生成式人工智能驱动下电信网络诈骗风险演化实证研究

周胜利[1,2]，徐睿[2]，陈庭贵[3]，汪邵杰[1]，王镇波[1]
（1. 浙江警察学院信息网络安全学院，浙江 杭州 310053；
2. 杭州电子科技大学网络空间安全学院，浙江 杭州 310018；
3. 浙江工商大学统计与数学学院，浙江 杭州 310018）

摘　要：利用知识图谱与事理图谱技术对生成式人工智能驱动下的电信网络诈骗案件进行实证研究，可以更直观地回溯受骗过程中风险的演化方式，对新型电信网络诈骗反制预警具有重要意义。基于利用生成式人工智能实施的电信网络诈骗案件数据，首先，进行语义角色标注和依存句法分析；然后，通过事件元素识别和事件关系抽取，构建案件知识图谱和事理图谱；最后，结合数理统计和图谱技术分析电信网络诈骗风险演化的关键环节和演化模式。研究表明，嫌疑人借助生成式人工智能技术能更有效地利用证真偏差现象，博取受害人的信任；生成式人工智能驱动下电信网络诈骗风险的演化模式可分为3类，长链型演化模式反映了案件中的完整风险事件及事件间的演化过程，星型和复合型演化模式反映了同类案件中存在的不同风险行为模式及核心风险事件节点，能为制定更加科学合理的电信网络诈骗治理对策提供理论依据。

关键词：生成式人工智能；电信网络诈骗；知识图谱；事件元素识别；深度聚类
中图分类号：D631.2
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2025135

Empirical study on the evolution of telecom fraud risks driven by artificial intelligence generated content

ZHOU Shengli[1,2], XU Rui[2], CHEN Tinggui[3], WANG Shaojie[1], WANG Zhenbo[1]
1. School of Information Network Security, Zhejiang Police College, Hangzhou 310053, China
2. School of Cyberspace Security, Hangzhou Dianzi University, Hangzhou 310018, China
3. School of Statistics and Mathematics, Zhejiang Gongshang University, Hangzhou 310018, China

Abstract: The application of knowledge graph and eventic graph technologies in the empirical study of telecom fraud cases driven by artificial intelligence generated content (AIGC) allows for a more intuitive tracing of the evolution of risks during the victimization process, which is of great significance for countering and early warning of new types of telecom fraud. Based on data from telecom fraud cases implemented using AIGC, semantic role labeling and dependency parsing were firstly performed during data preprocessing. Then, event element recognition and event relationship extraction were constructed to construct knowledge graphs and eventic graphs of the cases. Finally, the key

收稿日期：2025−03−09；修回日期：2025−05−14
基金项目：国家社会科学基金资助项目（No.23BGL272）
Foundation Item: The National Social Science Foundation of China (No.23BGL272)

stages and patterns of the evolution of telecom fraud risks were analyzed by combining mathematical statistics with graph technologies. The research revealed that, suspects using AIGC were able to more effectively exploit the phenomenon of confirmation bias to gain the victim's trust. The evolution patterns of telecom fraud risks driven by AIGC were categorized into three types: the long-chain type evolution pattern systematically identifies complete risk events and their inter-event evolutionary trajectories within cases, while investigation of the star-shaped and composite type evolution patterns enable recognition of divergent risk behavioral patterns and localization of core risk event nodes across homogeneous case clusters, there by establishing a theoretical foundation for developing scientifically rational governance strategies in telecom fraud countermeasures.

Key words: artificial intelligence generated content, telecom fraud, knowledge graph, event element recognition, deep clustering

0 引言

随着大数据、云计算、人工智能（artificial intelligence，AI）等新兴技术的快速发展，电信网络诈骗犯罪手法的科技化、智能化水平越来越高。在生成式人工智能等新技术的加持下，犯罪模式也在不断演进升级，导致相关犯罪的打击和防范工作难度不断增大，当前电信网络诈骗犯罪态势仍然严峻，人民群众的生命财产安全依然受到严重威胁。对此，本文基于某市级区域内与生成式人工智能相关的电信网络诈骗案件数据，分析案件中受害人信息及诈骗过程文本信息，分别构建案件知识图谱与案件事理图谱，再结合数理分析、拓扑分析等方法对诈骗过程中的风险关键要素进行挖掘，揭示生成式人工智能驱动下电信网络诈骗风险的演进特征，为打击和防范电信网络诈骗工作提供参考。

1 国内外相关研究

知识图谱最早由谷歌提出，现已广泛应用于信息检索、知识管理等领域[1]。知识图谱研究主要包括图谱构建技术与图谱实践应用两个部分。在图谱构建技术方面，Zhang 等[2]指出，在基于知识图谱根据三元组头实体与关系预测尾实体时，头实体与尾实体为相互决定关系，因此需引入交互矩阵来表示实体与向量间的关系。Chen 等[3]提出一种基于知识协同优化的调优方法，学习虚拟答案词、类型词等提示性知识，并在学习过程中植入实体关系约束来实现提示知识的构建与优化，进而提升任务间的感知能力。在图谱实践应用方面，Opdahl 等[4]提出知识图谱可以应用于统筹不同格式的新闻内容，进而为新闻的制作分发与消费提供借鉴。Simms 等[5]提出将知识图谱应用于新冠病毒疫情防控中，通过知识图谱对复杂、非结构化的疫苗数据进行建模，有效解决了疫苗研制中的知识分析问题。冯钧等[6]提出以知识图谱处理非结构化的水利文本数据，分层高效完成了水利数据的实例抽取与图谱构建，推动水利科学的智能决策。

知识图谱主要用于描述实体、属性以及实体关系等静态和确定的事实，但在表示事物的逻辑演化过程方面存在不足[7]。因此，有研究者提出了事理图谱，用于描述事件之间的演化规律和模式[8]。目前，事理图谱的构建理论研究仍在探索中，如熊凯等[9]提出了一个基于知识增强的预训练语言模型来进行文本推理的框架，充分发挥事理图谱的图结构逻辑进行脚本事件预测，拓展了事理图谱在自然语言处理中的功能。翟利志等[10]提出事理图谱的构建需要结合逻辑关系形成复合语义特征的知识网络，利用事理图谱抽象事件间的逻辑关系表示事件演化规律。此外，还有部分研究利用事理图谱对事件的演化规律进行分析，

例如，杨纪星等[11]面向金融领域热点事件构建事理图谱，通过制定句法分析方案并提出序列标识定义构建图谱，分析金融事件的演变与扩散规律；宁慧涵等[12]将事理图谱应用于事故灾难分析，在事件抽取后采用关系识别的方法获取事件关系，从而实现对事故后时空变化与事故演化过程的展示，为事故救险提供参考；周林兴等[13]将事理图谱应用于网络舆情的诱发与缓解机制研究，对事理图谱进行动因分析与路径提取，提升了相关机制规律的解析深度。

综上所述，当前对图谱技术的相关研究主要从知识图谱与事理图谱两个维度展开。知识图谱的研究相对更成熟，而事理图谱的核心技术及实践应用尚处于探索阶段。针对传统电信网络诈骗（本文指没有利用生成式人工智能技术实施的电信网络诈骗，如信贷理财诈骗、“杀猪盘”等），现有的大部分研究工作主要从统一资源定位符（uniform resource locator，URL）[14]、网络流量行为[15-16]等方面提取被害特征[17]，进而对诈骗行为风险进行识别；或从心理特征[18]、社会经济特征[19]等方面探索相关风险因素对电信网络诈骗的影响，并总结相应的防治手段[20]。此外，当前针对生成式人工智能的研究主要集中于风险分析[21-22]及相关治理体系的构建[23]。对生成式人工智能驱动下的电信网络诈骗风险演进规律的研究整体较少，且主要使用基于专家经验判断的定性推演模式[24]进行分析，存在分析方法缺乏实证数据支撑、研究结论时效性不足等问题，导致风险演化模式的推断结论存在一定的主观偏差。为此，本研究基于电信网络诈骗的真实案件数据和图谱技术，构建生成式人工智能驱动下的电信网络诈骗案件知识图谱与事理图谱，更准确地揭示电信网络诈骗风险的演进规律，并为相关部门开展新型电信网络诈骗防治工作提供理论基础与决策支撑。

2　知识图谱与事理图谱构建方法

生成式人工智能驱动下的电信网络诈骗风险图谱构建流程如图 1 所示。首先，对利用生成式人工智能实施的电信网络诈骗案件数据进行预处理，获取结构化的案件相关数据（包括案件类型、案件名称、人口属性特征等）和非结构化的受骗过程文本数据；然后，针对非结构化的文本数据，通过事件元素识别与事件关系抽取处理，得到事件元素数据与事件关系三元组数据；接着，基于人口属性数据和事件元素数据构建案件知识图谱；再通过研究设计的CTCM-V&G模型对事件关系三元组中的事件进行泛化处理，并构建对应的案件事理图谱；最后，基于构建的案件知识图谱与事理图谱，通过数理统计分析、事理图谱分析和拓扑特征分析，对生成式人工智能驱动下电信网络诈骗风险演化的关键环节与模式特征进行分析。

2.1　数据预处理

对于利用生成式人工智能实施的电信网络诈骗案件数据中的案件记录文本数据，使用语言技术平台（language technology platform，LTP）[25]

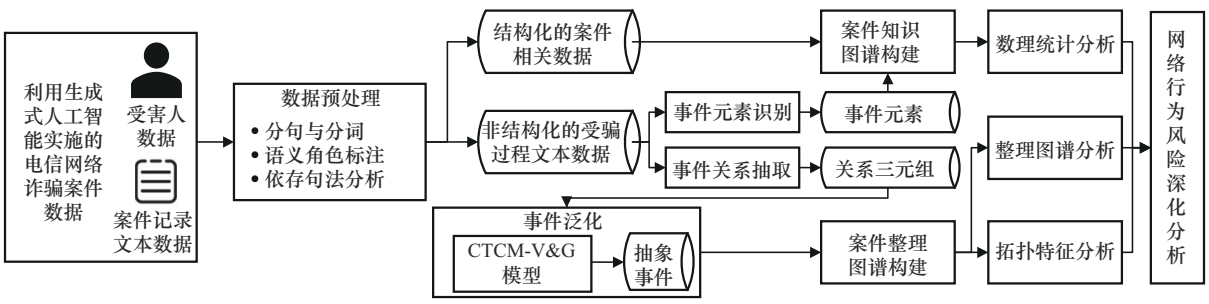

图 1　生成式人工智能驱动下的电信网络诈骗风险图谱构建流程

进行预处理，包括分词与分句、语义角色标注和依存句法分析，最后形成图谱构建所需的语料数据，为后续数据处理操作提供基础。

2.1.1 分句与分词

分句任务主要通过识别常见的分句标点符号（如句号、感叹号等），将长文本转化为单句形式。分词则是将原始文本进行分句后，再将每一个单句分割成词语的集合。分词与分句任务的实现为后续预处理任务奠定基础。

2.1.2 语义角色标注

语义角色是指词在句子中所扮演的角色，例如主语、宾语、状语等。语义角色标注（semantic role labeling，SRL）旨在识别句子中的语义角色，并将它们与每个谓词（动词或形容词）相关联。LTP中语义角色标注的标签见表1。

表1 LTP中语义角色标注标签

标签	描述	例子
A0	施事者、主体、触发者	[嫌疑人A0]鼓励受害人投资
A1	受事者	嫌疑人鼓励[受害人A1]投资
ADV	状语	受害人[将能ADV]提现
CND	条件	[如果不验证CND]，会影响征信记录
LOC	地点	受害人[在××市LOC]收到信息

2.1.3 依存句法分析

依存句法分析会解析句子中词之间的依存关系，即词与词之间的句法关系，如主谓关系、动宾关系等。依存句法关系示例见表2。通过语义角色标注和依存句法分析可以更深入地理解文本的语义，为后续事件元素识别等操作提供基础。

表2 依存句法关系示例

关系类型	标签	例子
主谓关系	SBV	嫌疑人要求受害人下载App (嫌疑人←要求)
动宾关系	VOB	嫌疑人要求受害人下载App (要求←下载)
动补结构	CMP	按照要求做完了相应操作(做→完)
介宾关系	POB	按照要求做完了相应操作(按照→要求)
定中关系	ATT	按照要求做完了相应操作(相应←操作)

2.2 事件元素识别

事件元素识别将包含事件信息的文本进行解析和结构化，并从中提取关键的事件信息，如相关人物、时间、地点、行动以及产生的影响等。研究从电信网络诈骗案件数据集的非结构化文本数据中抽取主谓宾事件和谓宾事件的元素三元组[主体，行动（谓词），客体]，抽取方法如算法1与算法2所示。

算法1 主谓宾事件元素识别

输入 事件文本text

输出 事件元素三元组triplets

```
if 'SBV' in text and 'VOB' in text: #检查是否存在 'SBV' 和 'VOB' 关系
    subject, predicate, object = Extractor(text)#提取事件元素
    Add_To_Triplets(subject, predicate, object, triplets)#将元素加入三元组
if 'SBV' in text and 'CMP' in text: #检查是否存在 'SBV' 和 'CMP' 关系
    subject, predicate, object = Extractor(text)
    Add_To_Triplets(subject, predicate, object, triplets)
if 'ATT' in text: #检查是否存在 'ATT' 关系
    subject, predicate, object = Extractor(text)
    if predicate + object in subject:
        subject = subject. replace (predicate + object, "")
Add_To_Triplets(subject, predicate, object, triplets)
return triplets #返回提取的事件元素三元组
```

算法2 谓宾事件元素识别

输入 事件文本text

输出　事件元素三元组 triplets

predicate = ExtractPredicate(text)# 提取谓词

if 'A0' in roles and 'A1' in roles: #检查是否存在 'A0'和 'A1' 标签

subject = ExtractRole(roles['A0'])# 'A0'标签设置为主体

object = ExtractRole(roles['A1']) # 'A1'标签设置为客体

Add_To_Triplets(subject, predicate, object, triplets)

else if 'A0' in roles or A1' in roles: #检查是否只存在'A0'或'A1'标签

subject = ExtractRole(roles['A0']) or "none"

object = "none" or ExtractRole(roles['A1']) #不存在标签的在三元组中置空

Add_To_Triplets(subject, predicate, object, triplets)

return triplets #返回提取的事件元素三元组

其中，算法 1 描述了基于依存句法分析结果对以谓语为中心的事件元素三元组进行提取的步骤；算法 2 描述了基于语义角色标注结果对主谓宾结构的事件元素三元组进行提取的步骤。利用两种算法提取的事件元素三元组将用于构建案件知识图谱。

2.3　事件关系提取

通过事件元素识别能有效地提取电信网络诈骗案件中所包含的元素，加强对电信网络诈骗构成要素的认知，但较难从中解析出电信网络诈骗风险的演进方式，仍须进一步通过事件关系抽取来分析电信网络诈骗案件中风险的演化规律。常见的关系事件抽取方法包括基于深度学习的方法（如 BiLSTM-CRF[26]）和基于模式匹配[27]的方法。当前带标注的利用生成式人工智能实施的电信网络诈骗犯罪案件语料数据较为稀缺，而基于深度学习的方法需要准备大量带标注的语料数据来保证准确性，因此，本文利用基于模式匹配的方法提取关系事件。同时，为聚焦风险演化的核心因果链与时序关系，制定了包含因果关系和顺承关系的事件关系提取规则模板，见表 3，用于提取事件关系三元组[前事件，关系，后事件]。

表 3　事件关系提取规则模板

模式名称	匹配关键词模板（部分）
因果关系	<由于|因为>{Cause},<因此|所以|导致>{Effect}
反因果关系	<本来|本应>{Effect},<反而|却因>{Cause}
顺承关系（完整）	<第一|首先>{Eventl},<然后|再|之后>{Event2}
顺承关系（居中）	{Eventl},<进而|就|之后>{Event2}

2.4　图谱构建

2.4.1　案件知识图谱构建

使用 Neo4j 图数据库构建图谱，可轻松地将三元组格式的数据转换为图谱形式。根据前期数据预处理结果，从非结构化的受骗过程文本数据中获取到了构建知识图谱所必需的事件元素三元组数据，然后结合结构化的案件相关数据，通过以下步骤构建案件知识图谱。

步骤 1　连接 Neo4j 数据库，读取每个案件数据中的“案件类型”数据，形成电信网络诈骗类型中心节点，每一个具体案件的图谱都与这一中心节点相连。

步骤 2　读取案件相关数据中的“案件名称”数据，形成单个具体案件的首节点，并与中心节点相连接，连接边的关系定义为包含关系。

步骤 3　读取“实际案损”和“受骗过程”数据，形成节点并分别与案件首节点进行连接，连接边的关系定义为包含关系。

步骤 4　生成“受害人”与“嫌疑人”节点，与“受骗过程”节点进行连接，连接边的关系定义为包含关系。然后，读取基于“受骗过程”数据提取出的事件元素三元组数据，筛选三元组中主体包含“受害人”与“嫌疑人”字样的数据，

将三元组中的客体形成节点，与对应的主体节点连接，连接边的关系定义为元素关系。

步骤5 读取案件相关数据中的受害人与嫌疑人的相关数据（受害人数据包含模糊化姓名、年龄与性别；嫌疑人数据包含模糊化姓名、年龄、性别、犯罪地以及有无前科），分别形成节点，并与“受害人”和“嫌疑人”两个节点连接，关系边根据数据属性决定。

步骤6 重复步骤1到步骤5，直至完成全部数据的处理，最终将形成案件知识图谱。

2.4.2 案件事理图谱构建

根据前期数据预处理结果，从非结构化的受骗过程文本数据获取到了构建事理图谱必需的事件关系三元组数据，再利用基于变分自编码器（variational autoencoder，VAE）和高斯混合模型（Gaussian mixture model，GMM）的中文文本聚类模型（Chinese text clustering model based on VAE and GMM，CTCM-V&G）对事件关系三元组中的前事件与后事件进行泛化，最后根据图谱构造规则生成案件事理图谱。

（1）CTCM-V&G模型

由于中文的语义具有较强的复杂性，在对中文文本进行聚类时，传统的无监督聚类算法（如*K*-means、Single Pass等）通常依赖于简单的距离度量，无法有效捕捉文本的深层语义特征，所得的聚类结果一般较差。鉴于此，研究构建了半监督学习的CTCM-V&G模型。电信网络诈骗案件事理图谱构建流程如图2所示。

CTCM-V&G模型使用预训练的RoBERTa模型对事件文本进行向量化，以获得更好的初始中文文本向量表示。为了捕捉文本的深层语义结构，构建了一个VAE模型用于生成特征表达能力更强的文本特征。VAE模型主要由编码器和解码器两部分组成。编码器主要将输入的数据x以编码的方式映射为变量z的分布参数（包括均值分布与方差分布），然后通过重参数化方法将变量z表示为：

$$z=\mu(x)+\sigma(x)\odot\epsilon \tag{1}$$

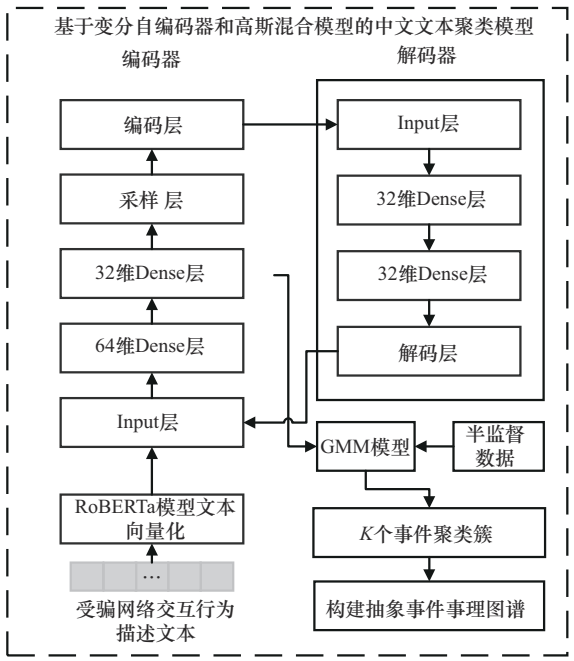

图2 电信网络诈骗案件事理图谱构建流程

其中，ϵ是从标准正态分布$N(0,1)$中采样的噪声，$\mu(x)$为数据x的均值分布，$\sigma(x)$为数据x的方差分布。该方式实现了对高维文本向量的低维化表示。

解码器主要将变量z重新映射回原数据空间并生成重构数据x'。同时，VAE模型在训练过程中会计算重构数据产生的误差并进一步更新模型参数。误差的计算式为：

$$L_{\mathrm{VAE}}=L_{\mathrm{recon}}+L_{\mathrm{KL}} \tag{2}$$

其中，L_{recon}为重构损失，由模型生成的样本与原始输入样本之间的差异决定；L_{KL}为KL（Kullback-Leibler）散度损失，由近似后验分布$P(z|x)$与先验分布$P(z)$之间的差异决定。

在构建的VAE模型中，编码器包含5层结构，输入（Input）层用于接收向量化后的文本数据；Dense层将向量化的文本逐步压缩到32维；采样层通过重参数化生成潜在变量z；编码层用于输出最终提取的低维文本向量。解码器包含4层结构，输入层用于接收编码器提取的文本向量特

征；Dense 层将 32 维的文本向量特征还原为 64 维；解码层通过计算重构数据产生的误差，并更新 VAE 模型各层的参数。通过以上方式，CTCM-V&G 模型能够从低维的文本向量数据表示中学习最能够代表文本数据的特征，实现文本聚类效果的提升。

在获取低维的文本向量特征后，使用半监督的 GMM 模型对风险事件进行聚类。由于 GMM 依赖大量无标注数据建模概率分布，因此先使用 *K*-means 算法对风险事件进行初步聚类，然后从初步聚类结果中根据每一类犯罪案件样本的数据量，人工筛选 1%～5% 且具有高代表性的风险事件并生成半监督数据集，再输入半监督的 GMM 模型中，实现风险事件的聚类泛化。半监督模型可以有效利用已知风险事件文本的特征，帮助识别和聚类新的风险事件文本，提高聚类的效果。

此外，为评估聚类效果，还引入了聚类评估常用的轮廓系数（Silhouette coefficient，SC）、CH（Calinski Harabasz）指数、DB（Davies Bouldin）指数和邓恩（Dunn）指数。

轮廓系数 $s(i)$ 通过综合评价内聚度和分离度来评价聚类效果：

$$s(i)=\frac{b(i)-a(i)}{\max\{a(i),b(i)\}} \tag{3}$$

其中，$a(i)$ 代表聚类簇的类内聚度，$b(i)$ 代表聚类簇的类间分离度。轮廓系数的取值范围为−1 到 1，其值越接近 1，则说明样本 i 的聚类结果越合理。

CH 指数通过聚类间的散布和聚类内的紧密度来评估聚类的效果：

$$\mathrm{CH}=\frac{T_r(B_K)}{T_r(W_K)}\times\frac{N-K}{K-1} \tag{4}$$

其中，B_K 代表聚类簇之间的离散矩阵，W_K 代表聚类簇内的离散矩阵，K 代表聚类簇的个数，N 代表用于聚类的数据条数。CH 指数越大表示聚类效果越好。

DB 指数基于聚类内的相似度和聚类间的不相似度来评估聚类的效果：

$$\mathrm{DB}=\frac{1}{N}\sum_{i=1}^{N}\max_{j\neq i}\left(\frac{\overline{S_i}+\overline{S_j}}{\left\|w_i-w_j\right\|}\right) \tag{5}$$

其中，$\overline{S_i}$ 是样本 i 到聚类中心的平均欧氏距离，$\left\|w_i-w_j\right\|$ 是第 i 类和第 j 类的聚类中心之间的欧氏距离。DB 指数的取值范围为（0，∞），其值越小代表聚类的有效性越高。

邓恩指数通过比较类间距离和类内距离来衡量聚类的紧密性和分离性：

$$\mathrm{Dunn}=\frac{\min_{1\leqslant i<j\leqslant k}\delta\left(C_i,C_j\right)}{\max_{1\leqslant l\leqslant k}\Delta\left(C_l\right)} \tag{6}$$

其中，$\delta\left(C_i,C_j\right)$ 表示聚类 C_i 和聚类 C_j 之间的最小距离（即类间距离），$\Delta\left(C_l\right)$ 表示聚类 C_l 内的最大距离（即类内距离）。邓恩指数的值越大表示聚类结果越好。

（2）案件事理图谱构建

电信网络诈骗案件中产生的事件均可被认定为风险事件。因此，将事件关系三元组中的具体事件输入 CTCM-V&G 模型中进行事件泛化，再根据以下步骤形成电信网络诈骗案件事理图谱。

步骤 1　连接 Neo4j 数据库，读取一条基于“受骗过程”文本数据生成的事件关系三元组列表，将其与事件泛化结果进行匹配，形成案件事理图谱五元组列表[前事件，泛化标签，事件关系，后事件，泛化标签]。

步骤 2　根据案件事理图谱五元组所属的“案件名称”形成案件的首节点。

步骤 3　读取一条案件事理图谱五元组数据，生成前事件与后事件节点，并在节点中记录对应的事件泛化标签结果，然后连接前事件与后事件节点，连接边关系由五元组中的“事件关系”决定。

步骤 4　判断是否为第一个读取的五元组数据。若是，则连接首节点与前事件节点，连接边关系定义为包含关系；若不是，则将本轮的前事件与上一轮的后事件进行连接，连接边关系定义

为顺承关系。

步骤5 重复步骤1到步骤4，直至全部数据处理完毕，最终将生成案件事理图谱。

综上，案件知识图谱更加关注利用生成式人工智能实施的电信网络诈骗案件中所包含的基本案件信息、受害人与嫌疑人做出的主要事件等元素；而案件事理图谱更加注重电信网络诈骗发生过程中风险事件发生的时序特征及风险事件之间的事理逻辑关系。

3 知识图谱与事理图谱构建结果

3.1 数据描述

鉴于电信网络诈骗相关研究数据的敏感性，同时为保证研究的可靠性，本次研究通过相关单位，获取了某市级区域内发生的电信网络诈骗案件数据共6 223条，数据采集工作于2024年10月完成。数据集中的案件类型分布如图3所示，该数据集既包含了2024年1月至9月发生的利用生成式人工智能技术实施的电信网络诈骗（即图3中的AI诈骗）案件，能精准捕捉AI换脸等生成式人工智能技术普及后的新型犯罪特征，也包含了2022年1月至2023年12月发生的购物消费、身份冒充等8种传统电信网络诈骗的典型案件数据，能够有效表征近几年的电信网络诈骗态势。同时，还获取了以上案件中已抓获的电信网络诈骗嫌疑人相关数据共2 807条。研究将基于以上数据开展相关实验与分析。

3.2 案件知识图谱构建结果

根据第2.4.1节中设计的知识图谱构建方法，研究实现了案件知识图谱的构建。案件知识图谱中包含了丰富的实体和事件元素，并可借助Cypher查询语言直观地从图谱中获取指定的数据模式和关系。例如，通过“MATCH (l:陈某被诈骗案) - [r*] -> (connected)； RETURN l, r, connected”查询语句，获得“陈某被诈骗案”的知识图谱查询结果展示，如图4所示。从图4中可以查看“陈某被诈骗案”中的案损、具体案情以及案件中嫌疑人与受害人间进行的关键事件等案件元素，从而帮助办案人员快速掌握案件的全貌和关键细节。此外，研究还将基于案件知识图谱开展数理统计分析，进一步挖掘案件中的潜在规律和特征。

3.3 案件事理图谱构建事件泛化结果

3.3.1 事件泛化结果

对于事件泛化处理，研究将CTCM-V&G模型与聚类常用基线方法DBSACN、*K*-means[27]以及Single Pass[28]算法进行对比实验。事件泛化模型对比结果见表4。

由表4可知，Single Pass算法的SC值为

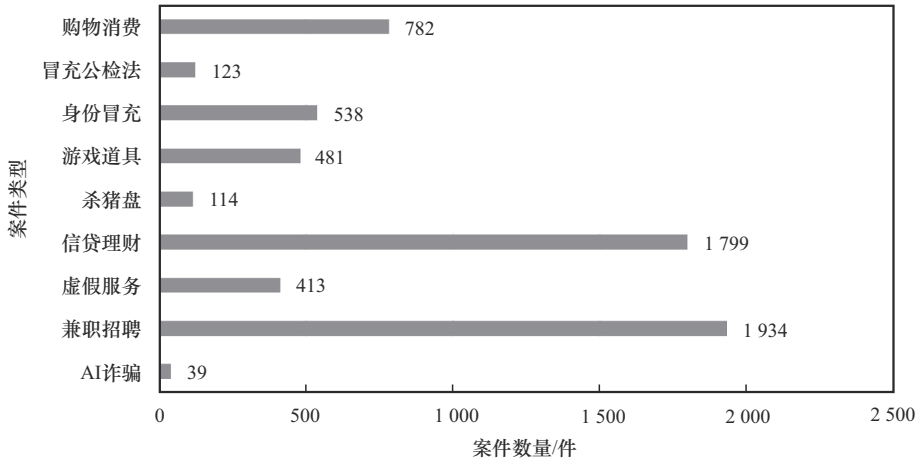

图3 数据集中的案件类型分布

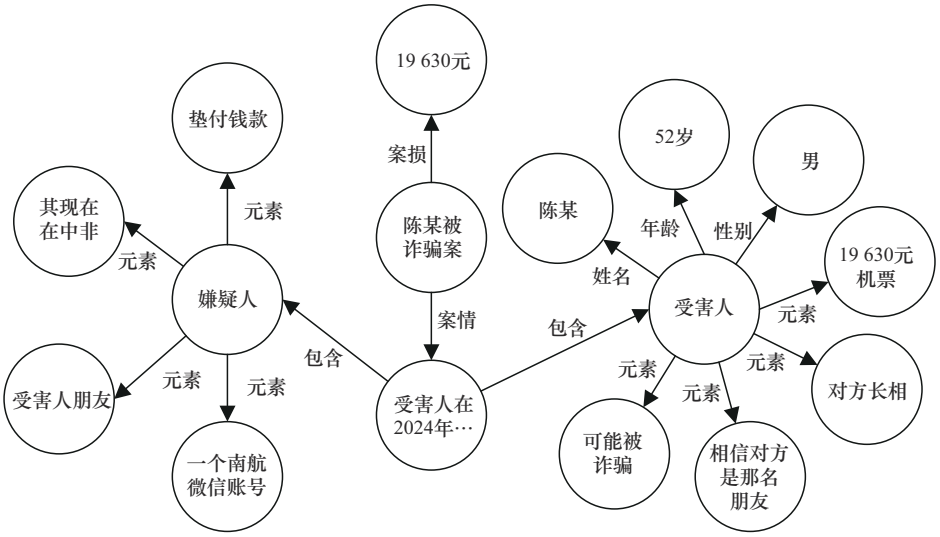

图4　案件知识图谱查询结果展示

表4　事件泛化模型对比结果

模型	SC指标	CH指标	DB指标	Dunn指标
CTCM-V&G	0.20	1 879.53	1.32	0.57
DBSACN	0.01	7.57	0.34	0.05
K-means	0.10	181.40	2.52	0.19
Single Pass	−0.02	0.26	0.39	0.07

−0.02，说明存在数据被错误地分配到不合适的聚类簇中，即该算法难以对电信网络诈骗中文文本进行有效聚类。CTCM-V&G模型在全部评估指标上相较于其他算法均存在明显优势，即CTCM-V&G模型在风险事件泛化任务上具有最好的表现。

在完成事件泛化处理的基础上结合标签定义，得到事件泛化结果标签，部分事件泛化结果示例见表5。

表5　部分事件泛化结果示例

事件	事件泛化结果标签
受害人收到了嫌疑人的视频聊天请求	建立联系
受害人看到了对方的长相，于是就相信对方是那名朋友	产生信任
嫌疑人现因购买机票支付不了，需要国内找人代付	提出要求
受害人添加了微信，并替嫌疑人代付了×元机票钱	按照要求转账
事后，嫌疑人以需要加急办理为由让受害人转更多的钱	意外事件
受害人随即意识到可能被诈骗	察觉受骗

3.3.2　案件事理图谱构建结果

根据第2.4.2节设计的事理图谱构建方法，研究实现了案件事理图谱的构建。案件事理图谱（局部）结果展示如图5所示。案件事理图谱用于展示电信网络诈骗过程中风险事件的前后发生顺序，以便更好地理解风险演化的流程。此外，研究还将进行图谱的拓扑特征分析，进一步挖掘生成式人工智能驱动下电信网络诈骗风险演化过程中的关键环节和演化模式。

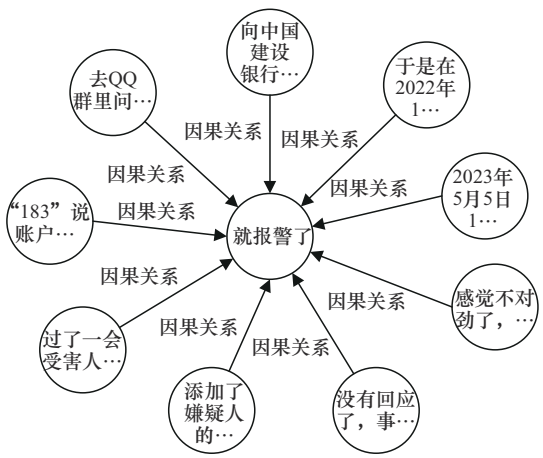

图5　案件事理图谱（局部）结果展示

4　电信网络诈骗风险演进实证分析

基于构建的案件知识图谱与案件事理图谱，

进一步结合数理统计分析及图谱分析技术进行实例分析，挖掘图谱中隐含的电信网络诈骗风险影响因素，解析电信网络诈骗风险的演化规律。

4.1 案件知识图谱分析

本节将基于构建的电信网络诈骗案件知识图谱开展数理统计分析研究，总结当前生成式人工智能驱动下电信网络诈骗的犯罪特征。

4.1.1 嫌疑人特征

通过对案件知识图谱中的嫌疑人特征进行统计分析可知：在性别特征方面，男性占比80.7%，女性占比19.3%，说明男性在电信网络诈骗犯罪中占主导。在犯罪前科方面，有前科的占比极少，仅占2.8%，说明大部分嫌疑人都没有犯罪前科。在地域特征方面，犯罪地的地域分布涉及多个省。在嫌疑人的罪名方面，帮助信息网络犯罪活动罪与诈骗罪成为电信网络诈骗犯罪中主要的罪名，分别占到了43.7%和33.0%，其分布特征基本符合当前我国电信网络诈骗犯罪的司法判决现状[29]。

在嫌疑人的年龄段分布特征方面，不满18岁的未成年人和超过60岁的老年人占比较低，分别仅占1.2%；占比最高的嫌疑人年龄段是满18岁不到40岁，达82.2%。原因可能是这一年龄段的人群在社会中处于活跃期，接触网络和电信设备的频率较高，同时也面临较大的经济压力和诱惑，而随着年龄的增长，嫌疑人数量显著减少，这既可能是由于年长群体在生活经验、法律意识和社会责任感方面的提升，使其不易参与犯罪活动，也可能是因为年长群体难以掌握电信网络诈骗所需的网络相关技术，进而不易参与犯罪活动。嫌疑人年龄特征统计结果见表6。

表6 嫌疑人年龄特征统计结果

年龄段	占比
不满18岁	1.2%
满18岁不到40岁	82.2%
满40岁不到60岁	15.4%
60岁以上	1.2%

同时，研究还进一步使用皮尔逊卡方检验方法对嫌疑人性别、年龄、犯罪前科和罪名特征进行了交叉检验分析，结果见表7。当交叉检验分析结果的显著性值小于0.05时，判定该特征对之间存在显著的统计学关联性。由表7可知，性别与罪名、性别与年龄以及年龄与犯罪前科之间存在显著的统计学关联性。其中，性别是影响嫌疑人罪名和犯罪前科的重要因素，而年龄与犯罪前科、犯罪前科与罪名等变量之间没有显著关联，表明嫌疑人的年龄与是否有犯罪前科对其所涉及的罪名类型影响较小。

表7 嫌疑人交叉检验分析结果

特征对	值	自由度	显著性
性别-罪名	79.68	6	<0.001
性别-犯罪前科	9.82	1	0.002
性别-年龄	126.89	59	<0.001
年龄-犯罪前科	57.91	6	0.52
年龄-罪名	421.48	354	0.008
犯罪前科-罪名	36.75	38	0.53

4.1.2 受害人特征

对案件知识图谱中的受害人特征进行统计分析可知：在性别特征方面，男女比例基本持平，男性占49.4%，女性占50.6%。但按照不同诈骗类型细分，性别差异较为明显。其中，男性受害人多是在网络游戏道具交易、虚假服务等场景下被骗，分别占比72.3%和70.1%。而女性受害人则更容易遭受冒充身份、“杀猪盘”、购物消费以及信贷理财等诈骗手法的侵害。

在年龄特征方面，受害人年龄主要集中于18岁到40岁，占总人数的61.2%。其中，遭受虚假服务、招聘兼职、购物消费、身份冒充以及游戏道具类诈骗的受害人主要集中在18岁至30岁年龄段；遭受信贷理财、冒充公检法和“杀猪盘”类诈骗的受害人主要集中30岁至40岁年龄段；而遭受AI诈骗的受害人没有明显的分布聚集性。分析其成因：一是由于网络技术的高速发展，18岁

到40岁的群体更加依赖网络空间，在网络购物、网络社交、网络服务等方面的活动更为频繁，更容易泄露个人信息，成为遭受虚假服务（男性）和购物消费（女性）类诈骗概率最高的群体；二是正在求学或刚步入社会的群体（18~24岁）受个人喜好、经济能力、社会阅历等多方面因素的影响，对电信网络诈骗防范意识不足，容易成为游戏道具、虚假服务、招聘兼职类诈骗的主要对象；三是有一定工作经验的群体（25~40岁），收入相对稳定且具有一定的经济基础，但往往承担着巨大的经济压力或来自家庭、事业和社会关系等方面的多重负担，同时也存在情感、婚恋方面的需求，极易遭受冒充公检法、“杀猪盘”、信贷理财等类型的诈骗。

在中国，电信网络诈骗犯罪的追诉标准要低于普通诈骗犯罪的追诉标准，且标准全国统一。当电信网络诈骗犯罪造成的损失金额在3 000元以下时，做报案记录；当损失金额达到3 000元以上30 000元以下时，认定为“数额较大”；当损失金额在30 000元以上500 000元以下时，认定为“数额巨大”；当损失金额达到500 000元以上时，认定为“数额特别巨大”。在案件损失的等级方面，电信网络诈骗案件损失金额统计见表8。由表8可知，电信网络诈骗案件对受害人的经济影响范围广泛，从小额损失到高额损失均有涉及，应加强针对中等和较大金额损失案件的防范和打击力度。

表8　电信网络诈骗案件损失金额统计

类型	报案记录/件	数额较大/件	数额巨大/件	数额特别巨大/件
信贷理财	70	698	981	50
兼职招聘	254	847	819	14
冒充公检法	8	72	39	4
“杀猪盘”	2	21	76	14
游戏道具	307	151	23	0
虚假服务	143	196	72	2
购物消费	344	319	117	2
身份冒充	164	219	151	4
AI诈骗	0	14	16	8

此外，研究进一步使用皮尔逊卡方检验方法对受害人性别、年龄、案件损失等级及受骗类型特征进行了交叉检验分析，结果见表9。由表9可知，性别、年龄、受骗类型与案件损失等级之间均存在显著的统计学关联性，即这些特征均为影响电信网络诈骗风险的重要因素。这一结果也与前文统计分析所得结论相符。

表9　受害人交叉检验分析结果

特征对	值	自由度	显著性
性别-受骗类型	1 578.65	20	<0.001
性别-案损等级	1 412.43	12	<0.001
性别-年龄	4 968.42	10	<0.001
年龄-案损等级	7 328.53	30	<0.001
年龄-受骗类型	7 868.97	50	<0.001
犯罪前科-罪名	8 147.92	60	<0.001

在生成式人工智能技术快速发展的背景下，当前电信网络诈骗虽仍以传统电信网络诈骗为主，但也已经发生利用生成式人工智能实施的电信网络诈骗案件，并呈现出单案损失金额较高的特征。同时，伴随着生成式人工智能技术门槛的降低及黑灰产业链中犯罪工具供应的产业化发展，该技术与传统电信网络诈骗手段的深度融合可能导致受害群体进一步扩散。针对这一趋势，需要深度挖掘其犯罪过程中的风险演化规律，从而为犯罪治理工作提供理论与决策支持。

4.2　案件事理图谱分析

本节将基于构建的案件事理图谱并结合拓扑特征分析理论，挖掘关键的风险事件节点，进而总结当前生成式人工智能驱动下电信网络诈骗的风险演化规律。

4.2.1　案件事理图谱分析

在本次获取的利用生成式人工智能实施的电信网络诈骗案件数据中，通过假冒身份手段实施诈骗的案件占78.95%。因此，本次研究主要围绕生成式人工智能对假冒身份类案件的驱动作用展开。

以“陈某被诈骗案”为例，其案件事理图谱如图6所示。在该案件中，受害人首先收到嫌疑人伪装的微信好友请求，在通过请求后与嫌疑人进行了微信视频通话。嫌疑人在进行微信视频通话的过程中利用生成式人工智能技术进行“换脸”，实现对受害人好友身份的伪装，导致受害人因眼见为实的惯性思维错误地认定了对方身份。然后，嫌疑人提出需要代缴国外机票费用的要求，受害人在完全没有怀疑的情况下，添加了转账账户并完成转账。直至嫌疑人再次提出大额转账要求后，受害人才察觉受骗并报警。

在传统身份冒充类案件中，犯罪分子往往仅通过社交账号伪装（如模仿账号的头像、ID等）的方式冒充身份并骗取受害人的信任，甚至部分实施广撒网式犯罪的嫌疑人会直接使用诈骗剧本，利用受害人趋利或避害的心理漏洞直接骗取受害人的信任，而较少如利用生成式人工智能实施的案件中主动与受害人进行视频、语音通信等身份认证方式来取得受害人信任。嫌疑人利用心理学中的证真偏差现象（即人们倾向于相信与自己已有认知一致的信息），通过主动的身份验证行为，破除受害人对网络中未知身份的天然警惕心理。当受害人看到视频通话中的熟悉面孔时，防备心理被削弱，导致其更容易接受对方的要求。嫌疑人通过生成式人工智能技术极大地增强了伪装身份的真实性和可信度，能够更有效地操控受害人的信任，使得受害人更难在早期阶段识破骗局，进而延长诈骗的持续时间和扩大损失金额。

4.2.2 拓扑特征分析及风险演化模式分析

针对构建的案件事理图谱，研究引入度、路径长度、图的半径等拓扑特征进行分析。拓扑特征说明见表10。

本文构建的案件事理图谱的拓扑特征统计结果见表11，包括对应特征的平均值、最大值和最小值。具体如下。

（1）对于度特征，平均值为0.78，表明大多数节点的连接数较少；最大入度为62、最大出度

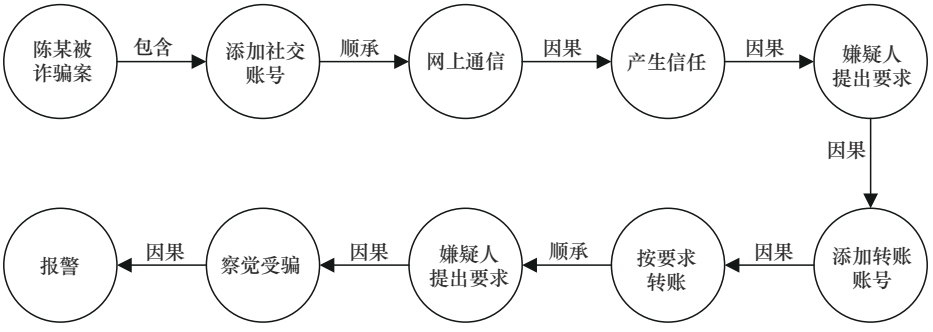

图6 陈某被诈骗案的案件事理图谱

表10 拓扑特征说明

拓扑特征	说明
度	节点的度是与该节点直接相连的边的数量。度的值越大，节点的连接性越强，分为入度与出度
路径长度	2个节点之间的最短路径上的边的数量，反映了节点之间的距离
图的半径	图中所有节点到其最远节点的最短路径长度的最小值，反映了图的紧密程度
图的直径	图中所有节点到其最远节点的最短路径长度的最大值，反映了图的扩展程度
集群系数	衡量一个节点与邻居节点之间实际存在的边与可能存在的边的比例，反映了节点的聚集性
中介中心性	一个节点在所有最短路径中所处的位置的频率，反映了节点在图中的中介作用
特征向量中心性	不仅考虑与节点直接连接的节点数量，还考虑连接节点的重要性，反映了一个节点的重要性

为18，说明存在部分中心事件节点。

（2）对于路径长度特征，平均路径长度为0.69，表明大多数节点之间的距离较短。

（3）对于图的半径与直径特征，整体而言图谱的紧密程度适中，半径平均值为4.54；图谱的扩展程度较小，直径平均值为2.269。

（4）对于集群系数特征，图谱的集群系数为0，即图谱中没有形成任何集群，表明事件节点之间不存在较为复杂的事理关系。

（5）对于中介中心性特征，平均值为0.1。表明大多数节点在网络中的中介作用较小，但也存在少部分节点在网络中起到了重要的中介作用（最大值0.5。）。

（6）对于特征向量中心性特征，平均值为0.24，表明大多数节点的重要性较弱，同时也存在一些重要节点（最大值0.99）。

表11　案件事理图谱拓扑特征统计结果

拓扑特征	平均值	最大值	最小值
入度	0.78	62	0
出度	0.78	18	0
路径长度	0.69	7.36	0
图的半径	4.55	80	2
图的直径	2.27	40	1
集群系数	0	0	0
中介中心性	0.10	0.50	0
特征向量中心性	0.24	0.99	0

综上所述，在构建的案件事理图谱中存在部分具有较高入度、出度和特征向量中心性的关键节点；而大多数节点的连接性较低，路径长度较短，图谱的整体线性程度较强，紧密程度适中。结合拓扑特征分析结果，对案件事理图谱进一步进行抽象和总结，并结合实际案情进行分析，归纳出案件事理图谱的3类主要风险演化模式。

（1）长链型风险演化模式

长链型风险演化模式主要反映电信网络诈骗风险事件逐步推进的特征。在此类风险演化模式中，节点之间呈现线性或接近线性的连接结构，每个节点仅与前一个节点和后一个节点相连。该结构也符合由平均出入度、集群系数等特征分析得出的图谱线性程度较强结论。长链型风险演化模式一般出现在单个案件形成的事理图谱中，反映了嫌疑人通过多个中间环节逐步骗取受害人财物的过程。当前利用生成式人工智能实施的身份冒充类电信网络诈骗案件的风险演化模式可总结为“建立联系-身份验证-博取信任-提出要求-转账支付-意外事件-察觉受骗”的长链型风险演化模式，其演化模式示例如图7所示。受害人首先从某种渠道（如社交账号等）与嫌疑人产生联系，然后嫌疑人会通过网络视频、语音等方式与受害人进行身份验证以博取信任。在受害人信任伪造的身份后，根据诈骗剧本提出转账要求，受害人在错误的信任下向对方转账，直至发生意外事件（如多次要求转账、失去联系等），才察觉受骗。分析长链型风险演化模式，可以识别诈骗活动中的完整事件节点，帮助有关部门对该类诈骗案件中所包含的关键事件进行整体性认知。

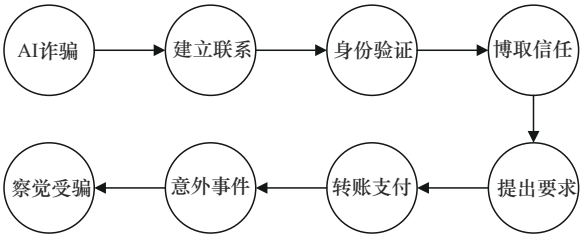

图7　长链型风险演化模式示例

（2）星型风险演化模式

星型风险演化模式主要反映一个中心节点与多个外围节点的连接特征。在此类风险演化模式中，一个中心节点与多个外围节点直接相连，而外围节点之间没有直接的关联性。该结构也符合由出入度最大值、中介中心性最大值、特征向量中心性最大值等特征分析得出的图谱中存在一些关键节点结论。星型风险演化模式往往出现在多个具有近似事件的案件所形成的事理图谱的中间部分。在利用生

成式人工智能实施的身份冒充类电信网络诈骗案件中，从事件的泛化标签视角看，其演化模式为“身份验证-博取信任-提出转账要求”，但从具体事件角度观察，则会得到“{视频通信，语音通信}-博取信任-{帮忙代付，要求汇款}”的星型风险演化模式，其演化模式示例如图8所示。嫌疑人会利用生成式人工智能技术进行“换脸”“拟声”等不同的身份验证方式，博取受害人的信任，再根据不同的诈骗剧本提出不同的要求。分析星型风险演化模式，可以识别出风险演进过程中的核心节点及外围节点，帮助执法部门集中资源打击核心事件节点，从而有效打击犯罪。

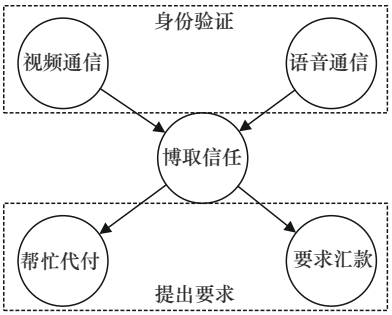

图8　星型风险演化模式示例

（3）复合型风险演化模式

复合型风险演化模式融合了长链型和星型风险演化模式的特征。在此类风险演化模式中，既存在线性或接近线性的长链结构，也存在中心节点与多个外围节点的星型结构。该结构也符合由出入度最大值、中介中心性最大值等特征分析得出的图谱中存在一些关键节点结论。复合型风险演化模式一般出现在多个具有近似事件的案件形成的事理图谱的末尾部分。复合型风险演化模式示例如图9所示，图中既存在如“发生意外-按要求转账-产生损失-报警”“发生意外-失去联系-报警”等长链型风险演化模式，也存在如“{产生损失，发生意外，察觉受骗，失去联系}-报警”的星型风险演化模式。在受害人与嫌疑人的交互过程中会产生不同的风险演化模式，包括线性推进的长链型模式和多渠道传播的星型模式，这也反映了诈骗活动的复杂性和多样性。分析复合型风险演化模式，可以更全面地了解风险事件的组织结构和受害人的行为模式，同时帮助有关部门优化劝阻工作流程。

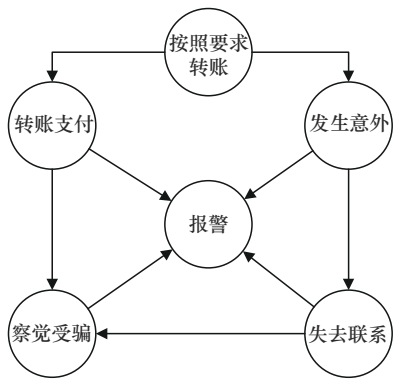

图9　复合型风险演化模式示例

5　结束语

本文对生成式人工智能驱动下的电信网络诈骗案件数据进行分句与分词、事件元素识别、事件关系抽取等处理后，构建了生成式人工智能驱动下电信网络诈骗风险的知识图谱与事理图谱。研究发现，当前电信网络诈骗案件中性别特征的影响较为显著。其中，嫌疑人主要为年龄18岁到35岁的男性群体，且大多数嫌疑人没有犯罪前科；受害人在性别比例上总体持平，年龄主要集中在18岁到40岁，遭受诈骗后产生的损失较大，但不同性别及年龄段的人群易遭受的电信网络诈骗类型具有显著差别。同时，对构建的案件事理图谱进行对比分析可知，当前利用生成式人工智能技术的电信网络诈骗案件呈现出更高的复杂性和隐蔽性，与传统电信网络诈骗手段相比，生成式人工智能技术能够模拟出更真实的身份特征，且能利用证真偏差现象更轻松地获取受害人的信任，使得受害人更难在诈骗的早期阶段识破骗局。此外，基于拓扑特征分析结果，识别出3类风险演化模式（长链型、星型和复合型）。其中，

长链型风险演化模式主要出现在单个案件形成的事理图谱中，该类演化模式完整体现了案件中电信网络诈骗风险随时间线性推进的特征；星型风险演化模式与复合型风险演化模式则常见于多个案情类似的案件共同形成的事理图谱中，这2类演化模式不仅反映了同类案件聚合后存在的不同风险行为模式，也反映了电信网络诈骗的核心风险事件节点，为制定有针对性的电信网络诈骗治理对策提供决策依据。

在实际工作中，建议有关部门将知识图谱与事理图谱纳入反诈预警系统，通过可视化技术动态追踪诈骗行为链条中的关键节点，针对长链型案件建立分阶段拦截机制，针对星型和复合型案件则强化对核心作案环节的精准打击。同时，可结合拓扑特征分析结果，针对不同风险模式研发定向监测模型。例如，通过长链型结构预测诈骗话术的演进方向，或基于星型结构识别犯罪网络的枢纽节点等，以此帮助有关部门更好地理解电信网络诈骗风险的演化规律，并制定更有效的打击和防范策略，综合提升对电信网络诈骗的防治能力。此外，未来的研究需要进一步优化图谱构建和分析方法，提升图谱的构建效果，并探索更多生成式人工智能驱动下的电信网络诈骗场景类型，完善对新型电信网络诈骗风险的认知。

参考文献：

[1] TIAN L, ZHOU X, WU Y P, et al. Knowledge graph and knowledge reasoning: a systematic review[J]. Journal of Electronic Science and Technology, 2022, 20(2): 100159.

[2] ZHANG W, PAUDEL B, ZHANG W, et al. Interaction embeddings for prediction and explanation in knowledge graphs[C]// Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining. New York: ACM Press, 2019: 96-104.

[3] CHEN X, ZHANG N Y, XIE X, et al. Knowprompt: knowledge-aware prompt-tuning with synergistic optimization for relation extraction[C]// Proceedings of the ACM Web conference 2022. New York: ACM Press, 2022: 2778-2788.

[4] OPDAHL A L, AL-MOSLMI T, DANG-NGUYEN D T, et al. Semantic knowledge graphs for the news: a review[J]. ACM Computing Surveys, 2023, 55(7): 1-38.

[5] SIMMS A M, KANAKIA A, SIPRA M, et al. A patient safety knowledge graph supporting vaccine product development[J]. BMC Medical Informatics and Decision Making, 2024, 24(1): 10.

[6] 冯钧, 畅阳红, 陆佳民, 等. 基于大语言模型的水工程调度知识图谱的构建与应用[J]. 计算机科学与探索, 2024, 18(6): 1637-1647.
FENG J, CHANG Y H, LU J M, et al. Construction and application of knowledge graph for water engineering scheduling based on large language model[J]. Journal of Frontiers of Computer Science and Technology, 2024, 18(6): 1637-1647.

[7] MAN N, WANG K C, LIU L. Using computer cognitive atlas to improve students' divergent thinking ability[J]. Journal of Organizational and End User Computing, 2021, 33(6): 1-16.

[8] ZHANG B, SUN X M, LI X M, et al. Construction and application of event logic graph: a survey[M]//Database Systems for Advanced Applications. DASFAA 2022 International Workshops. Cham: Springer International Publishing, 2022: 160-174.

[9] 熊凯, 杜理, 丁效, 等. 面向文本推理的知识增强预训练语言模型[J]. 中文信息学报, 2022, 36(12): 27-35.
XIONG K, DU L, DING X, et al. Knowledge enhanced pretrained language model for textual inference[J]. Journal of Chinese Information Processing, 2022, 36(12): 27-35.

[10] 翟利志, 李睿祥, 杨佳贝, 等. 基于复合语义特征的事件图谱构建技术研究进展[J]. 计算机科学, 2023, 50(9): 242-259.
ZHAI L Z, LI R X, YANG J B, et al. Overview about composite semantic-based event graph construction[J]. Computer Science, 2023, 50(9): 242-259.

[11] 杨纪星, 杨波, 朱剑林, 等. 金融领域事件因果关系发现及事理图谱构建与应用[J]. 中文信息学报, 2023, 37(7): 131-142.
YANG J X, YANG B, ZHU J L, et al. Event causality extraction, eventic graph construction and application in financial domain[J]. Journal of Chinese Information Processing, 2023, 37(7): 131-142.

[12] 宁慧涵, 眭海刚, 王金地, 等. 顾及时空关系的事故灾难事理图谱构建方法研究[J]. 武汉大学学报(信息科学版), 2024, 49(5): 831-843.
NING H H, SUI H G, WANG J D, et al. Construction of disaster event evolutionary graph based on spatiotemporal relationship[J]. Geomatics and Information Science of Wuhan University, 2024, 49(5): 831-843.

[13] 周林兴, 王帅. 事理图谱模型下的重大突发事件网络舆情诱发与缓释机理研究[J]. 图书情报工作, 2023, 67(12): 58-69.
ZHOU L X, WANG S. Research on the triggering and mitigating mechanisms of network public opinion in major emergencies under the event evolutionary graph model[J]. Library and Information Service, 2023, 67(12): 58-69.

[14] GOPAL R D, HOJATI A, PATTERSON R A. Analysis of third-party request structures to detect fraudulent websites[J]. Decision Support Systems, 2022, 154: 113698.

[15] CHU G J, WANG J Y, QI Q, et al. Exploiting spatial-temporal behavior patterns for fraud detection in telecom networks[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(6): 4564-4577.

[16] JIANG Y, LIU G N, WU J J, et al. Telecom fraud detection via Hawkes-enhanced sequence model[J]. IEEE Transactions on Knowledge and Data Engineering, 2023, 35(5): 5311-5324.

[17] PRIYA G J, SARADHA S. Fraud detection and prevention using machine learning algorithms: a review[C]//Proceedings of the 2021 7th International Conference on Electrical Energy Systems (ICEES). Piscataway: IEEE Press, 2021: 564-568.

[18] 陈红敏, 赵雷, 郭素然, 等. 电信诈骗如何导致误信: 影响因素、解释理论及研究展望[J]. 华南师范大学学报(社会科学版), 2023(2): 94-106.
CHEN H M, ZHAO L, GUO S R, et al. How telecom fraud leads to mistrust: influencing factors, interpretation theory and research prospect[J]. Journal of South China Normal University (Social Science Edition), 2023(2): 94-106.

[19] 唐赫, 许博洋, 赵民. 社会经济对电信网络诈骗犯罪率的影响机制: 基于全国300个城市样本的多重中介效应与空间规律分析[J]. 河南警察学院学报, 2022, 31(4): 58-65.
TANG H, XU B Y, ZHAO M. Mechanisms of socioeconomic influence on the fraudulent crime rate of telecommunication network: analysis of multiple mediating effects and spatial patterns in 300 cities of China[J]. Journal of Henan Police College, 2022, 31(4): 58-65.

[20] 陈如超. 电信网络诈骗涉案资金紧急止付的双重逻辑[J]. 法律科学(西北政法大学学报), 2024, 42(1): 124-134.
CHEN R C. The dual logic of emergency stop payment of funds involved in telecommunications network fraud[J]. Science of Law (Journal of Northwest University of Political Science and Law), 2024, 42(1): 124-134.

[21] 任江,吴舒颖. 人工智能生成数字化人格:侵权风险、伦理挑战与法律规制[J]. 南京邮电大学学报(社会科学版), 2025,27(1): 39-49.
REN J, WU S Y. Artificial intelligence generating digital personality: infringement risk, ethical challenges, and legal regulations[J]. Journal of Nanjing University of Posts and Telecommunications(Social Science Edition), 2025,27(1):39-49.

[22] 苏竣,宋立夫,魏钰明,等. 智能社会的舆论操控:理论机理、手段特征与社会影响[J]. 电子政务,2025(1):29-38.
SU J, SONG L F, WEI Y M, et al. The control of public opinion in intelligent society: theoretical mechanism, means and social influence[J]. E-Government, 2025(1):29-38.

[23] 汝鹏,苏竣,韩志弘,等. 智能引领未来:生成式人工智能的社会影响与标准化治理[J]. 电子政务,2025(1):2-14.
RU P, SU J, HAN Z H, et al. Intelligence leads the future: the social impact and standardized governance of generative artificial intelligence[J]. E-Government,2025(1):2-14.

[24] 钱洪伟, 王旭, 高宁. 生成式人工智能ChatGPT风险形成机理与防范策略研究[J]. 中国应急管理科学, 2024(11): 112-122.
QIAN H W, WANG X, GAO N. Research on the formation mechanism and prevention strategies of risks in generative artificial intelligence ChatGPT[J]. Journal of China Emergency Management Science, 2024(11): 112-122.

[25] CHE W X, FENG Y L, QIN L B, et al. N-LTP: an open-source neural language technology platform for Chinese[C]//Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing: System Demonstrations. Stroudsburg, PA: ACL, 2021:42-49.

[26] CHANG C, TANG Y, LONG Y X, et al. Multi-information preprocessing event extraction with BiLSTM-CRF attention for academic knowledge graph construction[J]. IEEE Transactions on Computational Social Systems, 2023, 10(5): 2713-2724.

[27] 李诗轩, 王璐, 沈愿, 等. 融合ERNIE的自然灾害舆情事理图谱构建及次生衍生事件探测研究[J]. 情报杂志, 2025, 44(3): 128-138.
LI S X, WANG L, SHEN Y, et al. Research on the construction of natural disaster public opinion event evolutionary graph integrated with ERNIE and detection of secondary derivative events[J].Journal of Intelligence, 2025, 44(3):128-138.

[28] 彭珺, 邓君, 鞠海龙. 面向网络游记文本的事理知识融合框架研究[J]. 情报科学, 2024, 42(3): 156-162.
PENG J, DENG J, JU H L. The framework of travelogue texts knowledge fusion based on the event logic graphs[J]. Information Science, 2024, 42(3): 156-162.

[29] 刘子良. 帮助信息网络犯罪活动罪的从属性否定与独立性证成: 基于规范论的立场[J]. 河南财经政法大学学报, 2024, 39(2):

106-118.

LIU Z L. Subordination falsification and independence justification of crime of aiding information network criminal activities: based on the position of normative theory in criminal law[J]. Journal of Henan University of Economics and Law, 2024, 39(2): 106-118.

[作者简介]

周胜利（1982– ），男，博士，浙江警察学院信息网络安全学院教授、硕士生导师，主要研究方向为网络安全、网络空间治理。

徐睿（2000– ），男，杭州电子科技大学网络空间安全学院硕士生，主要研究方向为网络安全、机器学习。

陈庭贵（1979– ），男，浙江工商大学统计与数学学院教授、博士生导师，主要研究方向为网络舆情演化分析。

汪邵杰（2004– ），男，浙江警察学院信息网络安全学院在读，主要研究方向为网络安全。

王镇波（1987– ），男，博士，浙江警察学院信息网络安全学院讲师，主要研究方向为人工智能和智能交通。