

| 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   | 算法组合清单      | 人脸比对算法、活体识别算法、OCR识别算法                                                             |
|            | 算法组合使用的开发框架 | 算法使用pytorch2的开发框架，python3的开发语言                                                    |
|            | 算法组合使用的开源软件 | 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；OCR将照片输入引擎后输出照片上包含的文本信息。 |
|            | 算法组合触发条件    | 所有算法均为集成客户主动控制触发。                                                                 |

| 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。<br>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、视频或其他伪制品。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。<br>OCR识别算法：算法用于将图片中的文本转换为可编辑、可搜索的文字。它通过分析图片中的字形、结构和排列，识别出其中的字符并将其转换为可编辑、可搜索的文字。 |
|            | 算法技术路线选择说明 | 采用当前人工智能领域广泛使用的深度学习技术，对人脸比对、活体识别、OCR识别进行建模。<br>1. 人脸比对：针对人脸局部和全局空间区域反复进行特征抽象，挖掘以上特征的相互关系，进而精准地融合形成最终的人脸特征。<br>2. 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。<br>3. OCR识别：通过对预训练模型迁移学习的方式，降低不同字体差异的影响，同时建立“所标即所得”的自动化数据处理及训练流程，降低不同版式的定制化成本，并自动进行语义结构化，降低识别的成本及门槛。                         |
|            | 算法技术成熟度说明  | 人脸识别、活体检测、OCR识别算法均为成熟算法技术，目前已在金融领域业广泛使用。                                                                                                                                                                                                                                                                                |
|            | 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、OCR识别算法，可进一步通过多模态注意力模型预测空间中最关键的区域，并对其进行深度挖掘。                                                                                                                                                                                                                                                       |
|            | 算法假设条件说明   | 算法开发需要对数据进行手动或自动化的标注。                                                                                                                                                                                                                                                                                                   |
|            | 算法使用限制说明   | 人脸识别与活体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；OCR识别需要保证识别信息清晰可见，但对于部分手写体或字迹潦草或特殊格式识别效果较差。                                                                                                                                                                                                                                   |
|            | 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、OCR识别结构化的字符或字段结果。                                                                                                                                                                                                                                                                 |
|            |            |                                                                                                                                                                                                                                                                                                                         |
|            |            |                                                                                                                                                                                                                                                                                                                         |

| 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   | 人脸识别与活体识别主要用于人员身份鉴别场景，如手机APP登陆、信息查询等；OCR主要应用于卡证填入、纸质文档转变电子文档等。           |
|            | 算法应用目的   | 人脸识别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；OCR目的为将纸质信息转为电子文档等。                    |
|            | 算法应用服务范围 | 人脸识别与活体识别主要应用于在手机银行、柜面办理业务时，对客户身份的鉴别；OCR主要应用于图片信息转文字信息，具体范围为交付OCR引擎种类为准。 |
|            | 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；OCR需要部署后端分析引擎。                         |
|            | 算法应用获得渠道 | 由人脸识别系统服务商提供。                                                            |

|  |               |                                                                                       |
|--|---------------|---------------------------------------------------------------------------------------|
|  | 算法应用潜在风险和防护措施 | 人脸识别与活体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；OCR识别需要保证识别信息清晰可见，但对于部分手写体或字迹潦草或特殊格式识别效果较差。 |
|  | 算法应用必要性       | 人脸识别算法和活体检测算法为较为普遍的人员信息鉴别技术；OCR也是常用的识别技术，可减少用户录入操作，提升用户体验。                            |
|  | 算法应用预期效果      | 十万分之一误识率下，通过率不低于99%<br>百万分之一误识率下，通过率不低于98%<br>千万分之一误识率下，通过率不低于97%                     |

| 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 | 人脸识别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；OCR识别相关数据为金融行业特定的卡证如银行卡信息或其他金融文件。                              |
|            | 算法数据来源说明       | 算法模型涉及的训练数据、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。                              |
|            | 算法数据采集说明       | 通过授权相机采集用户的影像信息与卡证信息，影像信息但不涉及到算法训练                                                                   |
|            | 算法数据质控说明       | 具备健全严格的算法数据质量管理体系，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 | 无                                                                                                    |

| 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  | 1、云之盾V1.1.8 2024-07-03<br>(1) 升级炫彩模型 提升炫彩的真人通过率和防攻击能力<br>(2) 针对近期出现的攻击事件进行优化处理<br>2、云之盾V1.1.7 2024-04-22<br>(1) 升级活体深伪模型到1218GR3D<br>(2) 升级光线模型, 提升真人通过率和防注入攻击能力<br>(3) 修改SDK的报文解析部分与检测逻辑，解决内存上涨问题;修改光线数据错误报错问题<br>(4) 新增风险背景和视线注意力开关 |
|            | 算法变更原因说明 | 3、云之盾V1.1.6 2023-11-23<br>(1) 提升了增加了补充mask3d模型，用于拦截仿真头模<br>(2) 提升了补充拼接图模型整体的真人通过率<br>(3) 提升了对e4s这类拼接图攻击的拦截<br>(4) 新增风险背景检测<br>(5) 新增历史指纹数据提升防注入攻击能力，调整光线阈值等级默认为4                                                                      |
|            | 算法变更影响说明 |                                                                                                                                                                                                                                       |
|            | 算法变更生效时间 |                                                                                                                                                                                                                                       |
|            | 算法变更实施说明 | 对于算法变更，我行严格遵照《石嘴山银行信息科技运行维护管理办法》以及《石嘴山银行信息科技变更管理实施细则》的要求，完成审批流程，制定回退计划和应急方案，并有详细的记录。                                                                                                                                                  |
|            | 算法变更保障措施 | 对算法的变更，在上线后开展功能验证，并持续进行效果监督，如存在效果不理想或其他生产问题，将及时对上线版本进行回退。                                                                                                                                                                             |