Journal of Computer Applications
计算机应用,2014,34(3):869-872,878
ISSN 1001-9081
CODEN JYIIDU
2014-03-10
http://www.joca.cn

文章编号:1001-9081(2014)03-0869-04
doi:10.11772/j.issn.1001-9081.2014.03.0869

# 基于有限信息融合的中央银行大额支付系统反洗钱管理模型

王　征[1,2*],彭嘉陵[1,2],傅立立[1,2],张佳琳[3]
(1.西南财经大学 经济信息工程学院,成都 611130;　2.西南财经大学 金融学院,成都 611130;
3.哈尔滨商业大学 研究生学院,哈尔滨 150028)
(*通信作者电子邮箱 wangzheng151400@163.com)

**摘　要**:针对跨行洗钱犯罪的复杂性和协作性,在中央银行大额支付系统(HVPS)框架内,综合有限信息管理新方法,构建了新型的反洗钱管理模型。该模型采用分布式检测点采集排队队列中的洗钱信息,从而对大额支付系统中的协作洗钱犯罪进行整合的动态跟踪。它采用了基于事件的描述方法记录洗钱犯罪过程,应用灰色关联度算法实现大额支付系统中的多检测点信息融合,通过有限信息发掘出大额支付系统中的异常操作行为,最终应用功率谱估计算法实现洗钱犯罪的快速分析与识别。仿真测试结果证明,该模型与传统的反洗钱管理模型相比,洗钱客户覆盖率和发现精确度超过12%以上,而洗钱事件召回率提高了5%以上。从总体来看,该模型具有较高的信息处理效率和处理精度。

**关键词**:有限信息;反洗钱;大额支付系统;信息融合;识别
**中图分类号**:TP391;TP393　　**文献标志码**:A

## Anti-money laundering management model of central bank high-value payment system based on limited information fusion

WANG Zheng[1,2*], PENG Jialing[1,2], FU Lili[1,2], ZHANG Jialing[3]
(1. *School of Economic Information Engineering, Southwestern University of Finance and Economics, Chengdu Sichuan* 611130, *China*;
2. *School of Finance, Southwestern University of Finance and Economics, Chengdu Sichuan* 611130, *China*;
3. *Graduate School, Harbin University of Commerce, Harbin Heilongjiang* 150028, *China*)

**Abstract:** To deal with the problem of inter-bank money laundering, combined with limited information management methods, a new anti-money laundering model was presented with central bank High-Value Payment System (HVPS) architecture. The proposed model utilized distributed monitor nodes to trace money laundering crimes. And it used event description method to record the crime procedures and so on. A new grey relational information fusion algorithm was invented to integrate multi-monitor information. And an improved power spectral algorithm was proposed to deal with fast data analysis and money laundering recognition operations. The simulation results show that the model has better processing performance and anti-money laundering recognition accuracy than others do. In detail, the model does well in money-laundering client coverage (by 12%), discovery rates (by 12%) and recall rates (by 5%).

**Key words:** limited information; anti money laundering; High Value Payment System (HVPS); information fusion; recognition

## 0　引言

反洗钱工作历来受到金融行业的高度重视,而洗钱信息发掘是其中的难点之一。全球性的反洗钱国际组织金融行动特别工作组(Financial Action Task Force on Money Laundering, FATF),将洗钱犯罪定义为:"隐匿或掩饰因犯罪行为所取得的财物的真实性质、来源、地点、流向及转移,或协助任何与非法活动有关系之人规避法律应负责任"。世界各国的中央银行,作为跨行(银行间)反洗钱管理的主力,除了加强反洗钱领域的法律和制度建设外,也在不断进行反洗钱管理的信息处理技术方面的研究,主要包括:加强反洗钱信息化建设,进行洗钱案例的智能化建模,提高金融信息数据的智能化分析水平,力争从有限的信息中发现洗钱犯罪行为等。在世界各国中央银行的支持下,国内外学者已取得了一定的研究成果,包括:Nikolosk 等[1]研究了中央银行在跨行反洗钱工作中的角色问题;Barone 等[2]、Unger 等[3]对洗钱犯罪的组织流程以及类型进行了详细分类;Shehu[4]、Sharman 等[5]研究了中央银行的反洗钱监管方法;Dolar 等[6]研究了跨行反洗钱的金融风险管理问题;Vlcek[7]研究了央行反洗钱的规则制定问题。随着研究的深入,越来越多的研究人员将注意力集中于各国央行的支付系统,并开展了一系列的研究工作,包括:Dreewski 等[8]开展的基于支付系统的反洗钱监测辅助决策模

**收稿日期**:2013-09-18;**修回日期**:2013-11-11。　**基金项目**:国家自然科学基金资助项目(60974104);教育部人文社会科学研究青年项目(10YJCZH169);四川省金融智能与金融工程重点实验室项目(FIFE2010-P05)。
**作者简介**:王征(1979-),男,新疆五家渠人,副教授,博士,主要研究方向:金融信息处理;　彭嘉陵(1985-),男,重庆人,博士研究生,主要研究方向:金融信息处理;　傅立立(1984-),女,四川成都人,博士研究生,主要研究方向:行为金融;　张佳琳(1979-),女,黑龙江哈尔滨人,副教授,博士,主要研究方向:信息融合。

型研究;Vandana 等[9]、Peng[10]等开展的基于支付系统的反洗钱模型研究;Bak 等[11]、Byrne[12]等进行的反洗钱规则模型研究;Cao 等[13]、Le-Khac 等[14]开展的基于数据挖掘的反洗钱模型研究。我国银行领域内的反洗钱研究开展较晚;尽管中国反洗钱监测分析中心等机构开展了诸如《中国特色的反洗钱犯罪类型学初探》一类的理论研究[15],但其主要内容集中在银行分行一级的洗钱犯罪识别,而基于新型央行信息系统的反洗钱探索鲜有研究人员涉足[16]。而从现今的使用效果来看,由于洗钱活动中能够识别到的信息数量极为有限,目前上述成果的应用仍然存在诸多问题。针对上述模型存在的不足和研究的缺失,本文提出了基于有限信息融合的央行反洗钱管理模型(Anti money Laundering management model in Central bank HVPS based on Information Fusion, ALCH),并设计了相关模块、数据结构以及处理流程。

## 1 模型结构与管理流程

ALCH 模型的功能模块与管理流程均依托央行大额实时支付系统环境,针对系统内,数量和内容均很有限的洗钱信息展开(如图 1),相关系统包括:国家处理中心(National Processing Center, NPC)、城市处理中心(City Clearing Processing Center, CCPC)和大额支付系统(High Value Payment System, HVPS)。具体内容如下:

1)分布式的检测点模块,内置洗钱事件生成器(Event generator)。该模块是反洗钱任务的基本执行单元。由于大额支付系统中以支付活动中的发起方(某银行)作为分类依据,划分支付清算任务队列,导致原本就很有限的支付清算数据(反洗钱基础信息)出现了局部视图分裂问题(各银行反洗钱信息未能存储在统一的队列中,因而给跨行洗钱犯罪以可乘之机)。如何建立整合的全局视图,这也是目前众多反洗钱模型未能解决的重难点问题之一[3-4,7]。为解决上述问题,ALCH 模型为所有的任务队列都建立了对应的分布式检测点;在检测点产生事件数据后,本模型将通过基于灰色关联度的多检测点信息融合算法对其进行处理,为后续模块生成整合的、相对完整的全局事件特征向量序列。

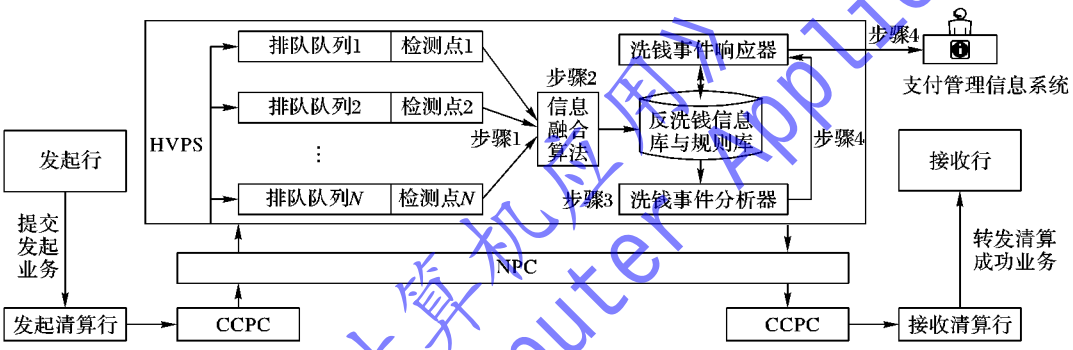


图 1 模型结构与管理工作流程

2)洗钱事件分析器(Event analyzer)模块。传统的反洗钱模型需要大量的信息积累才能进行数据挖掘,往往延误反洗钱战机[14];为解决上述问题,本模块研究了基于功率谱的洗钱犯罪预告警算法,从有限数据片断中,及时识别和发现洗钱犯罪活动。

3)洗钱事件响应器(Response unit)模块。在接到洗钱事件分析器的预告警后,该模块根据规则库中的设定,作“事件-预案”匹配,自动进行现场保护、上下文跟踪等反洗钱操作,并向管理人员告警。

4)洗钱事件信息与规则库(Event & Rule database)模块。用于存储反洗钱过程中产生的各种中间与结果信息,以及预设的反洗钱规则,并向管理人员提供信息检索接口。

该模型的管理工作流程如下:

1)各检测点启动,以支付清算业务的发起行、接收行、时间等序列标识信息,生成事件特征向量;

2)事件特征向量通过基于灰色关联度的多检测点信息融合算法,融合成相对完整和全面的整合信息序列(全局视图),并注入数据库中备用;

3)洗钱事件分析器从数据库中提取整合后的检测序列,通过功率谱算法,结合数据库中预设的反洗钱规则,完成洗钱识别与评判;

4)洗钱事件响应器接到分析器提交的结果后,根据其中的事件特征信息,从数据库中提取并执行对应事件的预案,同时向管理人员告警。

## 2 关键算法

### 2.1 预处理与洗钱事件模型

为准确和详细地描述并跟踪洗钱犯罪活动的过程,ALCH 模型使用的数据,由国家处理中心首先进行了数据归一化预处理,将局部数据以及各分行发来的异质数据进行规格上的统一:首先以缺省值填充监测的缺失,或发回补填;其次是将数值型数据规约到值域[-1,1]。最终,ALCH 模型在洗钱事件跟踪方面采用了事件特征向量(六元组)表示法,$E(\text{Event})=\langle O,A,T,E,P,L\rangle$。其中元素为:$O$ 为客户节点(Object,分为发起行、接收行等信息组成的列表),$A$(Action,大额实时支付系统中的合法操作)为动作,$T$(Time,包含规定的清算时间窗口内外时间)为时间,$E$(Environment,支付清算活动的上下文环境以及相关参数)为环境,$P$(Predict,指向后续操作的关联指针)为预言,$L$(Language,操作中包含的关键词)为表现词。

### 2.2 多检测点信息融合算法原理

由于大额支付系统中的检测点数量众多,且同一洗钱活动中的协作犯罪信息将分散于多条排队队列,由此将在多个检测点中分裂,并产生不同的检测视图,使得本身数量极为有限的反洗钱信息变得更加难于处理。针对这种问题,本模型中开发了基于灰色关联度的多检测点信息融合算法,将多个反洗钱检测视图融合为一,以备后续模块使用。

灰色关联度建模(Gray-relational Modeling, GM)方法主要用于度量事物发生发展过程中,各因素之间的相对变化情

况;在变化过程中,如果两因素的相对变化(通常用向量表示)一致或接近,则二者之间的关联程度较高。由于该方法对于连续变化的态势问题提供了量化的度量,因此非常适合于活动的历程分析。ALCH 模型中以 2.1 节中的事件特征向量作为基础元素,设定大额支付系统中初始检测点中某客户的操作序列(即以时间为序的基准参考序列):$X_0 = (x_1, x_2, \cdots, x_n)$,而 $y_j = (y_{j1}, y_{j2}, \cdots, y_{jm})$ 为相应时间段内,其他检测点产生的比较序列,则参考序列与各个比较序列在各个时间段的灰色关联系数为:

$$L_j(t_i) = \frac{\min\limits_j \min\limits_i |x_i - y_{ji}| + \rho \max\limits_j \max\limits_i |x_i - y_{ji}|}{|x_i - y_{ji}| + \rho \max\limits_j \max\limits_i |x_i - y_{ji}|} \tag{1}$$

其中 $\rho$ 为分辨系数($\rho \in (0,1)$)。$\rho$ 越小,检测点的分辨粒度越大。实际处理过程中将根据反洗钱系统的实际需求,对 $\rho$ 值进行调节。为防止过度细化导致的系统资源(计算资源)浪费,设定下列 $\rho$ 值选取原则:

当 $\Delta$ 为对比队列(序列)中所有差值的绝对值均值时 $\left(\Delta = \dfrac{\sum\limits_{j=1}^{m}\sum\limits_{j=1}^{n}|x_i - x_{ji}|}{m * n}\right)$,令 $\varepsilon = \dfrac{\Delta}{\max\limits_j \max\limits_i |x_i - x_{ji}|}$。当 $\max\limits_j \max\limits_i |x_i - x_{ji}| \geqslant 3\Delta$ 时,取 $\varepsilon < \rho < 1.5\varepsilon$;如 $\max\limits_j \max\limits_i |x_i - x_{ji}| < 3\Delta$,则取 $\varepsilon < \rho < 2\varepsilon$。基于上述方法,ALCH 模型能够自动确定 $\rho$ 参数的取值范围,避免了人工处理的繁琐过程,提高了反洗钱检测的决策效率。

### 2.3　基于灰色关联度的序列相似度

由 $n$ 个检测点服务器(软件概念,可以是实体服务器,也可以是单机中执行服务功能的进程)组成的检测群组,采用直接测量法,对事件特征向量中的静止或渐变参数 $X$ 进行动态跟踪,测量公式为:

$$z_i(k) = X + v_i(k);\quad i = 1,2,\cdots,n \tag{2}$$

其中:$E(v(k))$ 等先验知识均未知,$z_i(k)$ 为第 $i$ 个大额支付检测点服务器在 $k$ 时刻的观测值,$X$ 为真实值,$v_i(k)$ 为 $k$ 时刻的噪声。

在某一时刻 $l$,当检测序列 $z_i(k)(k = 1,2,\cdots,l)$ 和 $z_j(k)(k = 1,2,\cdots,l)$ 中的元素差异较大时,则它们的相似度较低。ALCH 模型中采用灰度关联分析理论,计算两条量测序列的灰色关联度,以量化各检测点在检测序列的相似程度,并构造相似度矩阵。

当某时刻 $l$,检测点 $i$ 和检测点 $j$ 的检测序列灰色关联度为 $a_{ij}(l)$,则有:

$$a_{ij}(l) = \begin{cases} 1, & i = j \\ \dfrac{1}{l}\sum\limits_{k=1}^{i} \dfrac{\min\limits_j \min\limits_k |z_i(k) - z_j(k)| + \rho \max\limits_j \max\limits_k |z_i(k) - z_j(k)|}{|z_i(k) - z_j(k)| + \rho \max\limits_j \max\limits_k |z_i(k) - z_j(k)|}, & i \neq j \end{cases} \tag{3}$$

至此,可得到该时刻的检测点中的灰色关联度(相关度)矩阵 $\boldsymbol{GM}(l)$:

$$\boldsymbol{GM}(l) = \begin{bmatrix} 1 & a_{12}(l) & \cdots & a_{1n}(l) \\ a_{21}(l) & 1 & \cdots & a_{2n}(l) \\ \vdots & \vdots & & \vdots \\ a_{n1}(l) & a_{n2}(l) & \cdots & 1 \end{bmatrix} \tag{4}$$

此时,如该式(4)中矩阵的第 $i$ 行元素之和较大,表明 $l$ 时刻第 $i$ 个检测点的观测结果与多数检测点接近或类似;反之表明,第 $i$ 个检测点的观测结果产生了较大的偏差。

### 2.4　基于一致性度量的融合

以 2.3 节中的灰色关联度矩阵为基础,通过累加可得第 $i$ 个检测点的检测序列与其他检测结果的一致关联度为 $r_i(l)(0 < r_i(l) < 1)$:

$$r_i(l) = \frac{\sum\limits_{j=1}^{n} a_{ij}(l)}{n} \tag{5}$$

式(5)中的关联度的实质是参考序列与比较序列的点对点之间距离的反映,从而在一定程度上揭示了信息变化时的依赖关系。式(1)反映了在某个观测时刻,两个检测点观测序列的接近程度;式(4)反映了在某个观测时刻,第 $i$ 个检测点的检测序列与其他检测序列的接近程度。综合上述两部分内容,在某时刻 $l$,事件特征向量融合结果可以描述为:

$$\hat{X}(l) = \left(\sum_{i=1}^{n} r_i(l) z_i(l)\right) \Big/ \left(\sum_{i=1}^{n} r_i(l)\right) \tag{6}$$

### 2.5　基于功率谱估计的预告警算法

2.4 节中通过信息融合产生了洗钱事件序列式(6),其规模和内容将随时间不断增加,通过一段时间积累后,反洗钱模型中的相关信息从内容到数量上均呈现相对稳定的状态,但相关信息仍非常有限,此时,ALCH 模型将采用基于功率谱估计的反洗钱预告警方法予以处理。该方法目前主要用于研究频域中的各种变化对象;它能够根据有限的原始信息,提取噪声中不断变化的状态,因此非常适用于事件发展的估计与预测工作。实际应用中,洗钱事件的功率谱是由特定信息的各个频率分量(事件特征向量中的各元素)融合而成的功率;因此,当各个分量的功率为事件特征向量中的不同频率元素(见 2.1 节的描述)在整个洗钱过程中所起到的作用,即:如果高频部分功率较大,则对应事件元素的变动速率将会较高;反之亦然。

ALCH 模型中的洗钱预告警算法基于客户在大额支付系统中的活动。当 ALCH 模型对某客户进行跟踪时,不断将其操作等信息汇总成事件元素传送至各检测点;在完成基本的信息筛选、过滤和预处理后,进行灰色关联度计算,并记录在信息库中;经过一定时间的信息积累,洗钱事件分析模块将整合该客户既往的事件特征元素,根据功率谱密度估计方法,对其洗钱的可能性进行评判,具体方法如下。

$\Phi_{xx}(m)$ 表示特定客户的洗钱事件特征 $x(n)$ 的自相关函数;$P_{xx}(m)$ 表示其功率谱密度,则有:

$$P_{xx}(\omega) = \sum_{m=-\infty}^{\infty} \varphi_{xx}(m) e^{-j\omega m}$$

其中:

$$\varphi_{xx}(m) = \lim_{N\to\infty} \frac{1}{2N+1} \sum_{n=-N}^{N} x(n) x^*(n+m)$$

代入后可得:

$$P_{xx}(\omega) = \lim_{N\to\infty} \frac{1}{2N+1} \left[\sum_{n=-N}^{N} x(n) e^{-j\omega n}\right] \cdot \left[\sum_{m=-\infty}^{\infty} x^*(n+m) e^{j\omega(n+m)}\right]$$

进而求平均,即为:

$$P_{xx}(\omega) = \lim_{N\to\infty} E\left[\frac{1}{2N+1}\left|\sum_{n=-N}^{N} x(n) e^{j\omega n}\right|^2\right] \tag{7}$$

在实际的评判运算中,由于洗钱活动的连续性,对于大额

支付系统中的反洗钱检测模型，均只能得到其事件序列中的一个信息子序列，而不是完整的全序列；所以，ALCH 模型采用了有限信息序列来估计它的功率谱密度。设该特征的有限信息序列为：$x(0),x(1),x(2),\cdots,x(N)$，则有：

$$\hat{\varphi}_{xx}(m) = \frac{1}{N}\sum_{n=-\infty}^{\infty} x_N(n)x_N(n+m) \tag{8}$$

$$\hat{P}_{xx}(\omega) = \sum_{m} \hat{\varphi}_{xx}(m)e^{-j\omega m} \tag{9}$$

式(8)和(9)中，就事件特征向量的分量(元素)而言，以“动作”(Action)分量为例：当某客户对参与洗钱活动时，将会有大量与常规操作相反相悖，或与洗钱发现规则相同相似的操作的信息注入该分量，则上述两个方向上的分量更新频率的绝对值之和激增，即可用于客户及其相关事件的洗钱评判。

## 3 仿真验证结果与分析

本模型的性能验证仿真由虚拟央行数据库(Virtual Central Bank Data Base, VCBDB)提供测试数据集，并与基于分布式的、非实时数据挖掘的反洗钱模型 ALDM(Anti-Laundering of Data Mining)性能对比[14]。限于微机仿真的系统容量与处理能力，仿真实验对象为 VLFDB 数据库中的(由计算机系统随机选用)15 个银行支付清算机构，2 493 名客户，其中参与洗钱犯罪的客户为 133 名；与这些客户相关的金融操作共计4 502 747条(含开户与销户等客户生灭操作)，其中涉及洗钱的事件项目共 4 139 条。

在仿真测试中，通过仿真 16 个反洗钱检测点(含备用检测点 1 个)，对比了两种模型的如下性能：1)洗钱客户发现覆盖度；2)洗钱客户发现精确度；3)洗钱事件召回率。

文献[12]给出的传统洗钱客户发现覆盖度可以定义为：反洗钱模型发现的洗钱客户集对最终的洗钱客户集合的最终静态覆盖程度[13]；实际的应用中，整个洗钱犯罪过程是动态的，其中的金额、客户以及事件本身都存在数量上的增减(例如：洗钱客户账户的添加、销户、隶属变更等)，这种增减随时序而变化，为更有效地测试两种模型的洗钱发现能力，仿真测试中通过定时监测的方式，对两种模型在运行过程中的洗钱客户覆盖率进行了跟踪，动态的洗钱客户发现覆盖度为：$Coverage(t) = (RS(t) \cap RR(t))/RS(t)$，其中：$t \geqslant 0$，$RS(t)$为整个大额支付系统在 $t$ 时刻的实际洗钱客户数量，而 $RR(t)$为系统中 $t$ 时刻已确定的洗钱客户数量。

洗钱客户发现精确度定义为：被标记告警的、确有洗钱行为客户数目占被标记告警的客户总数的比例。

洗钱事件召回率定义为：被标记告警的、实际的洗钱事件占实际发生的洗钱事件总数的比例。

从图 2(其中每 12 h 为一个检测周期)中可知：随着模型应用的延续，各系统中的客户数目不断增加，其中的活动也不断增加，不断暴露出洗钱痕迹，所以两种模型的洗钱客户发现覆盖度均不断增加，直至达到或接近其最大值。由于模型结构的优化和改进关键算法的使用，从覆盖的速度来看，ALCH 模型具有明显优势；如图 2 所示，本文模型在较短的时间段内，实现较高的洗钱客户发现覆盖率，与 ALDM 模型相比，具有较好的洗钱犯罪发现能力。

洗钱客户发现精确度随着被发现并处理的洗钱客户的数目而不断变化，两种反洗钱模型的客户发现精确度在达到各自的极值(总体客户数量趋于稳定)后，均将开始下降。从图3中可见，ALCH 模型的精确度极值高于 ALDM 模型，且随后的精确度下降速度也较为缓慢，体现了较好的总体发现精度。

在洗钱事件召回率方面，随着被告警的洗钱事件不断增加，两种反洗钱的模型的召回率不断随着客户数量的变化而变化。当客户总数趋于稳定时，洗钱事件召回率也逐渐平稳。从图 4 中可以看出，由于关键算法的处理精度和效率较高，使得 ALCH 模型的召回率一直高于 ALDM 模型。

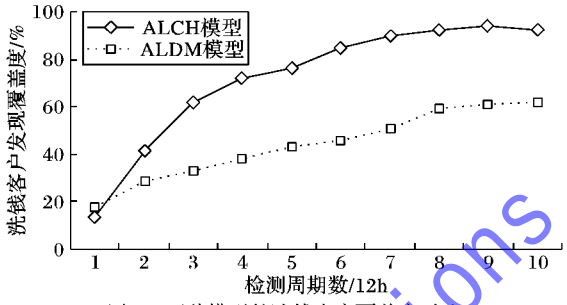


图 2 两种模型的洗钱客户覆盖度对比

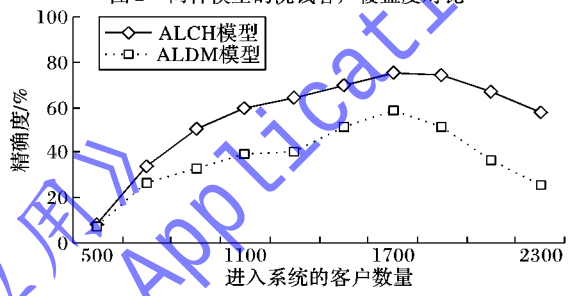


图 3 两种模型的洗钱客户发现精确度对比

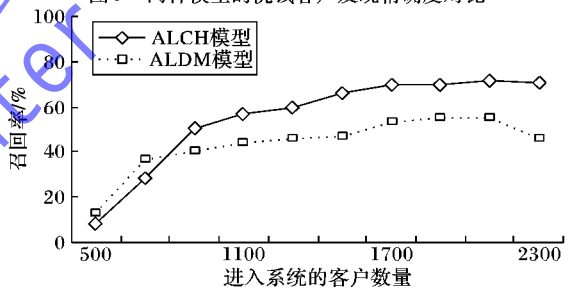


图 4 两种模型的洗钱事件召回率对比

## 4 结语

本文针对中央银行大额支付系统环境，研究并提出了新型的反洗钱管理模型(ALCH)的结构与管理流程，并研究了应用其中的关键算法，包括：针对局部视图问题，提出了基于灰色关联度的信息融合算法；针对洗钱犯罪识别中的信息完整性问题，提出了基于功率谱的识别算法。本文模型具有较高的反洗钱性能。仿真测试表明，ALCH 模型的精度、效率以及召回率均较高，有限信息利用率较高，具有一定的应用价值。未来的研究内容将集中在功率谱识别算法的性能提高、反洗钱规则信息库的标准化等。

**参考文献：**

[1] NIKOLOSK S, SIMONOVSKI I. Role of banks as entity in the system for prevention of money laundering in the Macedonia [C]// Proceedings of the 11th International Conference on Service Sector in Terms of Changing Environment. Amsterdam: Elsevier, 2012: 453-459.

[2] BARONE R, MASCIANDARO D. Organized crime, money laundering and legal economy: theory and simulations [J]. European Journal of Law and Economics, 2011, 32(1): 115-142.

[3] UNGER B, HERTOG J D. Water always finds its way: identifying new forms of money laundering [J]. Crime, Law and Social Change, 2012, 57(3): 287-304.

(下转第 878 页)

模型:理论回顾及其评论[J].管理评论,2011,23(9):144 -151.)

[2] ZHANG L, WANG Y, LIU J. Forewarning model of listed companies against financial crisis based on Bayesian discrimination [J]. Commercial Research, 2009(4): 112 -114.(张立军,王瑛,刘菊红.基于贝叶斯判别分析的上市公司财务危机预警模型研究[J].商业研究,2009(4):112 -114.)

[3] ZHU Y, YAO Y, ZHANG Y. Research on financial crisis pre-warning model of listed company based on PCA and Logistic regression [J]. Journal of Zhejiang University of Technology, 2012, 40(6): 692 -694,689.(朱永忠,姚烨,张艳.基于主成分分析和 Logistic 回归的上市公司财务困境预警模型的研究[J].浙江工业大学学报,2012,40(6):692 -694,698.)

[4] YANG S, WANG L. Research on financial warning for listed companies by using BP neural networks and panel data [J]. Systems Engineering—Theory & Practice, 2007, 27(2): 61 -67.(杨淑娥,王乐平.基于 BP 神经网络和面板数据的上市公司财务危机预警[J].系统工程理论与实践,2007,27(2):61 -67.)

[5] LIU Z, HUANG Z, YAN F, *et al*. Financial failure prediction using support vector machine with *Q*-Gaussian kernel [J]. Journal of Computer Applications, 2013, 33(6): 1767 -1770.(刘遵雄,黄志强,晏峰,等.*Q*-高斯核支持向量机的财务危机预报[J].计算机应用,2013,33(6):1767 -1770.)

[6] ZHANG H, LIU W. The application of combining forecasts in the early-warning of listed company's financial risk [J]. Friends of Accounting, 2011(2): 101 -102.(张红梅,刘文蕊.组合预测在上市公司财务预警中的应用[J].会计之友,2011(2):101 -102.)

[7] MIN J H, LEE Y. Bankruptcy prediction using support vector machine with optimal choice of kernel function parameters [J]. Expert Systems with Applications, 2005, 28(4): 603 -614.

[8] WANG B, LI N. Research of predicting financial distress [J]. Journal of Nanjing University of Aeronautics and Astronautics: Social Sciences, 2007, 9(3): 61 -64.(王宝富,李南.财务困境的预测研究[J].南京航空航天大学学报:社会科学版,2007,9(3):61 -64.)

[9] ZHANG H H, AHN J, LIN X, *et al*. Gene selection using support vector machines with non-convex penalty [J]. Bioinformatics, 2006, 22(1): 88 -95.

[10] FAN J, LI R. Variable selection via nonconcave penalized likelihood and its oracle properties [J]. Journal of the American Statistical Association, 2001, 96(456): 1348 -1360.

[11] WU Y, LIU Y. Robust truncated hinge loss support vector machines [J]. Journal of the American Statistical Association, 2007, 102(479): 974 -983.

[12] ZHU J, ROSSET S, HASTIE T, *et al*. 1-norm support vector machines [C]// Advances in Neural Information Processing Systems. Cambridge, MA: MIT Press, 2004: 49 -56.

[13] TORII Y, ABE S. Decomposition techniques for training linear programming support vector machines [J]. Neurocomputing, 2009, 72(4/5/6): 973 -984.

[14] LIU Y, SHEN X, DOSS H. Multicategory $\psi$-learning and support vector machine: computational tools [J]. Journal of Computational and Graphical Statistics, 2005, 14(1): 219 -236.

[15] ZHENG D, HUANG K. CSL: a comprehensive sparse learning package [EB/OL]. [2013-06-20]. http://www.enm.bris.ac.uk/staff/xkh/CSL1.0.rar.

[16] CHANG C, LIN C. LIBSVM: a library for support vector machines [J]. ACM Transactions on Intelligent Systems and Technology, 2011, 2(3): 1 -27.

[17] DUDA R O, HART P E, STORK D G. Pattern classification [M]. 2nd ed. Hoboken, NJ: Wiley, 2000.

(上接第 872 页)

[4] SHEHU A Y. Promoting financial inclusion for effective anti-money laundering and counter financing of terrorism (AML/CFT) [J]. Crime, Law and Social Change, 2012, 57(3): 305 -323.

[5] SHARMAN J C, CHAIKIN D. Corruption and anti-money-laundering systems: putting a luxury good to work [J]. Governance, 2009, 22(1): 27 -45.

[6] DOLAR B, SHUGHART W F, II. Enforcement of the USA patriot act's anti-money laundering provisions: have regulators followed a risk-based approach [J]. Journal of Global Finance, 2011, 22(1): 19 -31.

[7] VLCEK W. Global anti-money laundering standards and developing economies: the regulation of mobile money [J]. Development Policy Review, 2011, 29(4): 415 -431.

[8] DREEWSKI R, SEPIELAK J, FILIPKOWSKI W. System supporting money laundering detection [J]. Digital Investigation, 2012, 9(1): 8 -21.

[9] VANDANA P, LI J H, GAO P. A framework for preventing money laundering in banks [J]. Information Management and Computer Security, 2012, 20(3): 170 -183.

[10] PENG W B. Research on money laundering crime under electronic payment background [J]. Journal of Computers, 2011, 6(1): 147 -154.

[11] BAK J, JEDRZEJEK C, FALKOWSKI M. Application of an ontology-based and rule-based model to selected economic crimes: fraudulent disbursement and money laundering [C]// Proceedings of the 2010 International Conference on Semantic Web Rules. Berlin: Springer-Verlag, 2010: 210 -224.

[12] BYRNE J J. How IT auditing fights money laundering [J]. Journal of Corporate Accounting and Finance, 2011, 22(5): 63 -67.

[13] CAO D K, DO P. Applying data mining in money laundering detection for the Vietnamese banking industry [C]// Proceedings of the 4th Asian Conference on Intelligent Information and Database Systems, LNCS 7197. Berlin: Springer-Verlag, 2012: 207 -216.

[14] LE-KHAC N, MARKOS S, KECHADI M T. Towards a new data mining-based approach for anti-money laundering in an international investment bank [C]// Proceedings of the First International ICST Conference on Digital Forensics and Cyber Crime. Berlin: Springer-Verlag, 2010: 77 -89.

[15] OUYANG W. Chinese anti-money laundering crime preliminary typology [M]. Beijing: Law Press, 2007.(欧阳卫民.中国反洗钱犯罪类型学初探[M].北京.法律出版社.2007.)

[16] YU W, WANG J. Suspicious money laundering detection system based on eigenvector centrality measure of transaction network [J]. Journal of Computer Applications, 2009, 29(9): 2581 -2585.(喻炜,王建东.基于交易网络特征向量中心度量的可疑洗钱识别系统[J].计算机应用,2009,29(9):2581 -2585.)