CFCA

人工智能
在金融信息安全领域的应用探讨

一个中型公司的 AI 落地之路

李　闯
中国金融认证中心
2018.4

GTLC
GLOBAL
TECH LEADERSHIP
CONFERENCE

全球技术领导力峰会

通往**年薪百万**的CTO的路上，

如何打造自己的技术**领导**力？

扫描二维码了解详情

目录页

CONTENTS PAGE

展示厅

CFCA

工程项目

- OCR、笔迹鉴定
- 客户端行为分析
- 交易反欺诈系统

研究性项目

- AI模拟人类手写笔迹
- 基于机器学习的攻击手段

工程1 手写汉字的识别

CFCA

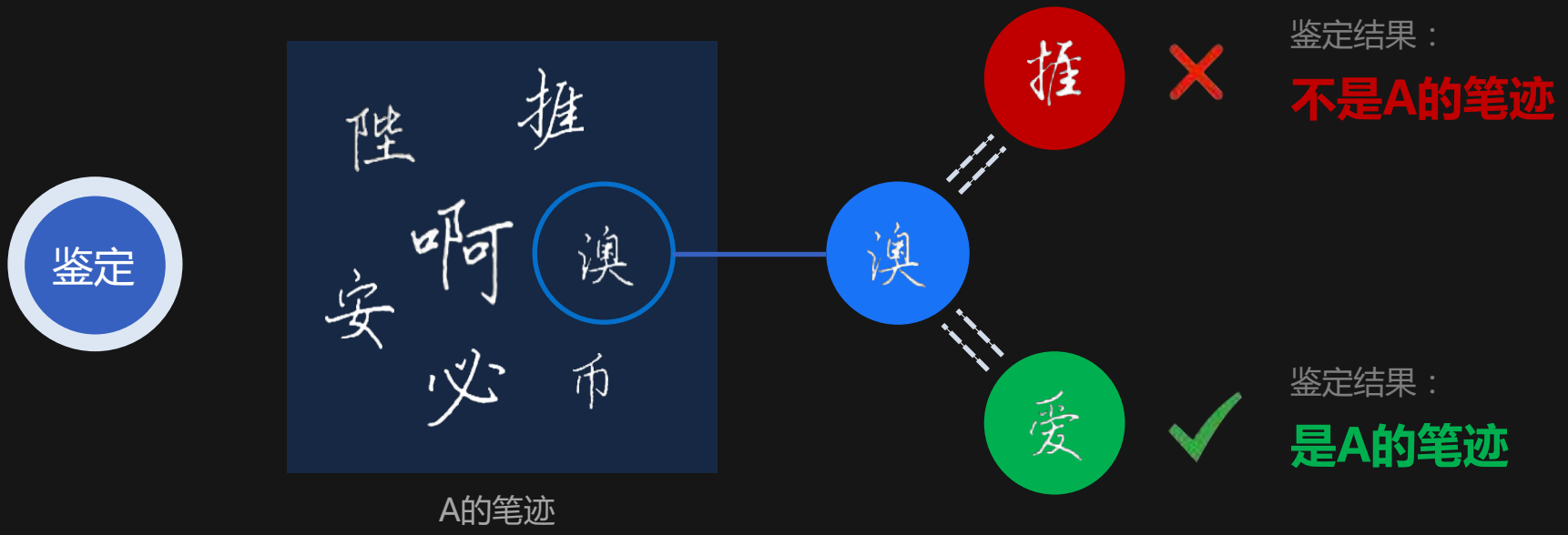
识别

深度学习模型能学到
人类的知识

中科院HWDB竞赛数据
准确率 **97.04%**

工程1 手写汉字的鉴定

CFCA



无关字符笔迹鉴定准确率 > 85%

工程1 手写汉字的鉴定

CFCA

鉴定

请签署您的名字：李明

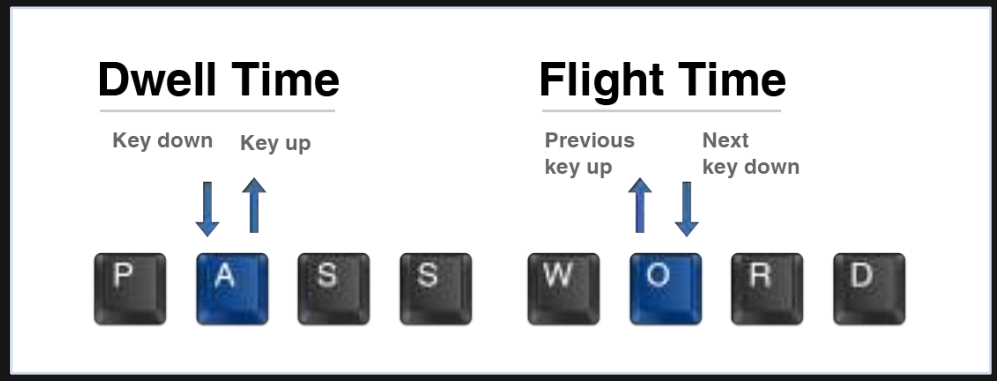
手写图片：

签名合法！

手写签名的笔迹鉴定准确率 > 96%

工程2 客户端行为分析

CFCA



工程2 行为分析的新形式

人工智能技术的
突破式发展

移动互联网更多的
行为特征

基于人机交互的
智能生物识别的技术基础

工程2 CFCA的研究进展

123456 ≠ 123456

Success > 90% —WIFI, GPS…→ 99%

工程3 用机器学习识别欺诈风险

CFCA

信用模型 → 还款能力 + 还款意愿

行为模型 → 本人识别 + 欺诈识别

工程3 事件驱动的欺诈风险分析预警

CFCA

银行交易
注册事件
登录事件
转账事件
支付事件
变更事件
营销推广

支付交易
注册事件
登录事件
绑卡事件
支付事件

互金业务
注册事件
登录事件
绑卡事件
充值、提现

互金业务
注册事件
登录事件
营销
订单支付

环境分析

设备环境分析　　地理环境分析

用户行为分析

行为轨迹　　异常行为　　关联行为

特征模型分析

伪卡盗刷　电信欺诈　撞库模型
模型　模型　虚假注册
信用卡套　暴力破解　模型
现模型　模型　欺诈名单

可信交易

可疑交易

高危交易

工程3 大数据反欺诈风险识别

CFCA

身份识别

交易风险识别

信用风险识别

设备异常识别

陌生设备
常用设备
设备多用户
设备跨机构
设备指纹

位置安全评估

GPS、
ＩＰ、基站
陌生地区
短时间异地
异地交易

行为特征识别

用户生物指纹
相似度模型
键盘按压
键盘间隔
输入间隔
输入时间
设备倾斜度

环境异常识别

代理ＩＰ
ＶＰＮ
虚拟机
越狱
刷机

撞库登录
频繁交易
暴力破解
大额交易
限额交易
盗刷
套现
陌生收款人

欺诈信息库

欺诈库
设备
IP
手机号
身份证
邮箱
MAC地址

失信信息库

高法失信
网贷失信
征信失信
经营异常
身份异常

高危账号库

诈骗账号
洗钱账号
虚假账号

欺诈关联分析

高危客户关联图谱
高危交易关联图谱
泄露点
串并案

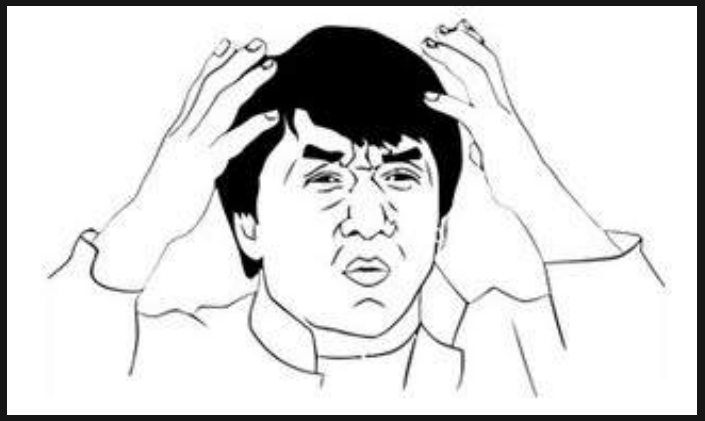
目录页

CONTENTS PAGE

AI作为武器？

CFCA

基于机器学习的攻击手段的研究



本来只是想小小研究下的你

CFCA

将机器学习技术用在 DDOS攻击中？

蚁群算法

利用GAN生成恶意软件？

论文：Generating Adversarial Malware Examples for Black-Box Attacks Based on GAN

AI作为武器

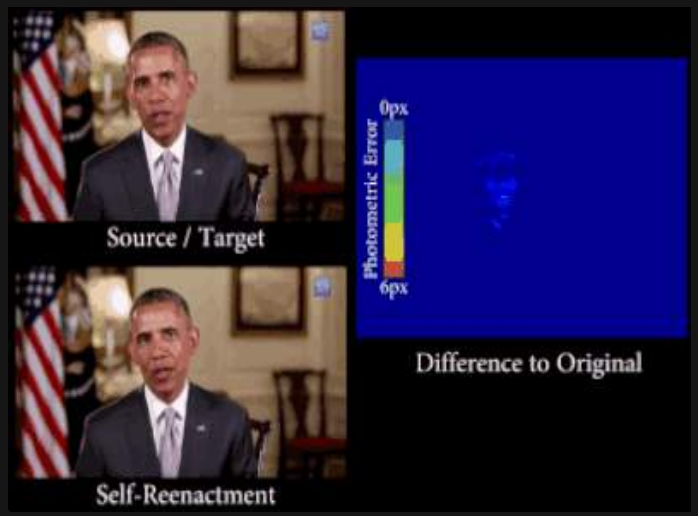
CFCA

对生物特征的攻击

AI作为武器

CFCA

对生物特征的攻击



AI作为武器

CFCA

合成语音，生成口型

AI作为武器

CFCA

平民化的FakeApp

AI作为武器

CFCA

黑客不再只能攻击你的电子设备

可能对你的线下日常生活也带来威胁

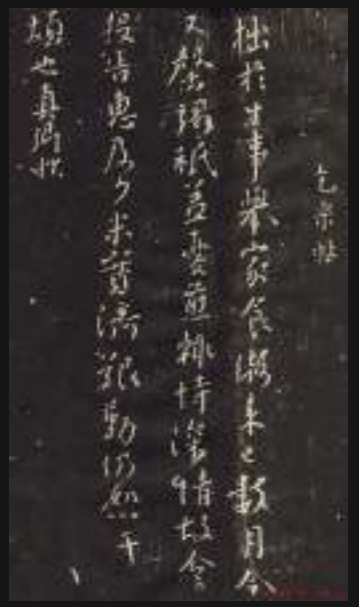
研究性项目

CFCA

AI 模仿人类 手写笔迹

研究性AI模拟手写笔迹

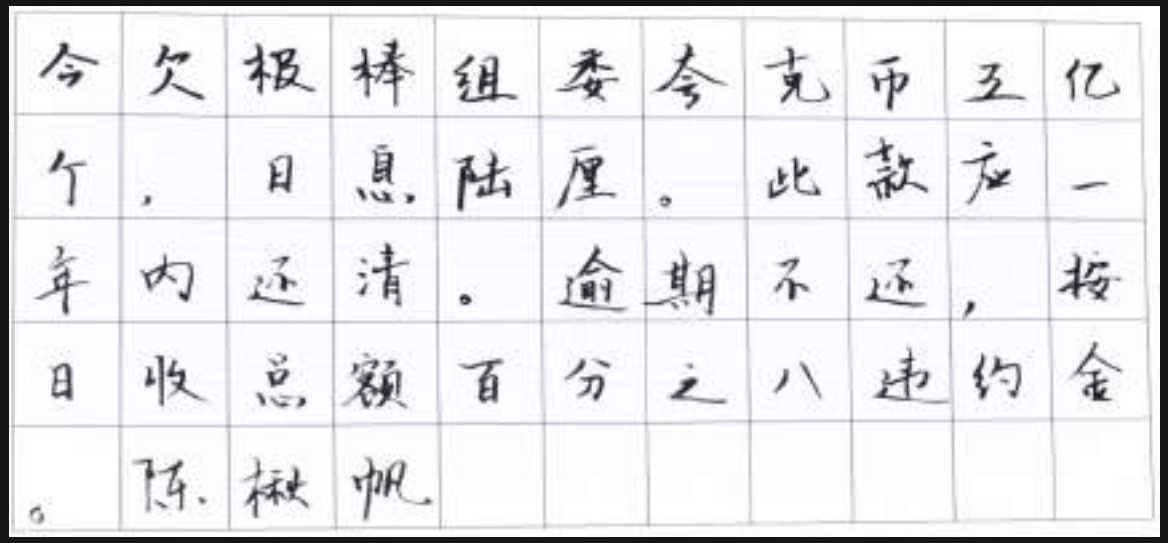
CFCA



使用 AI+机械臂 模拟人类手写笔迹？

研究性手写笔迹模拟

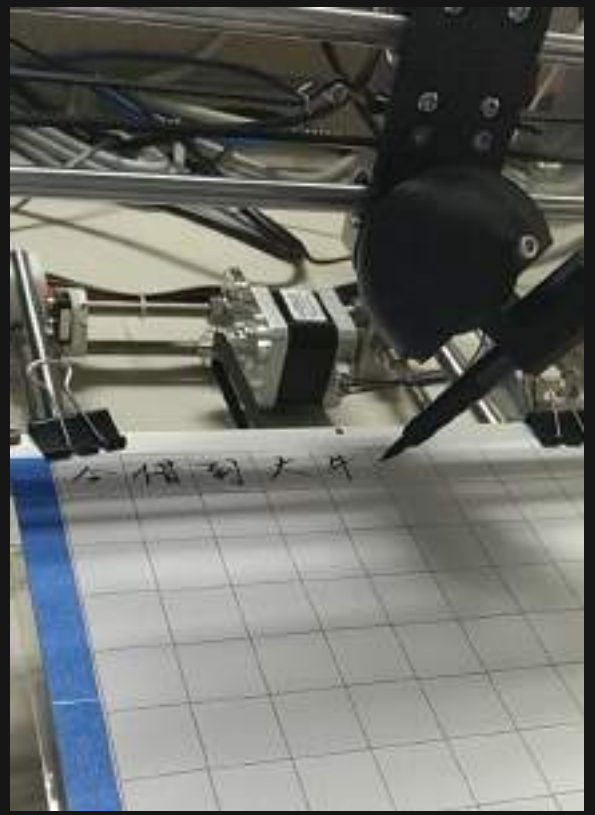
CFCA



GeekPwn2017极客大会的AI模仿笔迹挑战现场

研究性手写笔迹模拟

机械臂书写展示



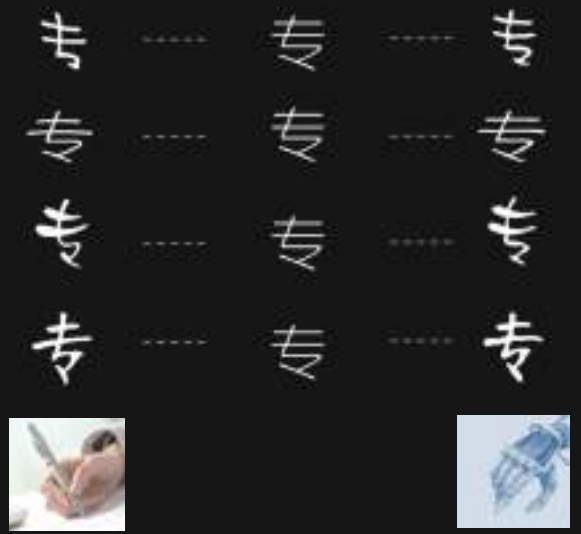
研究性手写笔迹模拟

CFCA

模拟

不同字

不同人

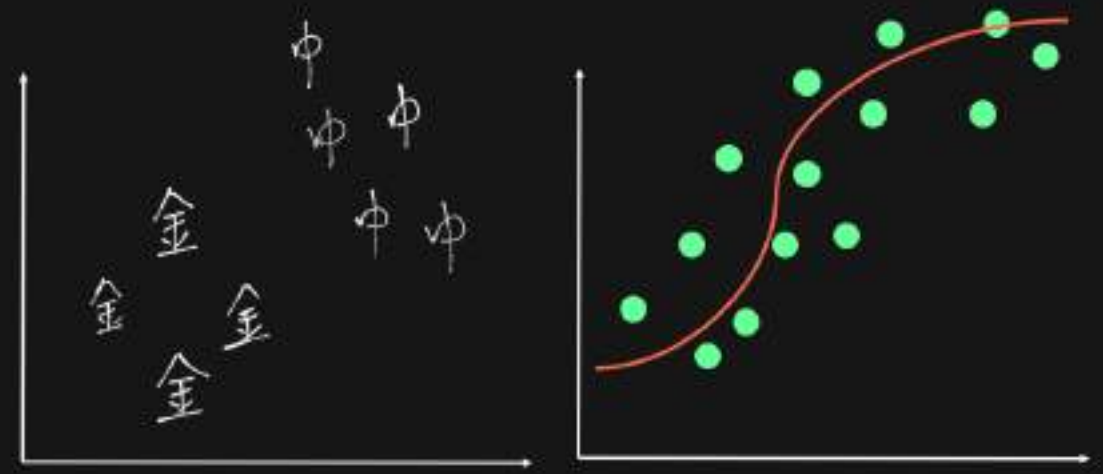


目录页

CONTENTS PAGE

技术解密 手写笔迹模拟

CFCA



AI学习人类书写风格的理论依据

人类书写风格是抖动变化的值域，机器学习的目标是找到近似解

技术解密 手写笔迹模拟

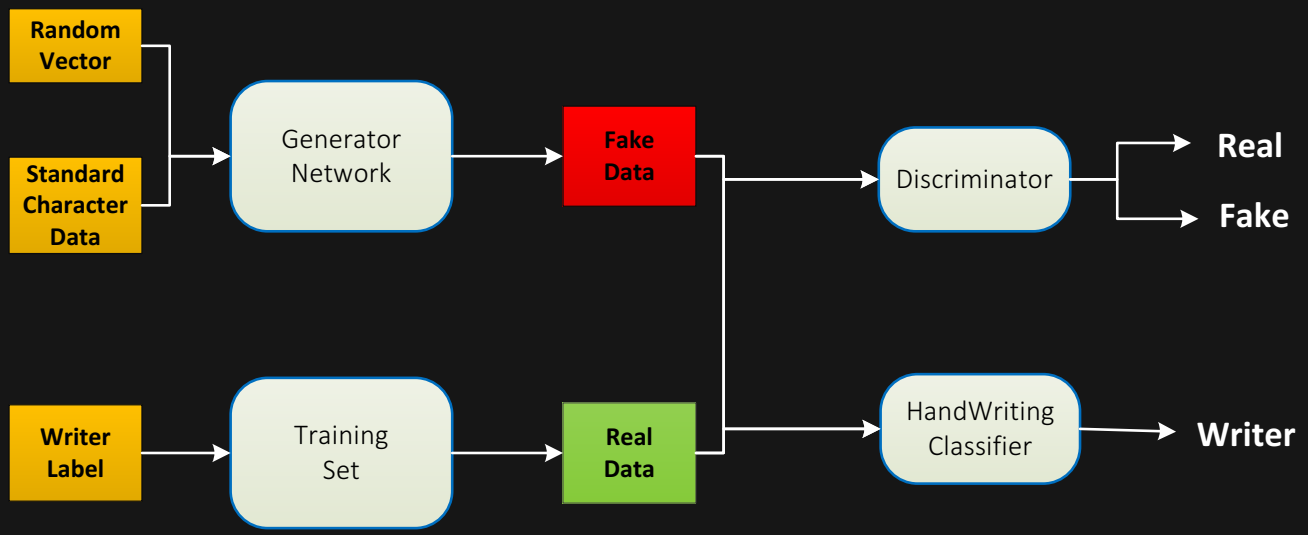
CFCA

神经网络学习到变换函数

标准文字数据和对应手写数据作为一个训练样本
Conditional GAN

技术解密 手写笔迹模拟

CFCA



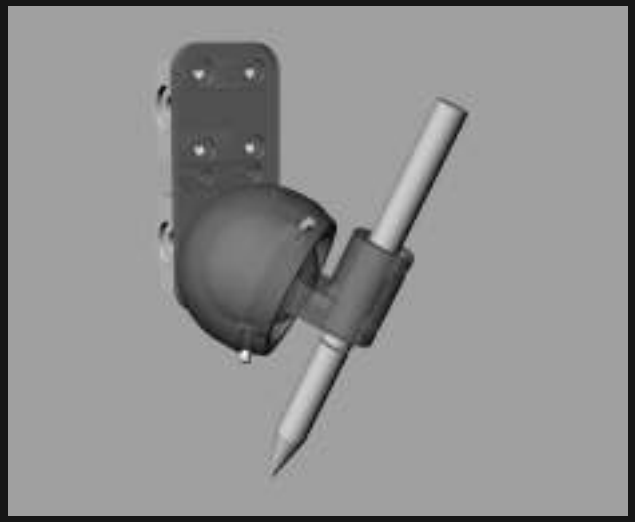
改造后的GAN 采用两个鉴别器进行优化

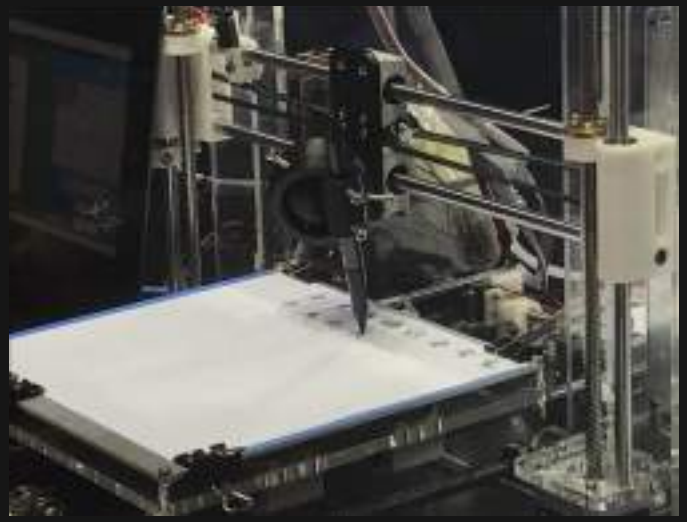
技术解密 手写笔迹模拟

CFCA

机械臂的选择

技术解密 手写笔迹模拟





机械臂自行改进组装

精度可达 0.02mm，以3D打印为技术基础

运笔速度可控，运笔力度可控

为什么我们要做研究性项目？

CFCA

- 容易做出震撼效果
- 提升同事们的信心
- 提升合作伙伴对技术的信心
- 提升团队的战斗力

CFCA

做正确的事情，正确的做事

工作方法 — 正确的做事

CFCA

采用 **成熟的** 机器学习框架

不要只关心**训练过程**

工作方法 — 正确的做事

CFCA

产品形态： 服务->设备->软件

- 持续改进
- 数据积累
- 接入简单
- 责任分离
- 性能保证

工作方法 — 正确的做事

CFCA

更重视团队**工程能力**

对中小公司来说，**编码能力**更重要

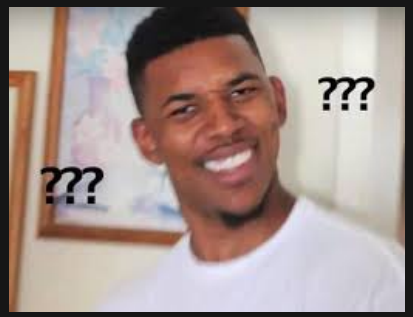
工作方法 — 重视可解释性

CFCA

深度学习虽好，但是要谨慎

最终用户

客户PM



你老板

出现问题时的你：

工作方法很重要 — 正确的做事

CFCA

工程项目 和 **研究性项目** 非常不同

选方向很重要 — 做正确的事情

CFCA

发掘独特的视角

避开热点

选方向很重要 — 做正确的事情

CFCA

从小处、实际出发

切忌好高骛远

选方向很重要 — 做正确的事情

CFCA

研究 — 工程相结合更好

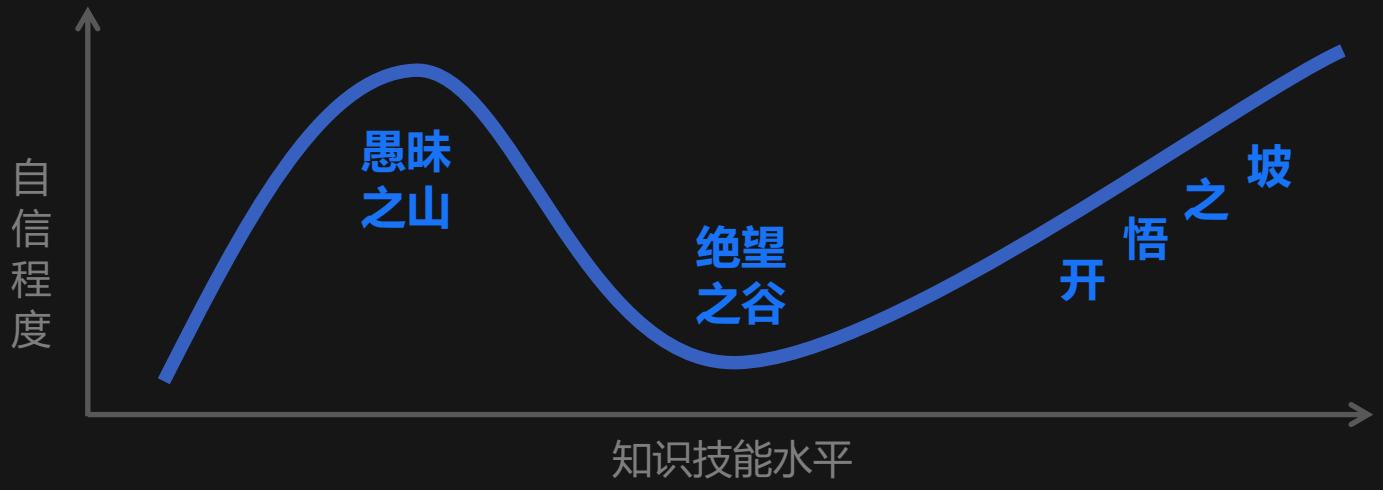
和现有产品、项目相结合

做OCR/笔迹方面的原因

共勉

CFCA

达克效应 Dunning-kruger Effect



CFCA

谢 谢！

极客邦科技
企业培训与咨询

Geekbang.

扫码关注

获取更多培训信息