海南农商银行人脸识别系统人工智能算法

金融应用信息披露报告

一、重要提示

本报告是依据《人工智能算法金融应用信息披露指南》对披露人工智能算法应用情况的要求，就海南农商银行基于人工智能算法提供的金融产品和服务情况进行说明，并通过我行官网进行披露。

二、基本情况

（一）机构简介

海南农村商业银行股份有限公司（以下简称海南农商银行）是在原海南省农村信用社联合社和19家市县法人农信社（农商银行）基础上，采取新设合并方式组建而成，是全国首家按照全省统一法人模式改革成立的地方法人银行，其前身可溯至1951年琼山区美兰椰子头信用社，拥有74年扎根守土历史。新组建的海南农村商业银行，注册资本金220亿元，总行内设19个部门，下辖总行营业部和18家一级支行,440余家营业网点,员工7000余人。

（二）人工智能算法应用情况

产品名称：人脸识别系统

服务内容：为行内各个业务渠道（系统）提供人脸识别、活体检测服务，提高业务办理效率，方便客户办理相关业务。

三、人工智能算法金融应用风险治理情况

（一）组织保障

海南农商银行按照《海南农村商业银行股份有限公司信息化项目建设实施管理办法》要求，成立人脸识别系统建设项目组，项目组由项目经理和项目成员组成，其中项目成员包括科技人员和业务人员共9人。项目组按照科学规划、严谨设计、周密部署、精心组织的原则，扎实有效推进项目建设。项目负责落实人工智能算法相关数据治理与隐私保护、模型风险和法规遵从与行业标准等方面的组织保障措施，研究、解决项目实施遇到的问题和困难，稳步推进项目进程。

（二）实施情况

人脸识别系统建设项目组组织项目组科技人员和业务人员对人脸识别、活体检测人工智能技术应用风险进行专项治理，根据法规遵从与行业标准要求，对人工智能技术在金融产品智能服务过程中，在技术应用方面、数据安全方面、系统风险方面以及科技伦理等方面进行风险控制设计与风险排查，确保系统人工智能技术应用安全可控，项目实施中发现问题均已完成整改。

四、人工智能算法技术应用信息披露

（一）算法组合信息披露情况

算法组合信息披露是对金融产品和服务所集成的全部人工智能模型算法组合使用情况的整体说明，算法组合信息披露情况见表1。

表1 算法组合信息披露情况

披露分类	披露项	信息披露内容
算法组合信息披露	算法组合单	算法组合清单包含两类人工智能算法：人脸比对算法、活体识别算法
	算法组合使用的开发框架	算法组合使用 pytorch2 开发框架，python3 开发语言
	算法组合使用的开源库	算法组合使用 opencv、tensorRT、numpy、c++的开源软件库
	算法组合调度机制	人脸识别输入照片后可与底库人员进行比对得出相似度、活体识别通过前端 SDK 输出报文信息，活体引擎分析后得出真人判断。
	算法组合触发条件	所有算法均为集成客户主动控制触发。
注： 1.PyTorch2 是一个由 Facebook 发布的用于机器学习和深度学习的开源		

深度学习框架。

2. NumPy 是 Python 的一个基础科学计算库。

3. Python3 为解释型的编程语言。C++为编译型的编程语言。

4. TensorRT 是 NVIDIA 推出的一个高性能深度学习推理优化器和运行时库。

5. OpenCV 是一个开源的计算机视觉和机器学习软件库。

（二）算法逻辑信息披露情况

算法逻辑信息披露是对组合中的每个算法对象逐一说明算法机理，算法逻辑信息披露情况见表 2。

表 2 算法逻辑信息披露情况

披露分类	披露项	信息披露内容

算法逻辑信息披露	算法功能说明	人脸比对算法：人脸识别算法用于通过分析人脸的特征来识别或验证一个人的身份。它通过检测人脸特征点（如眼睛、鼻子、嘴巴的相对位置）来构建每个人独特的人脸模型，从而进行身份匹配或访问控制。 活体识别算法：活体识别算法用于验证被识别对象是否为真实的活体，而不是照片、视频或其他伪造品。该算法通过检测面部特征、眼睛的眨动、微表情、头部表情、头部运动等生理特征这项技术常用于金融支付、手机解锁、机场安检等需要高安全性的场景，防止欺诈行为，例如使用照片或视频冒充身份。
	算法推理过程说明	人脸比对： 系统会从人脸图片中提取一组高维、独特的特征向量，用于表征身份。 活体识别： 1）生理信号：通过分析人脸皮肤因心跳导致的席位颜色变化来检测心率等生命体征。 2）纹理与运动特征：分析皮肤的纹理细节以及面部动作的自然连贯性。

	算法推理结果说明	人脸比对：人脸相似度比对是否与底库人员或联网核查人员一致。 活体识别：检测结果是否为真人。
	算法技术路线选择说明	人脸识别：针对人脸局部和全局空间区域反复进行特征抽象，挖掘以上特征的项目关系，进而精准地融合形成最终的人脸特征。 活体识别：为了提升活体检测对不同攻击的泛化性能，通过对抗攻击的方式不断探索模拟新的攻击方式，并优化防守检测的特征，提升活体检测的安全性及用户体验。
	算法技术成熟度说明	人脸比对、活体识别均为成熟算法技术，在银行金融业中广泛使用。
	算法重构条件说明	为了进一步提升人脸比对算法、活体识别算法，可进一步通过多模态注意力模型预测空间中最感兴趣的区域，并对其进行深度挖掘。

	算法假设条件说明	算法开发需要采用训练服务器，并对数据进行手动或自动化的标注
	算法使用限制说明	人脸比对与活体识别算法需要保证面部信息的完整性，如面部缺陷残疾会导致无法识别或体验较差。
	算法参数及超参数说明	算法输入参数主要是图片，算法输出参数主要包括人脸特征比对结果、活体识别结果。

（三）算法应用信息披露情况

算法应用信息披露是与人工智能算法金融应用场景相关信息的说明，避免因对算法应用的错误理解而误导客户，信息披露情况见表 3。

表 3 算法应用信息披露情况

披露分类	披露项	信息披露内容
算法应用信息披露	算法应用场景	算法输入参数主要是图片，算法输出参数主要包括人脸特征比对结果、活体识别结果。
	算法应用目的	人脸比对与活体识别主要提升身份鉴别的体验，确保当前用户为合法使用者等。

	算法应用服务范围	人脸比对与活体识别主要应用于用户身份鉴别，具体使用范围由集成方决定。
	算法应用服务前提	活体识别需要手机 APP 或网页集成前端采集 SDK，并部署后端分析引擎。
	算法应用获得渠道	人脸识别系统的算法模型应用从供应商下载私有化部署包。
	算法应用潜在风险和防护措施	人脸比对与活体识别算法需要保证面部信息的完整性，如面部缺陷残疾会导致无法识别或体验较差。
	算法应用必要性	人脸比对算法和活体识别算法为较为普遍的人员信息鉴别技术。

	算法应用预期效果	人脸对比技术可对两张人脸进行对比，得到两张人脸的相似度，从而判断是否是同一个人；活体检测技术可对采集到的视频进行识别，从而判断是否是活人。活体检测准确率可达 92%，人脸识别准确率可达 95%，有效提高行内各渠道涉及的相关业务办理效率。

（四）算法数据信息披露情况

算法数据信息披露是对算法使用的数据来源、数据采集、数据质量控制以及数据与场景的关联性进行充分说明，信息披露情况见表 4。

表 4 算法数据信息披露情况

披露分类	披露项	信息披露内容
算法数据信息披露	算法数据与金融应用相关性说明	人脸比对与活体识别主要应用于用户身份识别，相关性主要为金融领域用户人脸信息
	算法数据来源说明	算法调优、测试数据集主要来源于我行历史数据集。

	算法数据采集说明	算法模型涉及的调优数据、测试数据、推理数据均已经数据所有者（控制者）授权，采用去标识化进行脱敏处理，脱敏后无法直接关联真实客户身份。
	算法数据质控说明	具备健全严格的算法数据质量管理制度，覆盖数据采集、数据清 洗、数据整理、数据标注、数据集构建各个环节，保障算法数据的完整性、一致性，数据分布的合理性、无偏性，数据样本的充足性，数据操作的规范性、合规性。
	算法组合使用的第三方软件产品	不涉及

（五）算法主体信息披露情况

算法主体信息披露是对人工智能算法金融应用服务提供者建立的算法管理相关机制（安全保障、风险防范、伦理治 理等机制）的说明，信息披露情况见表 5。

表 5 算法主体信息披露情况

披露分类	披露项	信息披露内容
算法主	算法主体建立安全	我行建立健全数据使用管理办法、敏

体信息披露	保障机制说明	感信息内控管理制度，明确各环节责任分工，为人脸识别系统提供算法安全保障和数据安全保障。人脸识别场景模型部署环境属于生产环境，且有操作日志保存，保障推理过程安全。生产环境模型有应急处理机制，遇到任何上线失败情况可立刻回退。
	算法主体建立风险防范机制说明	我行建立产品创新管理办法、数据使用管理办法，形成“事前审核准入、事中监控预警、事后处置问责”的风险防范及补偿机制，作为智能客服的责任主体确保客户权益得到有效保障。
	算法主体建立伦理治理机制说明	我行成立产品创新委员会和产品创新办公室，审议本行涉及业务创新、技术创新的管理制度，审议数字化转型过程中的模式创新、机制创新等方案和制度。
	算法主体建立信息披露组织实施保障措施说明	建立健全严格的算法数据质量管理制度，覆盖数据采集、数据清洗、数据整理、数据标注、数据集构建各个环节，保障算法数据的完整性、一致性，数据分布的合理性、无偏性，数据样本的充足性，数据操作的规范性、合规性。同时建立完善的信息披露内部管理制度和流程，明确信息披露的责任部门和工作要求，确保信息披露及

		时、准确、完整。

（六）算法变更信息披露情况

人工智能算法金融应用采用在线实时服务，由于人工干预程度越少，服务及其策略的调整可能更加频繁快速，可能引发风险性活动，应运用与之匹配的实时监测技术并及时披露相关调整以及变更信息，信息披露情况见表6。

表6 算法变更信息披露情况

披露分类	披露项	信息披露内容
算法变更信息披露	算法变更版本号	云之盾引擎V1.3.2.20250709更新内容： 1. 升级深伪模型：通过增强不同场景和市面上新增AI合成软件合成样本的训练数据，持续优化深伪检测能力，相较于0523版本提升0.4%左右。 2. 升级翻拍模型：通过新增翻拍数据进行专项训练，优化算法模型，提升高

	算法变更原因说明	清屏幕翻拍检测能力。 3. 升级纸张面具模型：加入近期收集真实攻击数据和制造数据对当前模型进行持续升级，用加强防御纸张面具攻击场景。 4. 增加水印检测模型：在一些深伪攻击中，经常带有一些生成软件打的水印，通过检测水印特征进行针对性防御。 5. 升级背景检测模型：优化特征提取算法和增加训练数据，提升背景检测的准确率，减少误识情况。 6. 提升老人通过率：通过优化 3D 面具识别模型，减少老人识别场景的误识率，60 岁老人通过率相较于 0523 版本提升 3%左右。
	算法变更影响说明	
	算法变更生效时间	
	算法变更实施说明	提前对算法效果与稳定进行预发测试，通过后在正式环境上线。
	算法变更保障措施	对算法上线后的效果进行监督，如存在效果不理想或存在其他生产问题可及时对上线版本进行回退。

（七）算法审计信息披露情况

人工智能算法金融应用涉及数据、算力、场景等多种要素的深度融合与交互，一定程度上增加了算法金融应用的风 险。为保证金融产品和服务的业务连续性，降低技术风险、操作风险，有必要对人工智能算法金融应用进行合规性审计，并及时将算法审计活动所依据的政策、法规、标准等信息以及审计结果进行说明，信息披露情况见表 7。

表 7 算法审计信息披露情况

披露分类	披露项	信息披露内容
算法审计信息披露	算法审计依据	依据《人工智能算法金融应用信息披露指南》、《海南农村商业银行股份有限公司开源技术应用管理实施细则》、《海南农村商业银行股份有限公司信息化项目建设实施管理办法》等政策法规和内部制度开展算法审计工作。
	算法审计信息	1.上线前，利用算法对抗鲁棒性测试工具进行自动化算法审计，审计活动覆盖算法安全漏洞扫描、算法逻辑漏洞扫描等方面；所有严重和一般问题已完成整改。 2.上线前，依据相关管理制度进行算法审计，审计活动覆盖算法公平性、
	审计内容说明	
	算法审计结论	
	算法审计频率	

		算法可解释性、算法鲁棒性等方面。 3.上线后，依据相关内部制度开展算法跟踪审计，审计活动覆盖算法运行情况、算法安全风险事件、算法合规情况等方面。 通过算法审计活动，确认人脸识别算法组合满足算法上线条件，在运行过程中符合国家及行业相关规范和我行内部管理制度要求，未发现重大违法违规问题和安全风险隐患。

五、重大事项

报告期内，海南农商银行无人工智能算法金融应用业务相关的重大诉讼、仲裁事项。

报告期内，海南农商银行未发生人工智能算法金融应用业务相关的重大案件、重大差错等情况。