罪模式理论侧重于宏观的时空分布特征，而重复受害理论和临近重复现象则专注于微观的个体或区域特征[23-24]。这些理论均强调历史犯罪事件在预测未来犯罪中的重要作用，并通过揭示犯罪的空间聚集性与时间连续性，为犯罪预测提供了多层次视角。

为进一步理清环境犯罪学理论与机器学习犯罪预测的关系，将各主要理论的研究角度及其在预测方法设计中的具体作用进行总结（表 1）[25]。这些理论不仅奠定了犯罪可被预测的理论基础，同时也启发了基于机器学习的犯罪预测模型在特征选择和算法设计上的思路。例如，时空位置可以被用于构建犯罪风险的空间热力图，历史犯罪记录可以被用作训练机器学习模型的输入变量。

表 1　基于环境犯罪学的主要犯罪预测理论

犯罪理论	提出者	提出时间	研究角度	主要观点	对基于机器学习的犯罪预测方法的启示
理性选择理论	Cornish	1986 年	犯罪原因	犯罪者会权衡犯罪收益与成本，特定环境下收益大于成本可能导致犯罪	数据中应纳入有关犯罪成本和收益的相关因素，以帮助建模犯罪者决策过程
日常活动理论	Cohen&Felson	1979 年	犯罪原因	犯罪是犯罪者、犯罪目标和防范缺失三要素交互作用的结果	模型设计中应考虑犯罪三要素（如目标特性、时空特性等）
犯罪模式理论	Brantingham	20 世纪末	犯罪特点	犯罪活动与环境、地点特征相互作用	地点和环境变量可用作模型特征来解释犯罪聚集现象
重复受害理论	Farrell	1993 年	犯罪特点	受害个体或地区更易再次受害	历史犯罪记录应被用作模型的重要特征变量
临近重复现象	Townsley	2003 年	犯罪特点	犯罪地点周围区域在短期内风险增加	模型可通过时空聚类方法量化犯罪风险扩散

1.2 犯罪预测方法

随着犯罪研究的不断深入，犯罪预测逐渐成为学术界和实践中关注的重要领域。犯罪预测方法经历了从传统定性理论向现代定量分析与建模转变的过程。随着统计学的兴起，统计分析方法开始应用于犯罪预测当中。最早的利用统计学方法进行犯罪预测研究可以追溯到 Sutherland 等利用传统统计分析研究了犯罪与环境、人口数量的关系以及犯罪的季节差异与社区差异[26]。此后，犯罪预测方法不断更新，热点地图（Hotspot Mapping）[27-30]和基于地理信息系统（GIS）[31]的犯罪地理制图等技术相继被引入，极大地提高了犯罪预测的直观性和准确性。

在时空分析方法的推动下，犯罪预测进一步向动态化和精细化方向发展。例如，Johnson 等人借鉴传染病时空分析方法（Knox）研究了多国入室盗窃犯罪的时空风险特征，并提出了相关的犯罪预测方法[21,32,33]。基于前瞻性热点（Prospective Hotspot）[12]和时空扫描统计（Spatio-Temporal Scanning Statistics）技术[34]的研究则进一步深化对犯罪时空模式的理解。这些方法通过揭示犯罪行为的空间和时间分布规律，为动态预测和干预提供了科学依据。

核密度估计（Kernel Density Estimation, KDE）[12-14]是犯罪预测中较早采用的非参数统计方法之一。KDE 通过对历史犯罪记录的空间分布进行平滑估计，量化区域犯罪风险。KDE 方便实施，适用于任何有犯罪地点记录的地区，且无需对数据分布做强假设。但由于未能纳入环境变量等复杂因素，其预测能力和解释性较为有限。为了解决这一不足，Caplan 等提出了风险地形建模（Risk Terrain Modeling, RTM）[15]。RTM 通过引入与犯罪类型相关的环境变量，分析风险来源，从而提升了预测的科学性和可解释性。在进一步探索犯罪热点特性时，Short 等引入偏微分方程（PDE）[35-37]对犯罪热点进行建模，该模型通过宏观视角模拟犯罪行为的时空聚集特征，可以视为微观随机游动过程的连续极限。随后 Mohler 等[17]发现犯罪行为的发生具有类似于地震的聚类模式，因此基于自激点过程理论（Self-exciting Point Process, SEPP）建立流行型余震序列模型（Epidemic Type Aftershock Sequences, ETAS），该模型利用犯罪事件之间的时间和空间关联特性，成功预测了洛杉矶地

区的入室盗窃行为，验证了其在犯罪预测中的优越性。SEPP 的提出显著推动了犯罪时空预测领域的发展，引发了后续一系列基于该理论的研究[18-21]。

近年来，机器学习方法逐渐成为犯罪预测领域的重要工具。相较传统统计方法，机器学习能够处理更加复杂和大规模的数据场景，并通过自适应算法提升预测精度与效率。在犯罪预测研究中，学者们尝试了包括 K-近邻（K Nearest Neighbors, KNN）[38]、朴素贝叶斯（Naive Bayes）[39]、支持向量机（Support Vector Machine, SVM）[40]、决策树（Decision Tree）[41]、随机森林（Random Forest）[42]、神经网络（Neural Networks）[43]、长短期记忆网络（Long Short Term Memory, LSTM）[44]等多种方法，这些方法在预测犯罪时表现出高度灵活性和鲁棒性，适用于多种数据类型及复杂场景，显著提高了预测结果的精确性与应用价值。

作为一种交叉学科研究方法，机器学习通过模拟人类的学习过程，从犯罪数据中不断挖掘规律并迭代优化模型功能，从而有效提升学习效率与预测能力。在犯罪预测中，机器学习不仅可以有效捕捉犯罪的时空特征，还能够应对不同案件场景和预测需求。例如，某些研究专注于犯罪类型预测，探索特定行为模式的成因；另一些研究则着眼于时间和空间分布规律，优化资源分配和警力部署。与传统预测方法相比，机器学习具有更强的适应性和扩展性。其核心目标不仅是预测犯罪的变化趋势，还包括确定犯罪发生的具体时间与地点、分析潜在的犯罪类型及嫌疑人特征等。在机器学习的驱动下，研究者们不仅关注基于机器学习的预测方法本身，还深入探索不同预测对象与场景的多样化需求，并探讨这些方法在不同预测对象与场景中的适用性。本文后续将系统总结机器学习在犯罪预测中的应用，并从预测对象和场景的角度探讨相关方法的实际表现。

2 预测对象分类及机器学习应用

犯罪包含多个要素，比如时间、地点、犯罪嫌疑人、犯罪类型等。根据不同的犯罪要素，犯罪预测的内容即预测对象也不相同。因此，按照不同的预测对象将犯罪预测归为以下几类：犯罪趋势预测、犯罪热点预测、犯罪时空预测、犯罪类型预测、犯罪嫌疑人预测以及嫌疑人落脚点预测。针对不同预测对象的犯罪预测在预测目标、数据输入和使用算法上都有所差异，详见表 2。本节将具体对机器学习方法在上述六类犯罪预测问题中的研究与应用进行介绍。

表 2 犯罪预测问题分类

类型	要素	预测内容	算法类型
犯罪趋势预测	时间	对未来犯罪数量进行回归预测	回归
犯罪热点预测	地点	识别犯罪的高发地区	分类
犯罪时空预测	时间、地点、嫌疑人	预测未来何时、何地会发生犯罪	回归、分类
犯罪类型预测	犯罪类型	根据特征预测犯罪类型	分类
犯罪嫌疑人预测	嫌疑人	预测识别犯罪嫌疑人以及其犯罪的可能性	回归、分类
嫌疑人落脚点预测	时间、地点、嫌疑人	预测犯罪嫌疑人可能的落脚点或藏匿地点	回归、分类

2.1 犯罪趋势预测

犯罪趋势预测通常是指对未来犯罪数量或犯罪事件发生频率的回归预测。犯罪时间序列和一般的时间序列相同，具有明确的过去、现在和未来顺序。因此，可以通过对犯罪时间序列进行统计学习分析，学习和发现犯罪模式和变化趋势。犯罪趋势预测可为预防和控制犯罪风险以及打击犯罪提供重要的决策支持。

早期的研究多集中在传统统计方法，如回归分析和时间序列模型对犯罪趋势进行预测。1993 年，魏智远[45]从犯罪要素出发，以年为时间尺度建立线性回归方程预测未来犯罪的发展趋势和数量变动，预测的标准误差为 51.3 起。由于使用回归方程预测需要使用与犯罪数据高度相关的自变量，但找到这样的自变量具有一定难度。并且研究表明，当回归方程模型预测跨越三个或更多季度的时间范围时，预测准确性显著降低[46]。所以更多的学者转向使用时间序列方法对犯罪数据进行分析和预测，指数平滑模型[47]、ARMA[48]、ARIMA[49]、SARIMA[50]等均被使用于犯罪趋势预测当中。

然而，时间序列方法的局限性也逐渐显现：一方面，这些方法通常仅依赖于历史数据，忽视了其他环境因素（如天气、社会活动等）的影响；另一方面，当预测时段较长时，模型的预测准确度往往显著下降。随着机器学习方法的兴起，越来越多的学者采用机器学习方法进行犯罪数量的回归预测分析，以提高犯罪趋势预测的准确性和灵活性。其中基于深度学习的模型如 LSTM，在处理具有复杂时序特征的犯罪数据时表现出了显著的优势。与传统的回归和时间序列模型不同，LSTM 能够捕捉时间序列中的长短期依赖关系，因此在犯罪预测中得到了广泛应用。Feng 等[51]使用 LSTM 和 Prophet 模型对旧金山、芝加哥和费城的每日犯罪数据进行预测，结果表明 LSTM 模型相比传统神经网络表现更好，能够提供更加精准的趋势预测。颜靖华等[52]对中国 A 市日盗窃犯罪数据应用 LSTM 模型进行预测，比较了 LSTM 与 ARIMA、支持向量机等模型的预测效果，结果表明 LSTM 在多个场景下的预测效果最优。近年来，Butt 等[53]采用了深度学习方法进行犯罪趋势预测，并在芝加哥、纽约和拉合尔的犯罪数据集上进行了实验。通过比较 LSTM、BiLSTM 等深度学习模型与传统的移动平均法（SMA、WMA、EMA），发现 BiLSTM 模型在大多数情况下表现优于其他方法，尤其在每周预测中的误差率更低，展示了深度学习方法在处理犯罪趋势数据时的有效性。这些基于深度学习的非线性方法在处理长时间序列数据时展现出比传统模型更强的预测能力。虽然 LSTM 等深度学习模型在某些应用场景下取得了良好的效果，但其计算复杂度较高，且需要大量的训练数据和精细的参数调优，因此在实际应用中仍然面临一定的挑战。

除了传统的时间序列模型和基于 LSTM 的深度学习方法，研究者们也探索了其他创新型预测方法，以应对实际应用中的数据多样性和复杂性。例如，Ivanyuk[54]提出了一种集成预测系统，将线性预测、神经网络与小波预测相结合，应用于俄罗斯数字金融犯罪趋势预测。研究发现，这种方法通过结合多种预测技术的优势，在非线性数据处理中表现出更高的预测准确性。这一研究表明，集成模型在融合多种算法优点的同时，能够弥补单一模型在处理复杂犯罪数据时的局限性。此外，Bappee 等[55]提出了一种跨域学习方法，将多伦多和温哥华的犯罪数据知识迁移至哈利法克斯，以解决数据量不足背景下的犯罪预测问题。研究显示，跨域学习能够有效提升小样本数据的预测性能，为数据不足或资源受限的情境提供了新的解决方案。与传统的单域模型相比，这种方法能够利用不同区域的犯罪数据特征，提高模型的泛化能力。然而这些创新方法也存在一定的局限性。集成预测系统和跨域学习方法通常需要高质量的训练数据和精细的特征设计，这对数据的完整性和准确性提出了更高要求。并且模型复杂性的提升可能导致实际部署中的计算成本和技术门槛增加，限制了其在资源有限地区的应用。

犯罪趋势预测的效果不仅与选择的预测模型和数据质量密切相关，还受到预测时间尺度的显著影响，而时间尺度的确定在实际应用中尤为关键。现有研究可以分为短期（如每日、每周）[52-56]犯罪趋势预测和长期（如月度、季度、年度）[57-59]犯罪趋势的预测，较短时间尺度的预测对于日常犯罪防控和应急决策具有较好的时效性。相比之下，较长时间尺度的预测通常侧重于宏观犯罪规律的挖掘，虽然能够为社会安全政策提供参考，但在日常犯罪防控和应急决策方面的时效性较差。而很多现有模型仍面临着时效性问题，特别是在处理即时性要求较高的日常犯罪监控任务时，现有模型的预测能力和响应速度尚需进一步优化。

尽管机器学习方法在犯罪趋势预测中已取得一定成果，但仍然面临诸多挑战。比如数据层面的犯罪数据缺失、不完整或滞后可能导致预测结果的不准确等问题；模型层面的模型复杂性和可解释性问题，如何在保证预测精度的同时提高模型的可解释性，尤其是在实际应用中的可操作性，是未来研究的重要方向。总的来说，犯罪趋势预测领域正在向着更加精确和实时的方向发展，非线性机器学习方法在时序数据预测中的优势逐渐获得学术界和实践领域的认可。未来研究需在模型复杂性、数据质量与实时性需求之间找到平衡，以进一步提升模型在实际场景中的应用价值。

2.2 犯罪热点预测

犯罪热点预测以地理位置为核心预测对象，旨在判别特定地点的犯罪风险大小，并通过设定阈值将区域划分为犯罪热点区域和非热点区域。有关犯

罪热点预测问题很早就引起了学者们的关注，最开始基于传统统计分析方法进行预测研究分析，包括莫兰指数（Moran's I）[60]、核密度分析[11-14]、风险地形建模[15-16]、基于地理信息系统（GIS）的犯罪地理制图[31]等。这些方法利用犯罪的空间集聚特征开展犯罪的空间探索与分析，具有可视化效果直观、计算简便等优势，但在处理复杂和非线性犯罪模式时表现不足，无法对犯罪热点的动态变化进行高精度预测。此外，传统方法依赖历史数据，较难融入新的特征变量，限制了实际应用效果。

随着机器学习技术的发展，学者们开始探讨机器学习在犯罪热点预测中的应用。Kianmehr 等于 2006 年使用单分类 SVM 对犯罪热点进行预测[61]。随后进一步对单分类 SVM 与二分类 SVM 进行比较，结果显示二分类 SVM 效果更优，同时结合 K-means 聚类算法的数据预处理进一步提高了预测性能[62]。由于犯罪数据天然具有空间集聚特性，因此聚类算法在犯罪热点预测当中的应用十分广泛。Guevara 等[63]、石汝南等[64]均使用 K-means 算法对犯罪热点区域进行聚类分析预测。K-means 算法计算复杂度低、易于实现，适合处理空间聚类问题，但其结果依赖初始聚类中心，容易陷入局部最优。为弥补单一算法的不足，Kouziokas[65]将空间聚类方法与人工神经网络模型相结合，预测高犯罪风险的交通区域。并利用地理信息系统（GIS）进一步确定犯罪事件的高度集聚区域。这种结合方法有效融合了空间分析与非线性预测的优势，但模型复杂性与计算成本较高。

决策树算法作为一种易于理解且高效的分类方法，在犯罪热点预测中得到了广泛应用。该方法通过递归划分数据生成树状结构，对犯罪数据进行分类建模。Sathyadevan 等[66]通过命名实体识别（NER）提取网站文本信息中的时间与地点字段，并使用决策树算法预测犯罪发生的区域和模式。Emmanue 等[67]则基于 J48 决策树算法预测某县发生低、中、高暴力犯罪的可能性。决策树模型的优势在于其构建过程清晰，具有较高的透明性和解释性，同时对缺失值和噪声数据具备较强的容忍能力。然而决策树容易受到数据噪声的影响，尤其是在特征选择和数据不平衡的情况下，其预测性能可能会下降。此外，决策树容易出现过拟合现象，尤其在树深较大的情况下，模型对训练数据的依赖性可能过强，限制了其泛化能力。随机森林则通过集成多个决策树，综合不同树的预测结果，进一步提升了模型的稳健性和精度。在犯罪热点预测中，随机森林表现出优越的性能。Bogomolov 等[68]将犯罪热点预测看作二分类问题，采用 SVM、逻辑回归、神经网络和决策树等多种分类器进行训练，发现基于 Breiman 随机森林算法的决策树分类器在性能上表现最佳。随机森林能够处理大规模数据，并有效缓解决策树的过拟合问题，同时适应更多类型的异常数据。但其计算复杂度较高，对大规模数据集的处理存在内存和时间消耗瓶颈。此外，随机森林模型的“黑箱”特性限制了其解释性，实际应用中需要借助额外的技术手段提升模型的透明度。

近年来，基于位置的社交网络（LBSN）数据为犯罪热点预测提供了新方向。Huang 等[69]通过基于位置的社交网络提取犯罪相关特征，采用支持向量机与随机森林等监督学习方法，建立地区犯罪热点预测模型。研究发现，基于位置的社交网络数据可以有效补充传统犯罪数据的不足，但这类方法对数据质量和完整性要求较高，社交网络数据的隐私性和获取难度增加了模型开发的复杂性，同时噪声数据的存在可能对预测结果产生不利影响。

犯罪热点预测方法在传统统计分析与现代机器学习算法的演进过程中不断发展。传统方法在直观性与可操作性上具有优势，但在应对动态与复杂环境中的犯罪热点时显得力不从心。机器学习方法通过强大的非线性建模能力，显著提高了预测精度和适应性，但高计算成本和模型解释性仍是主要挑战。未来研究可以通过引入多源数据（如社交网络、天气和区域经济数据），结合先进的时空建模技术（如深度学习和图神经网络），进一步提升犯罪热点预测的实时性和精度，同时注重模型的透明性和应用可行性，以满足实际需求。

2.3 犯罪时空预测

从本质上来说犯罪数量预测是基于时序的角度、犯罪热点预测则是基于空间的角度，两者均将时空割裂开并分别将其当作独立变量进行研究。但犯罪往往不是独立发生的，而是具有强烈的时间和空间相关性，在警务实际应用场景中，综合考虑时间和空间相关性的犯罪时空预测显得格外重要。近年来，

越来越多的学者使用机器学习方法进行犯罪时空预测。根据输入数据的不同，犯罪时空预测研究可分为基于栅格数据的犯罪时空预测和基于非栅格数据的犯罪时空预测。

2.3.1 基于栅格数据的犯罪时空预测

基于栅格数据的犯罪时空预测通过将研究区域划分为固定大小的网格单元，将犯罪数据与网格绑定，形成栅格化犯罪数据集。这种方法将空间区域抽象为一致性研究单位，为时空数据的处理和建模提供了统一框架，同时便于整合地理信息和犯罪数据。在预测流程中，研究者通常设置滑动时间窗口，将犯罪数据按周期切片并聚合，提取时间序列特征（如周期性、趋势性）和空间特征（如邻近网格的犯罪密度），使用机器学习或深度学习算法进行建模，捕捉犯罪行为在时空维度上的变化模式，从而建立时空预测模型，具体流程见图 1。这种方法能够高效分析犯罪的时空分布特征，为犯罪风险的预测与防控提供科学支持。

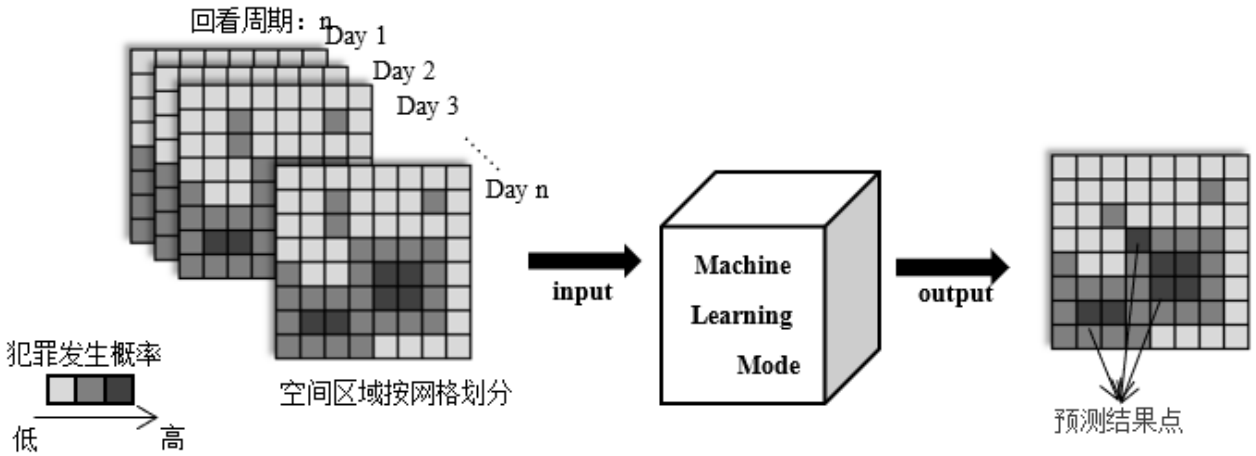

图 1　犯罪时空预测流程

早期研究中，机器学习算法如逻辑回归、SVM、KNN 和决策树等被广泛应用[70]。随着数字警务的不断发展，公安部门获取和存储大规模时空数据的能力显著增强，这为犯罪预测提供了数据支撑，同时也提出了新挑战。深度学习方法通过从大量数据中提取特征并进行训练，在一定程度上提高了预测的准确性。例如，Zhang 等[71]基于 150m×150m 的栅格数据，以两周为时间单位，采用 KNN、随机森林、SVM、朴素贝叶斯、卷积神经网络（CNN）和 LSTM 六种机器学习算法进行犯罪时空预测。结果表明 LSTM 模型在仅使用历史犯罪数据时表现最佳，而传统机器学习方法由于特征提取能力和处理非线性关系的局限性，其预测精度低于深度学习模型。此外，Zhang 等[71]的研究还表明结合建筑环境数据（如 POIs 和城市道路网络密度）后，预测效果显著提升。类似地，Lin 等[72]通过 Google Places API 获取地理信息数据，并将地理特征与深度神经网络（DNN）相结合以提高犯罪预测模型的性能，进一步证明地理特征设计对模型性能和解释力的重要性。

基于栅格数据的方法支持不同时间和空间尺度的预测。时间尺度上，短期预测如日度预测[70-73]能够快速响应犯罪动态，为执法部门调整巡逻策略和分配警力资源提供参考。而长期预测如双周预测[74-75]、月度预测[72]和年度预测[76]适合分析犯罪趋势的长期变化。空间尺度方面，细粒度的网格划分（如 150m×150m 或 600m×600m）能够定位高风险区域，指导执法部门在特定街区或网格单元内采取针对性措施[75-77]，而更大尺度的分析则适用于城市整体安全规划，帮助优化公共设施布局和减少犯罪诱因。

尽管栅格化方法通过标准化框架整合多源数据，并结合深度学习提升了对复杂时空特征的建模能力，但其局限性也不容忽视。例如，网格划分的尺度直接影响预测性能：过大可能忽略犯罪分布细节，过小则易导致数据稀疏。此外，栅格方法离散化空间数据，难以自然表达犯罪活动的流动性和跨网格关联性。针对这些问题，研究者尝试改进网络结构以提升模型性能。如 Zhuang 等[75]提出时空神经网络（STNN），通过针对高分辨率网格的回归模型，提

高了犯罪预测的精度。此外，有研究者结合图神经网络（GCN）进行改进，GCN 能够更好捕捉跨网格的复杂空间关联性[78]，Qian 等将 GCN 与 LSTM 结合，开发 GeST 模型用于综合时空特征，取得了较好的预测效果[79]。这些研究表明，优化网络结构对提升栅格化预测模型的性能至关重要，尤其是在高分辨率网格或稀疏数据环境下。然而，在高分辨率网格下，模型的训练和预测往往面临时间与资源消耗的显著挑战。总之，基于栅格数据的犯罪时空预测在理论研究和警务实践中具有重要价值，能够在预测精度与模型复杂性之间实现平衡。未来研究应注重多源异构数据的融合，如社交媒体和实时监控信息，并结合基于路网等的动态模型，以进一步提升预测性能和适用性。这将推动栅格化犯罪预测在高分辨率、实时化和动态化环境中的广泛应用，助力数字警务的进一步发展。

2.3.2 基于非栅格数据的犯罪时空预测

基于非栅格数据的犯罪时空预测是指利用轨迹数据、不规则区域（如行政区、社区）和路网数据等非栅格化形式的信息，对犯罪的时空分布进行分析与预测。这种方法通过构建更贴近真实场景的空间表达方式，捕捉复杂的空间拓扑关系，弥补了栅格化方法在空间连续性与精细度上的不足。

在基于轨迹数据进行犯罪预测的研究中，肖延辉等[80]提出了一种基于长短记忆型卷积神经网络（LSTM-CNN）的犯罪地理位置预测方法。该方法以轨迹数据（经度、纬度和时间）为输入，利用 CNN 提取犯罪的空间特征，挖掘位置数据在空间维度上的局部相关性，并结合 LSTM 学习时间维度上的连续性，从而实现对下一个潜在犯罪位置的准确预测。

在基于不规则区域进行犯罪预测的研究中，Rumi 等[81]研究了以布里斯班的人口普查区域为地理单元，通过支持向量机、随机森林、神经网络等方法，结合历史犯罪数据和地理、人口动态特征进行犯罪预测。此外，Huang 等[82]开发了一个名为 DeepCrime 的框架，利用深层神经网络探索纽约市行政区内犯罪模式与城市其他数据的依赖关系。Wang 等[83]提出了深度时态多图卷积网络（DT-MGCN）模型，在芝加哥社区内捕获犯罪与外部因素的复杂关联。

在基于路网数据进行犯罪预测的研究中，路网数据将犯罪场景关联到街道环境，包括街道网络、道路与节点三层结构[84]。这一方法为分析犯罪风险的空间分布提供了新的视角。图传播模型是其中一种重要的技术，通过在图结构上设计风险传播算法，有效捕捉了犯罪风险在路网中的传播规律。研究表明，基于路网的模型在预测精度上优于非路网模型[85-86]。Zhang 等[87]则进一步创新，开发了门控局部扩散网络模型（GLDNet），通过将街道网络表示为加权无向图并结合深度学习技术，实现了稀疏犯罪事件的热点预测，显著提升了预测能力和实用性。

相比栅格数据方法，基于非栅格数据的犯罪时空预测能够更加准确地表达空间的连续性和复杂性，尤其在应对稀疏数据和复杂网络拓扑时表现出色。这类方法对指导警力部署、优化巡逻策略以及降低犯罪率具有重要的实际意义。然而该方法在应用上也面临一些挑战。如在数据获取方面，高质量轨迹数据及动态路网信息的获取难度较大，这在一定程度上制约了其应用范围与精度。同时，预测模型复杂度高，对计算资源需求高增加了实施成本与技术门槛。此外，预测模型的可解释性大多较弱，需借助可视化工具及领域知识来增强其实际应用中的可操作性与理解性，以更好地服务犯罪预测与防控工作。总体而言，非栅格数据的犯罪时空预测为犯罪学研究和警务实践提供了新视角与新思路。犯罪时空预测相比单纯的犯罪时间、犯罪地点预测更合理，相关研究也较多，是警务时空大数据研究与应用热点，对指导巡逻、降低犯罪率有重要应用价值。

2.4 犯罪类型预测

犯罪类型预测是指通过分析历史犯罪数据和相关特征，利用机器学习或深度学习算法对未来犯罪可能的类型进行分类预测。此类研究旨在针对不同类型的犯罪问题采取精准化的预防和管控措施，从而提升公安部门的工作效率和决策水平。犯罪类型预测能够有效辅助资源分配，如优化警力部署和制定针对性的执法策略，在犯罪预防和减少犯罪率方面具有重要意义。

犯罪类型预测的主要方法以分类算法为主，涵盖传统机器学习和深度学习。传统方法中，K-means、K 近邻、决策树、随机森林、朴素贝叶斯和 SVM 等分类算法被广泛应用。Baculo 等[88]通过对多分类方法包括贝叶斯网络、朴素贝叶斯、决策树和随机森

林的对比研究，发现随机森林在多项评价指标上表现最佳。此外，Alparslan 等[89]和 Wu 等[90]分别将随机森林与其他机器学习算法进行比较，均得出随机森林在分类精度和泛化性能上表现更优的结论。随机森林作为一种集成学习算法，通过结合多个决策树的结果，能够捕捉犯罪数据中多维特征的复杂非线性关系。其在处理包含犯罪时间、地点和作案手段等多种特征的大规模数据集时表现较为优异，能够显著提高预测准确性。然而，随机森林模型对计算资源的需求较高，在处理较小规模数据或单一特征数据时可能会显得效率不足。朴素贝叶斯和 SVM 因其理论简单且计算高效，在犯罪类型预测中有广泛应用。朴素贝叶斯模型假设特征之间相互独立，适合处理具有条件独立性的犯罪数据[91-92]。但这一假设在实际场景中可能不完全成立，从而限制了模型的预测性能。SVM 在小样本情况下具有出色的分类能力，尤其适用于线性可分的犯罪类型数据，其通过构建最优超平面，实现对不同犯罪类型的有效分离[93]。但在犯罪数据具有显著非线性特征的情况下，SVM 的性能受到核函数选择和参数调优的限制，难以与深度学习方法竞争。Nguyen 等利用神经网络对犯罪类型进行预测，通过自动提取犯罪数据中的高阶特征，捕捉犯罪模式的复杂性[94]。神经网络的优势在于能够自动提取高阶特征并建模复杂的非线性关系，尤其在处理时间序列和多维数据时表现突出。然而，其训练过程需要较大的计算资源，对数据量的需求也较高，适用于拥有丰富标注数据的大规模预测任务。

总体而言，犯罪类型预测需根据数据特性、任务需求和计算资源等选择适当的算法。传统机器学习方法简单高效，适用于中小规模数据或初步探索性分析；深度学习方法则能挖掘复杂数据关系，更适合大规模、高复杂度的犯罪类型预测任务。未来的研究可以进一步探索多模型融合的方法，以充分利用不同算法的优势，提高预测精度和模型的泛化能力，为警务决策提供更精准的技术支持。

2.5 犯罪嫌疑人预测

犯罪的主体是犯罪嫌疑人，因此在犯罪预测中对犯罪嫌疑人进行预测既是重点，也是难点。犯罪嫌疑人预测是通过对历史犯罪数据和相关特征的分析，识别潜在犯罪嫌疑人或预测特定犯罪事件可能涉及的嫌疑人群体。犯罪嫌疑人预测是犯罪预测领域的重要方向，其意义在于帮助公安部门精准锁定嫌疑对象，提高破案效率，并为预防犯罪提供技术支持。在实践中，根据数据类型的不同，犯罪嫌疑人预测可以分为基于文字特征的犯罪嫌疑人预测[95]和基于图像数据的犯罪嫌疑人预测[96]。

累犯预测是犯罪嫌疑人预测的重要领域，其核心在于分析历史数据以预测特定个体再次犯罪的概率。实验统计证明，犯罪者再次进行犯案的概率比其他没有犯罪经历的人犯罪概率更大，因此针对再犯者和惯犯的预测具有重要的实际意义。累犯预测的研究最早可追溯至 1928 年，Burgess 提出一个预测假释结果的简单模型[97]，其后便陆续出现了各种参数模型和非参数模型[98]，但由于犯罪数据噪声水平高以及没有其他相关变量，这些模型的性能存在显著差异。为解决上述问题，Schmidt 等提出了“分裂人口”生存时间模型，该模型能够区分一般人口与高风险群体，从而提高累犯预测的准确性[99-100]。

深度学习方法在累犯预测领域取得了显著进展。Brodzinski 等[101]利用神经网络对青少年累犯进行预测，准确率高达 99%，表明神经网络在建模复杂行为模式方面具有显著优势。但深度学习模型的高计算资源需求和较差的结果解释性限制了其实际应用。Palocasy 等[102]在 2000 年使用人工神经网络对惯犯进行预测，通过对惯犯行为模式的学习，实现了较高的预测精度。2010 年，Wang 等[103]提出基于 SVM 的累犯预测模型，结合个人相关信息构建特征空间以区分累犯与非累犯。实验结果表明，SVM 在高维特征空间中通过最大化超平面间隔有效分离不同类别的个体，尽管其性能在不同年份的数据集上与神经网络和逻辑回归相比存在波动。结合这三种方法的研究进一步证实了多模型融合在累犯预测中的潜力，为该领域提供了新的方向。Tollenaar 等[104]通过分析不同类型的惯犯（如暴力惯犯和性犯罪惯犯），提出针对性的模型建构策略，通过结合逻辑回归、Adaboost 和线性 SVM 等方法，探讨了数据特征与模型性能之间的关系。研究表明，在较大的样本量和清晰的特征描述下，机器学习方法表现优于传统统计模型；在小样本条件下，其表现存在较大差异。

综上所述，犯罪嫌疑人预测结合了传统统计方法与现代机器学习技术，不同方法在处理特定任务

时各有优势。在未来，研究者应进一步优化模型性能并提升其可解释性，同时探索跨领域数据的整合应用，以满足实际场景中复杂多变的预测需求。

2.6 犯罪嫌疑人落脚点预测

犯罪嫌疑人落脚点预测旨在通过分析犯罪嫌疑人可能的行动轨迹和相关特征，定位其潜在藏匿地点。这一研究方向对精准执法和缩短破案周期具有重要意义，但由于嫌疑人藏匿范围的广泛性及其活动的隐蔽性，实现高精度预测仍是警务工作中的挑战之一。20 世纪 90 年代，Rossmo 提出犯罪地理目标模型（Criminal Geographic target, CGT）用于预测犯罪嫌疑人落脚点[105]。该模型结合犯罪地理学和数学等相关学科知识，通过使用分段距离递减函数对犯罪活动距离进行模拟，并使用案件的地理轨迹信息，计算研究区域内的嫌疑人落脚点概率分布，从而缩小犯罪嫌疑人的搜索范围。CGT 已在国外警务实战中进行了广泛应用[106-107]，但该模型仍存在其不足，如：未考虑到嫌疑人分布地点类型的复杂性[108]；未考虑到犯罪嫌疑人移动数据的稀疏性[109]等。为改进 CGT 模型的不足，研究者提出了多种增强方法。方嘉良等[110]和李卫红等[111]在 CGT 基础上引入了更多地理和行为变量，使模型能够更全面地刻画犯罪行为特征。而 Duan 等[112]提出犯罪多阶贝叶斯模型（Crime Multi-order Bayes model，CMoB）并结合时空语义分析对嫌疑人的多步位置进行预测，其预测性能优于传统方法。

在基于聚类方法的研究中，姜丁菊等[113]使用 Kmeans 聚类得到作案点的聚类中心，然后通过求解无约束优化问题得到嫌疑人的据点，并使用仿真实验推断了 ISIL 组织近几年在伊拉克进行恐怖袭击的据点位置，验证了该方法在恐怖袭击据点预测领域的有效性。尽管如此，聚类方法在面对高维复杂数据时的适应性较差，且需要依赖数据的聚集性特征。

深度学习技术的引入为犯罪嫌疑人落脚点预测提供了新的思路。肖延辉等[80]利用长短记忆型卷积神经网络（LSTM-CNN）对犯罪分子位置进行预测，在结合时空信息后实现了 0.79 的精准度。这一方法通过自动提取时间和空间维度的特征，有效克服了传统模型对特征工程的依赖。然而，深度学习模型的计算复杂性较高，对数据量和硬件资源的要求也较大。

总体来看，犯罪嫌疑人落脚点预测涵盖了传统统计模型、机器学习和深度学习方法。传统模型如 CGT 和 CMoB 在地理行为建模中具有重要贡献，而聚类方法和深度学习则为复杂数据和动态环境的预测提供了更灵活的解决方案。未来的研究应进一步结合多源数据和实时动态分析技术，以提升预测性能并满足实际警务需求。

综上所述，犯罪预测按照研究对象可以划分为犯罪趋势预测、犯罪热点预测、犯罪时空预测、犯罪类型预测以及犯罪嫌疑人预测。针对不同的预测对象，研究内容和机器学习方法的选择存在显著差异。犯罪数量预测通常采用回归模型，犯罪热点预测倾向于利用聚类与时空分析模型，而犯罪时空预测、犯罪类型预测及犯罪嫌疑人预测则依赖于分类与深度学习方法的协同应用。为了更直观地对比不同机器学习方法在犯罪预测中的适用类型及其优缺点，本文总结了常用方法的特征，见表 3。通过上述分析和表 2 总结可以看出，不同方法在犯罪预测中的适用场景和性能表现各有千秋。在实际研究与应用中，应结合预测对象的具体需求、数据特性及计算资源选择最优方法，以提高预测的准确性与实际效用。

3 预测场景分类及机器学习应用

通常来说，一个地区可能发生多种类型的犯罪，经网格或行政划分后其中某一个区域可能被标记为盗窃类案件热点地区，而另一个区域则可能被标记为抢劫类或其他特定类型的犯罪热点区域。研究表明，犯罪的类型和频率在空间上的分布往往是不均匀的。Butt 等通过整理纽约市犯罪数据发现，不同类型犯罪在空间分布上存在显著差异[114]。为了增加犯罪数据的样本量，在一定程度上减少犯罪数据稀疏性对模型算法的影响，现有的大部分有关犯罪预测的研究中并未对案件类型进行区分。但事实上不同类型的案件具有不同的特征且影响不同类型案件发生的因素也各不相同。因此，针对不同案件类型进行场景划分并展开预测研究显得尤为重要。Rumi 等针对盗窃、毒品犯罪、攻击、欺诈、非法入境和交通肇事等类型案件，分别使用机器学习方法进行犯罪预测，揭示了不同类型案件在预测模型应用中的差异[81]。根据已有文献，基于机器学习的犯罪预测研究主要集中于侵财案件、凶杀案件、金融犯罪和网络犯罪四大类场景（表 4）。这些场景的划分为犯

罪预测提供了更具针对性的研究框架，同时也对方法选择和数据处理提出了更高的要求。

3.1 侵财类案件犯罪预测

侵财类案件是指通过非法手段占有他人财物的犯罪行为案件，也称多发性侵财犯罪，主要包括盗窃、抢劫等犯罪案件。这类案件因其高发性、影响广泛且直接关系到公共安全，长期以来成为犯罪预测研究的重点领域。侵财类案件的犯罪预测具有以下场景特征：案件数量庞大且分布广泛，时空动态特征显著，受社会经济因素和环境变量的综合影响。这些特点对预测模型的准确性和适用性提出了较高要求。通过对侵财类案件的精准预测，执法部门可以合理配置警力资源，制定针对性的防控措施，有效降低此类犯罪的发生率，从而提升社会治安管理水平。

表 3　常用机器学习方法在犯罪预测中的适用类型及优缺点

方法	适用类型	优点	缺点
线性回归	犯罪趋势预测	模型简单、解释性强	适用范围有限，难以处理非线性和复杂关系
决策树	犯罪热点预测、犯罪时空预测、犯罪类型预测	直观易理解、对特征选择不敏感	容易过拟合，对噪声数据敏感
随机森林	犯罪热点预测、犯罪时空预测、犯罪类型预测	抗过拟合能力强、可处理高维数据	计算复杂度高，训练时间较长，模型解释性较差
支持向量机	犯罪趋势预测、犯罪时空预测、犯罪类型预测、犯罪嫌疑人预测	能处理非线性问题，适合小样本学习	对核函数和参数选择敏感，计算复杂，训练速度慢
K-means 聚类	犯罪热点预测、犯罪类型预测、犯罪嫌疑人落脚点预测	简单高效，适合空间分布分析	对初始值敏感，难以处理非球形分布
朴素贝叶斯	犯罪时空预测、犯罪类型预测	快速、可扩展，在特定条件下表现良好	假设特征独立，实际应用中可能不成立，对特征分布敏感
K 近邻算法	犯罪热点预测、犯罪类型预测、犯罪嫌疑人预测	简单易懂，无需模型假设，无需训练数据	对大数据集计算成本高，对不平衡数据和噪声数据敏感
神经网络（深度学习）	犯罪类型预测、犯罪热点预测、犯罪嫌疑人预测	强大的非线性建模能力，适用于复杂数据	模型黑箱化、计算成本高、对数据规模依赖强

表 4　预测场景分类及机器学习应用

预测场景	分类	特征
侵财案件	抢劫、盗窃（入室盗窃、盗三车等）	时空动态特征显著，受社会经济因素和环境变量影响，如人口密度、交通条件、商业活动密度等。
凶杀案件	行凶、杀人	数据稀缺，受社会经济变量（失业率、文盲率等）影响，复杂的非线性关系显著。
金融犯罪	金融诈骗、信用卡欺诈、公共采购欺诈、洗钱、贷款诈骗	高隐蔽性和技术性，涉及金融交易数据、时序模式、不平衡数据问题。
网络犯罪	网络诈骗、网络暴力、网络攻击	高度动态化，受技术手段影响显著，需考虑文本特征（如网络评论）和时序特征。

盗窃犯罪是侵财类案件中最常见的类型。近年来，随着电子支付的兴起与发展，盗窃犯罪数量总体呈下降趋势，但所占比例仍然较高，对警力资源的占用比例也较大。研究者针对盗窃类犯罪提出了多种预测方法。Yu[76]提出聚类置信率提升算法（CCRBoost），该算法通过整合多层加权 ESTP 模型，显著提高了盗窃案件的预测精度。Liu 等[115]采用多元贝叶斯空间建模方法，结合武汉市江汉区入室盗窃和非机动车辆盗窃案件的历史数据，完成了两类犯罪数量的预测，为不同类型案件的建模提供了参考。此外，Rummens 等[74]利用逻辑回归、神经网络和集成学习等方法，对入室盗窃和街头抢劫进行了预测，结果表明，不同算法在应对特定类型犯罪时具有不同的适用性，其中集成学习在捕捉复杂特征关系方面表现较好。

时空特征的挖掘是盗窃犯罪预测的重要环节。

Lin 等[72]通过谷歌 API 获取多达 84 种地理信息，构建了时空特征集，并将其应用于台湾桃园市盗窃案件的预测研究，验证了地理信息在提高模型性能方面的重要性。柳林等[116]对比了时空核密度估计法与随机森林模型，发现随机森林在不同周期的盗窃犯罪预测中表现更优，尤其在短期预测中能够更好地捕捉时空动态特征。

相比盗窃案件，抢劫犯罪因其直接威胁人身安全而社会危害性更大。抢劫案件的预测研究更多关注社会经济因素对案件分布的影响。Wheeler 等[117]通过将美国达拉斯市划分为 200×200 英尺的网格单元，结合公寓密度、商业零售活动等变量，利用随机森林算法对抢劫案件热点进行了预测，验证了将环境特征纳入模型的必要性。这种基于多因素综合分析的方法，不仅提高了预测的精准度，还为抢劫犯罪防控的策略制定提供了科学依据。

以侵财类案件为主的研究已经开始得到国内外学术界的关注，但在准确性方面还有待提升。未来的研究应进一步整合多源异构数据，优化算法性能，并关注模型的可解释性与实际应用场景的适配性，以推动侵财类案件犯罪预测在警务实践中的有效落地。

3.2 凶杀类案件犯罪预测

凶杀类案件是指以故意非法剥夺他人生命为核心行为的犯罪行为所构成的案件。该类案件性质极为严重，不仅直接损害公民的生命安全，而且对社会治安造成极大危害，引发社会恐慌情绪，严重阻碍社会的稳定与发展进程。与侵财类案件相比，凶杀类案件的研究相对较少。其原因主要包括凶杀案件的样本数据量较小，相关影响因素复杂，且相关数据的公开程度较低等，这些特点为研究者在建模和数据处理方面带来了较大挑战。

在凶杀案件犯罪预测的研究中，Rui 等[93]基于 NIBRS 数据库分析了一年多的凶杀案数据，采用决策树、随机森林、支持向量机和神经网络等方法对谋杀案的受害者与罪犯之间的关系进行了分类预测。研究表明，通过建立二分类模型可以获得较高的预测精度，其中支持向量机和随机森林在处理复杂关系特征时表现出较大的优势。这一研究揭示了机器学习方法在探索犯罪行为复杂关系中的潜力，但也表明模型的表现受限于特征变量的设计和数据质量。

Alves 等[118]通过随机森林来预测巴西某城市凶杀案的犯罪情况并量化城市指标对凶杀案的影响，同时对城市指标对犯罪的影响进行排序，指出并解释失业和文盲是影响巴西城市凶杀案的最重要的变量。这项研究强调了社会经济因素在凶杀案件发生中的作用，为政策制定提供了依据。Campedelli 等[119]对美国凶杀数据集进行了系统研究，使用并比较了包括 XGBoost、随机森林、支持向量机和神经网络在内的九种机器学习算法。结果显示，XGBoost 在总体预测性能上表现最佳，其优势在于能够高效处理不平衡数据和复杂的非线性关系。这一研究表明，基于梯度提升的算法在处理凶杀类案件预测时具有更好的适用性，尤其是在特征变量多样且分布不均的情况下。

凶杀类案件犯罪预测的研究不仅对于减少凶杀案件、保护公民安全具有重要意义，而且对于理解犯罪动机、预防犯罪行为提供了科学依据。尽管当前的研究已表明机器学习方法在凶杀类案件预测中的潜力，但仍存在一些限制需要进一步探索解决。例如，凶杀案的数据稀缺性限制了模型的泛化能力，而社会经济变量的时效性和完整性也影响了预测的准确性。因此，未来的研究应注重多源数据的融合，例如结合社会经济数据、犯罪行为数据以及犯罪现场的时空特征，通过多模态数据的集成建模提升预测的全面性和准确性。同时，在实际应用中，需平衡模型的复杂性与可解释性，确保其预测结果能够为执法部门和社会政策制定提供科学依据。

3.3 金融犯罪预测

金融犯罪被定义为违反刑法并导致金融损失的非暴力行为[120-121]，包括但不限于信用卡欺诈、公共采购欺诈、洗钱以及贷款诈骗等类型。金融犯罪影响市场稳定和社会发展，并且随着金融市场的发展与进步，金融犯罪尤其是金融诈骗类犯罪，在犯罪数量和犯罪金额上都呈现大幅上升趋势。相较于其他犯罪类型，金融犯罪具有高智商、高技术特征，并往往通过复杂的金融交易和信息技术手段实现，其隐蔽性和技术难度不仅增加了犯罪检测的挑战，也使传统的犯罪防控手段难以奏效。因此，探索数据驱动的科学预测方法，开展金融犯罪预测研究具有重要意义，可以帮助执法部门和金融机构提前发现潜在犯罪行为，从而提高风险管理的效率。

在金融犯罪预测中，信用卡欺诈检测是一个重要的研究领域。在过去的几十年里，信用卡的使用量不断增加，信用卡已经成为消费者频繁使用的一种支付手段。然而，随着信用卡的广泛使用，欺诈交易风险也不断增加，预防打击欺诈已变得十分重要。由于欺诈者通常有着高度适应能力，会通过调整行为模式以逃避检测，使得正常交易和欺诈交易的区分变得困难，即动态欺诈问题[122]。又因为信用卡数据集具有高度隐私性和不平衡性，信用卡欺诈预测问题长期以来吸引了研究者的关注。为了应对这些问题，多种机器学习方法被用于信用卡欺诈预测。人工神经网络[123]、朴素贝叶斯[124]、K 近邻[125]、支持向量机[126]、决策树[127]、集成学习[128]等均已在欺诈预测中被使用，并在一定程度上解决了动态欺诈问题和数据不平衡问题。2021 年，Lim 等[129]对信用卡欺诈预测领域的研究进行了综述，指出在信用卡欺诈预测中没有绝对最优的算法，需根据不同数据集选择合适算法，但机器学习算法相比仅静态匹配交易数据模式的规则系统算法在可靠性和适应性方面具有优势。

公共采购欺诈预测是另一个重要场景。公共采购是国家花费财政资金的过程包括采购商品、服务和工程等，涉及行业广泛，是国家经济中的一个重要部分。作为涉及财政支出的关键环节，公共采购的透明性和公平性直接影响国家经济利益。预测公共采购过程中的欺诈违法犯罪行为如腐败、勾结以及可疑投标等则对于提高采购流程的透明度、公平度和保护公共财政利益而言至关重要。研究者通过机器学习方法对招标文件、投标行为等数据进行分析，以识别腐败、勾结和可疑投标行为。Arief 等[130]在 2016 年研究了印度尼西亚电子公共采购平台中的欺诈行为，运用朴素贝叶斯、贝叶斯网络、神经网络、决策树算法，发现有监督学习适用于此类预测，但数据标签质量至关重要。Rabuzin 和 Modrusan 等[131-133]通过文本挖掘技术和机器学习方法从招标文件中提取数据建立可疑投标预测模型，为从文本数据角度进行金融犯罪预测提供了思路。Decarolis 等[134]通过 LASSO 回归、岭回归和随机森林分析了公共采购特征与腐败风险之间的关系，强调事前的特征筛选对提高预测模型性能的重要性。

洗钱是将犯罪所得非法收入转化为合法收入的过程，也是金融犯罪的一种。洗钱因其交易行为的隐蔽性和跨国性质，对犯罪预测提出了更高要求。Jayasree 等[135]提出基于位图索引的决策树模型（Bitmap Index-based Decision Tree, BIDT）对洗钱风险进行检测，BIDT 在真阳性率、假阳性率、风险识别时间和适应率方面都取得较优的结果。张成虎等[136]通过对外汇洗钱活动的相关特征分析，利用决策树模型建立了洗钱交易预测识别系统，为国内金融犯罪防控提供了实用参考。

此外，贷款诈骗风险的预测也是金融犯罪预测研究的重要组成部分。如王超[137]通过构建朴素贝叶斯模型、马尔可夫覆盖结构的贝叶斯网络模型和神经网络模型，对贷款诈骗风险进行了建模分析。这些模型在处理不同数据特征时表现出不同的适应性，展现了多模型融合在复杂场景中的应用潜力。

综上所述，金融犯罪预测结合了多种数据驱动方法，从信用卡欺诈、公共采购欺诈到洗钱和贷款诈骗，各类研究为这一领域提供了丰富的技术工具和理论支撑。现有研究表明，金融犯罪预测问题需根据数据的特性和研究的目标决定合适的预测模型。未来的研究应进一步探索多模型融合的方法，以提高预测的准确性和鲁棒性，同时加强对模型解释性的研究，以便更好地理解金融犯罪的复杂性，为政策制定提供更有力的支持。

3.4 网络犯罪预测

近年来互联网发展迅速，网络作为一把双刃剑，在给人们带来便利的同时也带来一系列的犯罪隐患，如网络诈骗、网络暴力等。英国首席警官协会（ACPO）和美国司法部（DOJ）将网络犯罪定义为由电子计算设备实施的任何犯罪[138]。网络类犯罪随着互联网和数字技术的迅速发展日益猖獗，其表现形式多样，隐蔽性强，且犯罪手段复杂多变，与传统犯罪相比具有跨地域性和高技术性。这些特性使网络犯罪的预测研究具有重要意义，不仅能够为执法部门提供技术支持，还可以为公众和企业提供更为有效的防护措施，减少因网络犯罪造成的经济损失和社会危害。

网络犯罪预测的研究场景中，针对不同犯罪类型的分类和识别是核心任务之一。Alves 等[118]使用推特数据开发了一个网络欺凌的预测模型，采用朴素贝叶斯、LibSVM、随机森林和 K 近邻等分类器，

通过分析社交媒体文本中的潜在欺凌行为，成功构建了高效的分类模型。类似地，Ch 等[139]研究了网络犯罪的三种主要类型——身份盗窃、版权攻击和黑客行为，通过逻辑回归、随机森林、支持向量机和多项式朴素贝叶斯进行分类预测，验证了机器学习方法在识别复杂网络犯罪模式中的应用价值。这些研究表明，基于社交媒体数据的文本挖掘技术能够有效捕捉犯罪线索，但其性能依赖于数据的质量和标注的准确性。

在综合性网络犯罪预测框架的研究中，Abbass 等[140]开发了一种针对社交媒体犯罪的分类框架，覆盖了网络跟踪、网络欺凌、网络黑客、网络攻击、骚扰和网络诈骗等多种犯罪行为。该框架通过多项式朴素贝叶斯、K 近邻和支持向量机方法对犯罪数据进行分类和预测，展示了多模型结合在应对复杂犯罪行为中的潜力。然而，尽管这些方法在数据有限的情况下表现出色，其扩展能力和适应性在面对海量实时数据时仍需进一步验证。

网络攻击是网络犯罪预测的另一重要领域，对个人、企业和国家安全均有重大影响。Deylami 等[141]通过支持向量机和 AdaBoost 算法，构建了一个专注于网络攻击检测和预防的预测模型。该模型通过分析 Facebook 数据集中的恶意代码活动，证明了集成学习方法在提高检测精度和降低误报率方面的优势。此外，Bilen[142]利用土耳其埃拉泽 5 年的真实网络犯罪数据，通过支持向量机预测网络攻击方法，取得了 95.02%的准确率。这些研究揭示了不同算法在处理不同任务时的适用性，同时强调了结合多种算法以提升预测精度的重要性。

尽管现有研究已表明机器学习方法在网络犯罪预测中的广泛应用潜力，但在实际应用中仍面临诸多挑战。例如，网络犯罪数据分布的不均衡性和标注成本高昂的问题限制了模型的训练质量。为了解决这些问题，Zhou 等[143]提出了一种基于 Bert 迁移学习的新型网络电信犯罪监测与预警模型，通过预训练模型迁移和高效数据标记实现了更高的分类精度。该方法在应对新型网络犯罪行为时表现尤为突出，进一步验证了深度学习模型在处理复杂文本数据中的强大能力。

总体来看，网络犯罪预测因其复杂性和动态性需要结合多种技术方法，不同模型在特定场景中各有适用性。基于传统机器学习的模型在结构化数据分析中表现稳定，而深度学习技术则凭借其强大的特征提取能力在非结构化和实时数据处理中展现了独特优势。未来的研究应进一步提升模型的扩展性和泛化能力，并探索与多源数据融合的可能性，以更全面地应对网络犯罪的多样性和复杂性。通过不断优化算法和丰富应用场景，网络犯罪预测技术将在保护信息安全和社会稳定方面发挥更大的作用。

4 总结与展望

综上所述，犯罪学理论的不断完善为犯罪预测研究奠定了坚实的理论基础。随着警务大数据的广泛应用，越来越多的学者致力于基于机器学习的犯罪预测研究。研究不仅聚焦于优化机器学习方法以提升其在犯罪预测中的表现，还探讨了机器学习在不同预测对象和场景中的具体应用。从方法角度来看，各类机器学习方法均具有自身的优势与局限，在犯罪预测中需根据具体问题场景选择适宜的算法。从预测对象角度分析，犯罪预测可细分为犯罪趋势预测、犯罪热点预测、犯罪时空预测、犯罪类型预测和犯罪嫌疑人预测，不同预测对象的内容、过程和方法各有侧重。从场景应用的角度看，当前研究多集中于侵财类案件的预测，其他如凶杀案、金融犯罪、网络犯罪等领域的研究还在进一步研究发展中。总体而言，基于机器学习的犯罪预测研究已经取得了一系列重要进展，但仍存在若干亟待突破的问题：

（1）犯罪数据稀疏性问题的解决。犯罪数据通常表现为本质稀疏，即大多数地点一天内发生的犯罪数为零，这使得模型在学习时容易将偶发犯罪误判为异常值，难以捕捉真实的时空规律。现有研究通过不考虑从未发生过犯罪的地区[72]、扩大预测单位面积[144]或缩小预测范围[144]等方式处理，但这些措施未根本缓解稀疏性带来的信息缺失问题。近年来，生成对抗网络（GAN）和图神经网络（GNN）被用于增强稀疏犯罪数据的表示能力。基于 GAN 的模型可通过生成虚拟样本实现数据增强，提高稀疏区域的预测精度[145]；而基于图结构学习的方法可利用空间邻接与关联信息，有效捕捉低频犯罪事件的潜在关系[146,147]。未来研究可结合 GAN 的数据生成能力与 GNN 的结构化特征传播机制，构建统一的稀疏数据增强与表示学习框架。

（2）犯罪预测方法的多样化与融合。各类机器

学习方法在犯罪预测中各具优势，但单一算法往往难以兼顾预测准确性与可解释性。未来研究可以尝试融合多种模型，如结合深度学习与统计学习方法，既提升预测性能，又增强结果的可解释性。此外，利用迁移学习在不同犯罪类型或区域之间共享知识，也是一个具有潜力的方向。

（3）深度学习的可解释性提升。深度学习在犯罪预测中的应用逐渐增加，但由于其“黑箱”特性，研究结果的可解释性始终是一个重要问题。未来研究可以引入可解释性技术，如注意力机制、特征重要性分析或可视化工具，揭示深度学习模型在处理犯罪数据时的内在机制，以提高模型的可信度与可接受性。

（4）多学科交叉研究与应用扩展。犯罪预测研究需要更多借鉴社会学、心理学与行为科学的理论与方法，结合犯罪动机、行为模式等因素提升预测能力。同时，应拓展应用场景，从传统的侵财类案件预测扩展到凶杀案、金融犯罪、网络犯罪等领域，以提高研究的全面性与实际价值。

（5）伦理与隐私保护。需注意，犯罪预测模型在实际应用中应严格遵守伦理与法律边界，避免对特定群体造成歧视、偏见或误判风险。模型的开发与使用应遵循“可解释、可审计、负责任”的原则，确保预测结果用于公共安全决策的科学辅助，而非个人行为的先验评判。未来研究应加强数据匿名化、隐私保护与算法公平性设计，推动犯罪预测技术在伦理可控的框架下健康发展。

总之，随着大数据与人工智能技术的快速发展，机器学习在犯罪预测中的应用将进一步深化。通过解决数据稀疏性、模型可解释性及伦理治理等关键问题，未来研究有望为社会治安防控提供更加科学、精准与负责任的技术支撑。

参考文献

[1] Jeffery C R. Crime prevention through environmental design[M]. CA:Sage, 1971.

[2] Cornish D B, Clarke R V. The reasoning criminal: rational choice perspectives on offending[M]. New York: Springer-Ver-lag, 1986.

[3] Cohen L E, Felson M. Social change and crime rate trends: A routine activity approach[J]. American Sociological Review, 1979, 44(4): 588-608.

[4] Brantingham P J, Brantingham P L. Patterns in crime[M]. New York: Macmillan, 1984.

[5] Brantingham P L, Brantingham P J. Environment, routine, and situation: toward a pattern theory of crime[J]. Routine Activity and Rational Choice, 1993, 5: 259-294.

[6] Farrell G, Pease K. Once bitten, twice bitten: Repeat victimisation and its implications for crime prevention[M]. London: Home Office Police Research Group, 1993.

[7] Townsley M. Infectious Burglaries. A test of the near repeat hypothesis[J]. British Journal of Criminology, 2003, 43(3): 615-633.

[8] Ellis L, Walsh A. Criminology: A global perspective[M]. Boston: Allyn and Bacon, 2000.

[9] Singh J P, Grann M, Fazel S. A comparative study of violence risk assessment tools: A systematic review and metaregression analysis of 68 studies involving 25,980 participants[J]. Clinical Psychology Review, 2011, 31(3): 499-513.

[10] Braga A A, Weisburd D L. The effects of focused deterrence strategies on crime: A systematic review and meta-analysis of the empirical evidence[J]. Journal of Research in Crime and Delinquency, 2012, 49(3): 323-358.

[11] Wand M P, Jones M C. Comparison of smoothing parameterizations in bivariate kernel density Estimation[J]. Journal of the American Statistical Association, 1993, 88(422): 520-528.

[12] Bowers K J, Johnson S D, Pease K. Prospective hot-spotting: the future of crime mapping? [J]. British Journal of Criminology, 2004, 44(5): 641-658.

[13] Chainey S, Tompson L, Uhlig S. The utility of hotspot mapping for predicting spatial patterns of crime[J]. Security Journal, 2008, 21(1): 4-28.

[14] Fielding M, Jones V. ‘Disrupting the optimal forager’: predictive risk mapping and domestic burglary reduction in Trafford, Greater Manchester[J]. International Journal of Police Science & Management, 2012, 14(1): 30-41.

[15] Caplan J M, Kennedy L W. Risk terrain modeling

compendium[J]. Rutgers Center on Public Security, Newark, 2011: 51.

[16] Caplan J M, Kennedy L W, Piza E L, et al. Using vulnerability and exposure to improve robbery prediction and target area selection[J]. Applied Spatial Analysis and Policy, 2020, 13(1): 113-136.

[17] Mohler G O, Short M B, Brantingham P J, et al. Self-exciting point process modeling of crime[J]. Journal of the American Statal Association, 2011, 106(493): 100-108.

[18] Reinhart A, Greenhouse J. Self-exciting point processes with spatial covariates: modelling the dynamics of crime[J]. Journal of the Royal Statal Society, 2018, 67(5): 1305-1329.

[19] Mohler G O, Short M B, Brantingham P J. The concentration-dynamics tradeoff in crime hot spotting[A]. Unraveling the crime-place connection[M]. New York: Routledge, 2017: 19-39.

[20] Short M B, Mohler G O, Brantingham P J, et al. Gang rivalry dynamics via coupled point process networks[J]. Discrete and Continuous Dynamical Systems Series B, 2014, 19(5): 1459-1477.

[21] Johnson S D, Bowers K J. The burglary as clue to the future: The beginnings of prospective hot-spotting[J]. European Journal of Criminology. 2004, 1(2): 237-255.

[22] 吴玲. 入室盗窃近重复现象研究及其警务应用[J]. 湖北警官学院学报, 2014, 27(8): 154-157.

[23] Farrell G, Phillips C, Pease K. Like taking candy-why does repeat victimization occur[J]. Brit. J. Criminology, 1995, 35: 384.

[24] Brantingham P J, Brantingham P L. The geometry of crime and crime pattern theory[M]//Environmental criminology and crime analysis. Routledge, 2016: 117-135.

[25] Wortley R K, Mazerolle L A. Environmental Criminology and Crime Analysis[M]. Devon: Willan Publishers, 2008.

[26] McKay, D Henry. Juvenile delinquency and urban areas: a study of rates of delinquents in relation to differential characteristics of local communities in American cities [M]. Chicago: University of Chicago Press, 1942.

[27] Hough M, Tilley N. Getting the grease to the squeak: Research lessons for crime prevention[M]. London: Home Office, 1998.

[28] Vigne N, Wartell J. Crime mapping case studies: Successes in the field[M]. Washington: Police Executive Research Forum, 1998.

[29] Harries K D. Mapping crime: Principle and practice[M]. Washington: US Department of Justice, Office of Justice Programs, National Institute of Justice, 1995.

[30] Goldsmith V, McGuire P G, Mollenkopf J B, et al. Analyzing crime patterns: Frontiers of practice[M]. London: Sage Publications, 1999.

[31] Chainey S, Ratcliffe J. GIS and crime mapping[M]. New Jersey: John Wiley & Sons Inc, 2005.

[32] Johnson S D, Bernasco W, Bowers K J, et al. Space-time patterns of risk: A cross national assessment of residential burglary victimization[J]. Journal of Quantitative Criminology, 2007, 23(3): 201-219.

[33] Johnson S D. Repeat burglary victimisation: A tale of two theories[J]. Journal of Experimental Criminology, 2008, 4(3): 215-240.

[34] Takahashi K, Kulldorff M, Tango T, et al. A flexibly shaped space-time scan statistic for disease outbreak detection and monitoring[J]. International Journal of Health Geographics, 2008, 7(14): 14-14.

[35] Short M B, Bertozzi A L, Brantingham P J. Nonlinear patterns in urban crime: Hotspots, bifurcations, and suppression[J]. SIAM Journal on Applied Dynamical Systems, 2010, 9(2): 462-483.

[36] Short M B, Brantingham P J, Bertozzi A L, et al. Dissipation and displacement of hotspots in reaction-diffusion models of crime[J]. Proceedings of the National Academy of Sciences, 2010, 107(9): 3961-3965.

[37] Short M B, D'orsogna M R, Pasour V B, et al. A statistical model of criminal behavior[J]. Mathematical Models and Methods in Applied Sciences, 2008, 18(1): 1249-1267.

[38] Cover T M, Hart P E. Nearest neighbor pattern classification[J]. IEEE Transactions on Information Theory, 1967, 13(1): 21-27.

[39] Friedman N, Geiger D, Goldszmidt M. Bayesian network classifiers[J]. Machine Learning, 1997, 29(2): 131-163.

[40] Vapnik V N, Chervoneva A Y. On class of perceptrons[J]. Automation and Remote Control, 1964, 25(1): 821-837.

[41] Hunt E B, Marin J, Stone P J. Experiments in induction[M]. New York: Wiley, 1966.

[42] Breiman L. Random Forests[J]. Machine Learning, 2001, 45(1): 5-32.

[43] Franklin J. The elements of statistical learning: data mining, inference and prediction[J]. The Mathematical Intelligencer, 2005, 27(2): 83-85.

[44] Hochreiter S, Schmidhuber J. Long Short-Term Memory[J]. Neural Computation, 1997, 9(8): 1735-1780.

[45] 魏智远. 刑事犯罪回归分析与数量预测[J]. 公安大学学报, 1993(1): 47－51.

[46] Zhang G P. Time series forecasting using a hybrid ARIMA and neural network model[J]. Neurocomputing, 2003, 50: 159-175.

[47] Gorr W, Olligschlaeger A, Thompson Y. Short-term forecasting of crime[J]. International Journal of Forecasting, 2003, 19(4): 579–594.

[48] 屈茂辉, 郝士铭. 基于 ARMA 模型的我国财产类犯罪人数预测研究[J]. 中国刑事法杂志, 2013(4): 100－106.

[49] Chen P, Yuan H, Shu X. Forecasting crime using the arima model[A]. 2008 Fifth International Conference on Fuzzy Systems and Knowledge Discovery[C]. Piscataway: IEEE, 2008, 5: 627-630.

[50] 侯苗苗, 胡啸峰. 基于时间序列模型 SARIMA 的犯罪预测研究[J]. 中国人民公安大学学报(自然科学版), 2021, 27(2): 67－73.

[51] Feng M, Zheng J, Ren J, et al. Big data analytics and mining for effective visualization and trends forecasting of crime data[J]. IEEE Access, 2019, 7(99): 106111-106123.

[52] 颜靖华,侯苗苗. 基于 LSTM 网络的盗窃犯罪时间序列预测研究[J]. 数据分析与知识发现, 2020, 4(11): 84-91.

[53] Butt UM, Letchmunan S, Hassan FH, Koh TW. Leveraging transfer learning with deep learning for crime prediction [J]. PLoS ONE, 2024, 19 (4): e0296486.

[54] Ivanyuk V. Forecasting of digital financial crimes in Russia based on machine learning methods[J]. Journal of Computer Virology and Hacking Techniques, 2024, 20: 349–362.

[55] Bappee FK, Soares A, Petry LM, Matwin S. Examining the impact of cross-domain learning on crime prediction[J]. Journal of Big Data, 2021, 8 (1): 1 - 27.

[56] 黄娜, 何泾沙, 孙靖超, 等. 基于改进 LSTM 网络的犯罪态势预测方法[J]. 北京工业大学学报, 2019, 45(8): 742-748.

[57] Gao Y, Yin D, Zhao X, et al. Prediction of Telecommunication Network Fraud Crime Based on Regression‐LSTM Model[J]. Wireless Communications and Mobile Computing, 2022, 2022(1): 3151563.

[58] Biswas A A, Basak S. Forecasting the trends and patterns of crime in bangladesh using machine learning model[A]. 2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT)[C]. Piscataway: IEEE, 2019: 114-118.

[59] 于红志, 刘凤鑫, 邹开其. 改进的模糊 BP 神经网络及在犯罪预测中的应用[J]. 辽宁工程技术大学学报(自然科学版), 2012, 31(02): 244-247.

[60] Gallison J K, Andresen M A. Crime and public transportation: a case study of Ottawa's O-Train system[J]. Canadian Journal of Criminology and Criminal Justice, 2017, 59(1): 94-122.

[61] Kianmehr K, Alhajj R. Crime hot-spots prediction using support vector machine[A]. IEEE International Conference on Computer Systems and Applications[C]. Los Alamitos: IEEE Computer Society, 2006: 952-959.

[62] Kianmehr K, Alhajj R. Effectiveness of support vector machine for crime hot-spots prediction[J]. Applied Artificial Intelligence, 2008, 22(5): 433-458.

[63] Guevara C, Santos M. Crime prediction for patrol routes generation using machine learning[A]. Computational Intelligence in Security for Information Systems Conference[C]. Cham: Springer, 2019: 97-107.

[64] 石汝楠, 王聪. 基于改进 K-means 算法的犯罪预测模型[J]. 警学研究, 2021(02): 51-60.

[65] Kouziokas G N. The application of artificial intelligence in public administration for forecasting high crime risk transportation areas in urban environment[J]. Transportation Research Procedia, 2017, 24: 467-473.

[66] Sathyadevan S, Devan M S, Gangadharan S S. Crime analysis and prediction using data mining[A]. 2014 First International Conference on Networks & Soft Computing (ICNSC2014)[C]. Piscataway: IEEE, 2014: 406-412.

[67] Emmanuel A, Elisha O O, Danison T, et al. Crime prediction using decision tree (J48) classification algorithm[J]. International Journal of Computer and Information Technology, 2017, 6(3): 188-195.

[68] Bogomolov A, Lepri B, Staiano J, et al. Once upon a crime: towards crime prediction from demographics and mobile data[C]. Proceedings of the 16th international conference on multimodal interaction, 2014: 427-434.

[69] Huang Y Y, Li C T, Jeng S K. Mining location-based social networks for criminal activity prediction[A]. 2015 24th Wireless and Optical Communication Conference (WOCC)[C]. Piscataway: IEEE, 2015: 185-189.

[70] Kadar C, Maculan R, Feuerriegel S. Public decision support for low population density areas: An imbalance-aware hyper-ensemble for spatio-temporal crime prediction[J]. Decision Support Systems, 2019, 119: 107-117.

[71] Zhang Q, Yuan P, Zhou Q, et al. Mixed spatial-temporal characteristics based crime hot spots prediction[A]. 2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD)[C]. Piscataway: IEEE, 2016: 97-101.

[72] Lin Y L, Yen M F, Yu L C. Grid-based crime prediction using geographical features[J]. ISPRS International Journal of Geo-Information, 2018, 7(8): 298-314.

[73] 沈寒蕾, 张虎, 张耀峰, 等. 基于长短期记忆模型的入室盗窃犯罪预测研究[J]. 统计与信息论坛, 2019, 34(11): 107-115.

[74] Rummens A, Hardyns W, Pauwels L. The use of predictive analysis in spatiotemporal crime forecasting: Building and testing a model in an urban context[J]. Applied Geography, 2017, 86: 255-261.

[75] Zhuang Y, Almeida M, Morabito M, et al. Crime hot spot forecasting: A recurrent model with spatial and temporal information[A]. 2017 IEEE International Conference on Big Knowledge (ICBK)[C]. Piscataway: IEEE, 2017: 143-150.

[76] Yu C H, Ding W, Chen P, et al. Crime forecasting using spatio-temporal pattern with ensemble learning[A]. Pacific-Asia Conference on Knowledge Discovery and Data Mining[C]. Cham: Springer, 2014: 174-185.

[77] Zhang X, Liu L, Xiao L, et al. Comparison of machine learning algorithms for predicting crime hotspots[J]. IEEE Access, 2020, 8: 181302-181310.

[78] Kipf T N, Welling M. Semi-supervised classification with graph convolutional networks[J]. arXiv preprint arXiv:1609.02907, 2016.

[79] Qian Y, Pan L, Wu P, et al. GeST: A grid embedding based spatio-temporal correlation model for crime prediction[A]. 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC)[C]. Piscataway: IEEE, 2020: 1-7.

[80] 肖延辉, 王欣, 冯文刚, 等. 基于长短记忆型卷积神经网络的犯罪地理位置预测方法[J]. 数据分析与知识发现, 2018, 2(10): 15-20.

[81] Rumi S K, Deng K, Salim F D. Crime event prediction with dynamic features[J]. EPJ Data Science, 2018, 7(1): 43-70.

[82] Huang C, Zhang J, Zheng Y, et al. DeepCrime: Attentive hierarchical recurrent networks for crime prediction[A]. Proceedings of the 27th ACM International Conference on Information and Knowledge Management[C]. New York: ACM, 2018: 1423-1432.

[83] Wang Y, Ge L, Li S, et al. Deep temporal multi-graph convolutional network for crime prediction[A]. International Conference on Conceptual Modeling[C]. Cham: Springer, 2020: 525-538.

[84] Mao Y, Yin L, Zeng M, et al. Review of Empirical Studies on Relationship between Street Environment and Crime[J]. Journal of Planning Literature, 2021, 36(2): 187-202.

[85] Lu Y, Chen X. On the false alarm of planar K-function when analyzing urban crime distributed along streets[J]. Social science research, 2007, 36(2): 611-632.

[86] Rosser G, Davies T, Bowers K J, et al. Predictive crime mapping: arbitrary grids or street networks?[J]. Journal of Quantitative Criminology, 2017, 33(3): 569-594.

[87] Zhang Y, Cheng T. Graph deep learning model for network-based predictive hotspot mapping of sparse spatio-temporal events[J]. Computers Environment and Urban Systems, 2019, 79.

[88] Baculo M J C, Marzan C S, de Dios Bulos R, et al. Geospatial-temporal analysis and classification of criminal data in manila[A]. 2017 2nd IEEE International Conference on Computational Intelligence and Applications (ICCIA)[C]. Piscataway: IEEE, 2017: 6-11.

[89] Alparslan Y, Panagiotou I, Livengood W, et al. Perfecting the Crime Machine[J]. arXiv preprint arXiv:2001.09764, 2020.

[90] Wu S, Wang C, Cao H, et al. Crime prediction using data mining and machine learning[A]. International Conference on Computer Engineering and Networks[C]. Cham: Springer, 2018: 360-375.

[91] Almanie T, Mirza R, Lor E. Crime prediction based on crime types and using spatial and temporal criminal hotspots[J]. Computer Science, 2015, 5(4): 1-19.

[92] Iqbal R, Murad M A A, Mustapha A, et al. An experimental study of classification algorithms for crime prediction[J]. Indian Journal of Science and Technology, 2013, 6(3): 4219-4225.

[93] Rui Y, Olafsson S. Classification for predicting offender affiliation with murder victims[J]. Expert Systems with Applications, 2011, 38(11): 13518-13526.

[94] Nguyen T T, Hatua A, Sung A H. Building a learning machine classifier with inadequate data for crime prediction[J]. Journal of Advances in Information Technology Vol, 2017, 8(2): 3-9.

[95] Vural M S, Gök M. Criminal prediction using Naive Bayes theory[J]. Neural Computing and Applications, 2017, 28(9): 2581-2592.

[96] Mohan A, Dhir R, Hirashkar H, et al. Matching witness' account with mugshots for forensic applications[A]. 2018 Eleventh International Conference on Contemporary Computing (IC3)[C]. Piscataway: IEEE, 2018: 1-5.

[97] Burgess E W. Factors determining success or failure on parole[J]. The workings of the indeterminate sentence law and the parole system in Illinois, 1928: 221-234.

[98] Caulkins J, Cohen J, Gorr W, et al. Predicting criminal recidivism: A comparison of neural network models with statistical methods[J]. Journal of Criminal Justice, 1996, 24(3): 227-240.

[99] Schmidt P, Witte A D. Predicting Recidivism Using Survival Models[J]. Contemporary Sociology, 1989, 18(2): 245.

[100] Schmidt P, Witte A D. Predicting criminal recidivism using ‘split population’ survival time models[J]. Journal of Econometrics, 1989, 40(1): 141-159.

[101] Brodzinski J D, Crable E A, Scherer R F. Using artificial intelligence to model juvenile recidivism patterns[J]. Computers in Human Services, 1994, 10(4): 1-18.

[102] Palocsay S W, Wang P, Brookshire R G. Predicting criminal recidivism using neural networks[J]. Socio-Economic Planning Sciences, 2000, 34(4): 271-284.

[103] Wang P, Mathieu R, Ke J, et al. Predicting criminal recidivism with support vector machine[A]. 2010 International Conference on Management and Service Science[C]. Piscataway: IEEE, 2010: 1-9.

[104] Tollenaar N, Van der Heijden P G M. Which method predicts recidivism best?: a comparison of statistical, machine learning and data mining predictive models[J]. Journal of the Royal Statistical Society, 2013, 176(2): 565-584.

[105] Rossmo D K. Geographic profiling: Target patterns of serial murderers[D]. Theses (School of Criminology)/Simon Fraser University, 1995.

[106] Snook B, Taylor P J, Bennell C. Shortcuts to Geographic Profiling Suces: A Reply to Rosmo (2005)[J].Applied Cognitive Psychology, 2005, 19(5): 655-661.

[107] Levine N, CrimeStat I. A spatial statistics program for the analysis of crime incident locations[J]. National Institute of Justice, 2000, 25(2): 162-168.

[108] Shiode S, Shiode N, Block R, et al. Space-time characteristics of micro-scale crime occurrences: an application of a network-based space-time search window technique for crime incidents in Chicago[J]. International Journal of Geographical Information Science, 2015, 29(5-6): 697-719.

[109] Song C, Koren T, Wang P, et al. Modelling the scaling properties of human mobility[J]. Nature physics, 2010, 6(10): 818-823.

[110] 方嘉良, 李卫红. 犯罪嫌疑人落脚点预测模型改进研究——基于地理环境因素与 CGT 模型组合方法[C]. //2016 中国地理信息科学理论与方法学术年会论文集. 2016: 1-8.

[111] 李卫红, 戴侃, 闻磊. 顾及地理因素的犯罪地理目标模型改进方法[J]. 测绘科学, 2015, 40(7): 86-91.

[112] Duan L, Ye X, Hu T, et al. Prediction of suspect location based on spatiotemporal semantics[J]. ISPRS International Journal of Geo-Information, 2017, 6(7): 185.

[113] 姜丁菊, 刘学文, 姜晓雪. 基于聚类的恐袭事件嫌疑人与可疑据点预测[J]. 重庆工商大学学报：自然科学版, 2019, 36(3): 6.

[114] Butt U M, Letchmunan S, Hassan F H, et al. Spatio-temporal crime hotspot detection and prediction: A systematic literature review[J]. IEEE Access, 2020, 8: 166553-166574.

[115] Liu H, Zhu X. Joint modeling of multiple crimes: A bayesian spatial approach[J]. ISPRS International Journal of Geo-Information, 2017, 6(1): 16-32.

[116] 柳林, 纪佳楷, 宋广文, 等. 基于犯罪空间分异和建成环境的公共场所侵财犯罪热点预测[J]. 地球信息科学学报, 2019, 21(11): 1655-1668.

[117] Wheeler A P, Steenbeek W. Mapping the risk terrain for crime using machine learning[J]. Journal of Quantitative Criminology, 2021, 37(2): 445-480.

[118] Alves L G A, Ribeiro H V, Rodrigues F A. Crime prediction through urban metrics and statistical learning[J]. Physica A: Statistical Mechanics and its Applications, 2018, 505: 435-443.

[119] Campedelli G M. Explainable machine learning for predicting homicide clearance in the United States[J]. Journal of criminal justice, 2022, 79: 101898.

[120] Sudjianto A, Nair S, Yuan M, et al. Statistical methods for fighting financial crimes[J]. Technometrics, 2010, 52(1): 5-19.

[121] Pickett K H S, Pickett J M. Financial crime investigation and control[M]. Hoboken: John Wiley & Sons, 2002.

[122] Mena J. Investigative data mining for security and criminal detection[M]. Butterworth-Heinemann, 2003.

[123] Serrano A, Costa J, Cardonha C, et al. Neural Network Predictor for Fraud Detection: A Study Case for the Federal Patrimony Department[A]. The Seventh International Conference on Forensic Computer Science[C]. 2012.

[124] Kiran S, Guru J, Kumar R, et al. Credit card fraud detection using Naïve Bayes model based and KNN classifier[J]. International Journal of Advance Research, Ideas and Innovations in Technoloy, 2018, 4(3): 44-47.

[125] Sudha C, Raj T N. Credit card fraud detection in internet using k-nearest neighbor algorithm[J]. Int. J. Comput. Sci, 2017, 5: 22-30.

[126] Abdelhamid D, Khaoula S, Atika O. Automatic bank fraud detection using support vector machines[A]. The International Conference on Computing Technology and Information Management (ICCTIM)[C]. Society of Digital Information and Wireless Communication, 2014: 10.

[127] Gaikwad J R, Deshmane A B, Somavanshi H V, et al. Credit card fraud detection using decision tree induction algorithm[J]. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2014, 4(6): 66-69.

[128] Sohony I, Pratap R, Nambiar U. Ensemble learning for credit card fraud detection[A]. Proceedings of the ACM India Joint International Conference on Data Science and Management of Data[C]. 2018: 289-294.

[129] Lim K S, Lee L H, Sim Y W. A review of machine learning algorithms for fraud detection in credit card transaction[J]. International Journal of Computer Science & Network Security, 2021, 21(9): 31-40.

[130] Arief H A, Saptawati G A P, Asnar Y D W. Fraud detection based-on data mining on Indonesian E-Procurement System (SPSE)[A]. 2016 International Conference on Data and Software Engineering (ICoDSE)[C]. IEEE, 2016: 1-6.

[131] Rabuzin K, Modrusan N. Prediction of Public Procurement Corruption Indices using Machine Learning Methods[A]. KMIS[C]. 2019: 333-340.

[132] Modrusan N, Rabuzin K, Mrsic L. Improving Public Sector Efficiency using Advanced Text Mining in the Procurement Process[A]. DATA[C]. 2020: 200-206.

[133] Rabuzin K, Modrušan N, Križanić S, et al. Process Mining in Public Procurement in Croatia[A]. Industrial Innovation in Digital Age[C]. Springer, Cham, 2022: 473-480.

[134] Decarolis F, Giorgiantonio C. Corruption red flags in public procurement: new evidence from Italian calls for tenders[J]. EPJ Data Science, 2022, 11(1): 16.

[135] Jayasree V, Balan R V S. Money laundering regulatory risk evaluation using bitmap index-based decision tree[J]. Journal of the Association of Arab Universities for Basic and Applied Sciences, 2017, 23: 96-102.

[136] 张成虎, 赵小虎. 基于决策树算法的洗钱交易识别研究[J]. 武汉理工大学学报, 2008, 30(2): 154-156.

[137] 王超. 金融犯罪之人工智能预防路径研究——以贷款诈骗风险智能建模预测为分析路径[J]. 河南警察学院学报, 2019, 28(2): 27-33.

[138] Brar H S, Kumar G. Cybercrimes: A proposed taxonomy and challenges[J]. Journal of Computer Networks and Communications, 2018, 2018.

[139] Ch R, Gadekallu T R, Abidi M H, et al. Computational system to classify cyber crime offenses using machine learning[J]. Sustainability, 2020, 12(10): 4087.

[140] Abbass Z, Ali Z, Ali M, et al. A framework to predict social crime through twitter tweets by using machine learning[A]. 2020 IEEE 14th International Conference on Semantic Computing (ICSC)[C]. IEEE, 2020: 363-368.

[141] Deylami H M, Singh Y P. Adaboost and SVM based cybercrime detection and prevention model[J]. Artificial Intelligence Research, 2012, 1(2): 117-130.

[142] Bilen A, Özer A B. Cyber-attack method and perpetrator prediction using machine learning algorithms[J]. PeerJ Computer Science, 2021, 7: e475.

[143] Zhou S, Wang X, Yang Z. Monitoring and early warning of new cyber-telecom crime platform based on BERT migration learning[J]. China Communications, 2020, 17(3): 140-148.

[144] Kanoga S, Kawai N, Takaoka K. Deep neural networks for grid-based elusive crime prediction using a private dataset obtained from Japanese municipalities[A]. International Conference on Applied Human Factors and Ergonomics[C]. Cham: Springer, 2020: 105-112.

[145] Jin G, Wang Q, Zhao X, et al. Crime-GAN: A context-based sequence generative network for crime forecasting with adversarial loss[A]. 2019 IEEE International Conference on Big Data (Big Data)[C]. IEEE, 2019: 1460-1469.

[146] Li Z, Huang C, Xia L, et al. Spatial-temporal hypergraph self-supervised learning for crime prediction[A]. 2022 IEEE 38th international conference on data engineering (ICDE)[C]. IEEE, 2022: 2984-2996.

[147] Wang C, Lin Z, Yang X, et al. Hagen: Homophily-aware graph convolutional recurrent network for crime forecasting[A]. Proceedings of the AAAI Conference on Artificial Intelligence[C]. 2022, 36(4): 4193-4200.