
云智未来
9th
第九届中国系统架构师大会
SYSTEM ARCHITECT CONFERENCE CHINA 2017

AI领域的人机识别对抗 千亿美金的验证码攻防

锦佰安　冯继强

冯继强（网名：风宁）

国内知名网络安全专家。
现任锦佰安信息技术有限公司创始人&CEO。
目前创业，主导公司产品研发负责行为识别认证产品；设计研发及移动互联网、物联网身份管理，帐号安全解决方案。
曾担任通付盾首席安全官、青藤云首席安全官、智泰华瑞副总裁，担任多个政府部门及大型企业网络安全顾问。
SACC中国架构师大会顾问组专家成员、Kcon黑客入门闭门讲师、xKongfu演讲嘉宾。

移动营销的千亿市场

民间爱心网

685 文章 | 39万 总阅读

查看TA的文章>

移动营销汹涌而至 互联在线布局千亿市场

2016-07-14 16:13 广告 / 移动 / 用户

国内领先的移动互联网企业级服务商——互联在线，已为近百万中小企业用户提供服务。中小企业营销移动互联网化，从自运营营销到主动投放广告是一个必经的过程。互联在线耐得住寂寞，强练内功。在该领域深耕两年后，即将推出“点点圈圈”移动营销精准投放平台。

千亿美金量级所言不虚

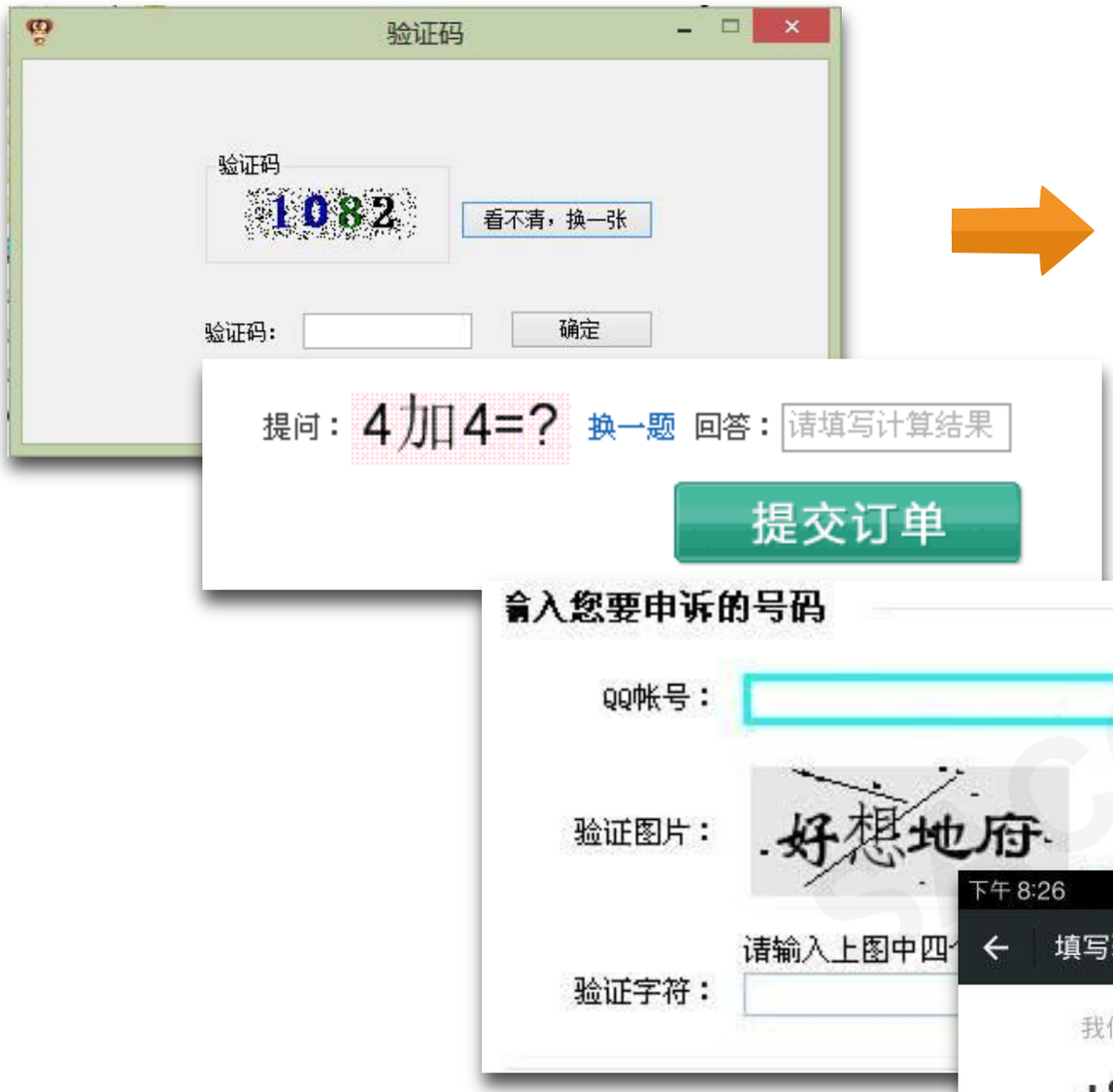
“ 艾瑞咨询发布数据显示，2015年中国网络广告市场规模达到2097亿元，预计到2018年将达到4105亿元。艾瑞咨询分析师认为，移动广告将是未来互联网广告市场不断增长的驱动力，网络广告手段将趋于整合营销的方式，精准营销和效果可量化成为广告主考虑的重要因素。 ”

CONTENT目录

PART1

传统人机验证技术概览

传统人机验证技术的衍进



数字验证码

数学计算验证码

中文验证码

短信验证码

传统人机验证技术的衍进

数字加字母变形

图形验证

滑动验证

图片验证码

PART2

传统人机验证技术的缺陷

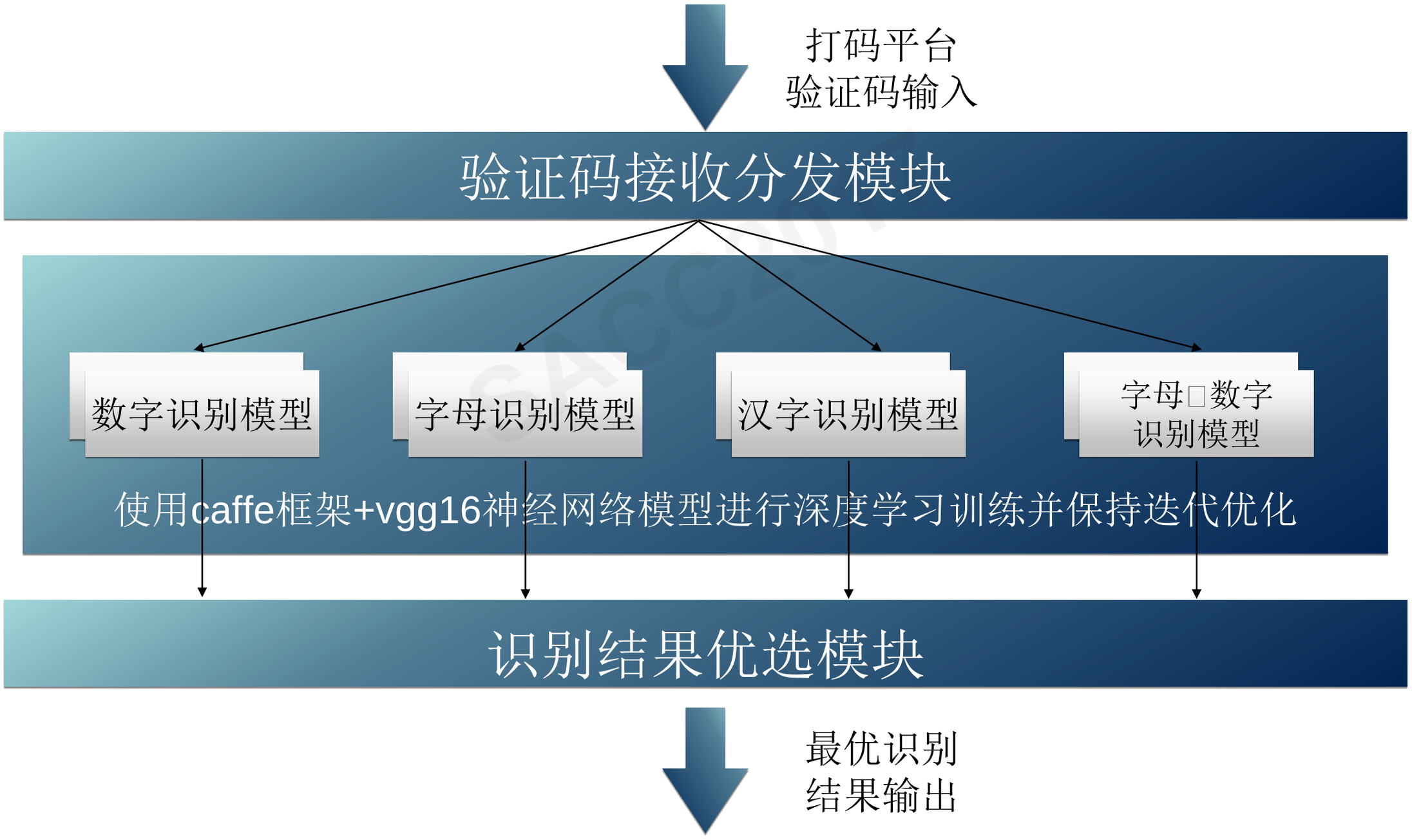
传统人机验证面临重大挑战

全国首例利用AI侵犯公民信息犯罪案告破，黑客破解验证码快至毫秒级

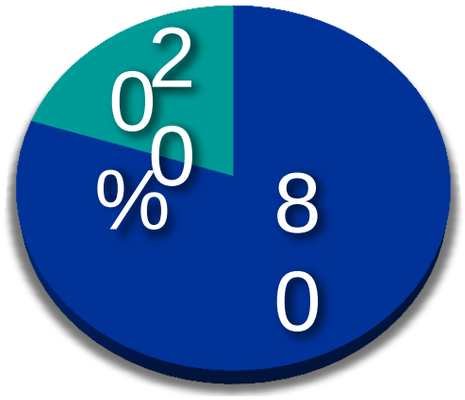
2017-09-29 腾讯安全观

分布式AI验证码识别系统工作原理

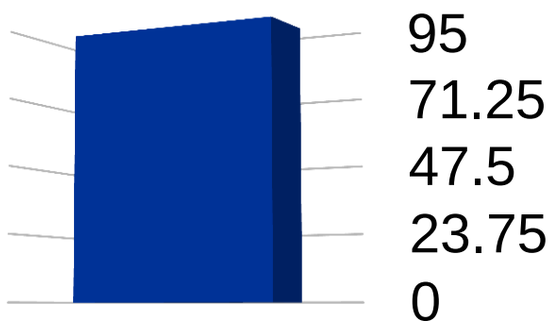
以“快啊”打码平台为例



黑产AI与风控AI之间的对抗



黑产验证码识别系统覆盖市面验证码



黑产验证码识别系统准确率高达95%

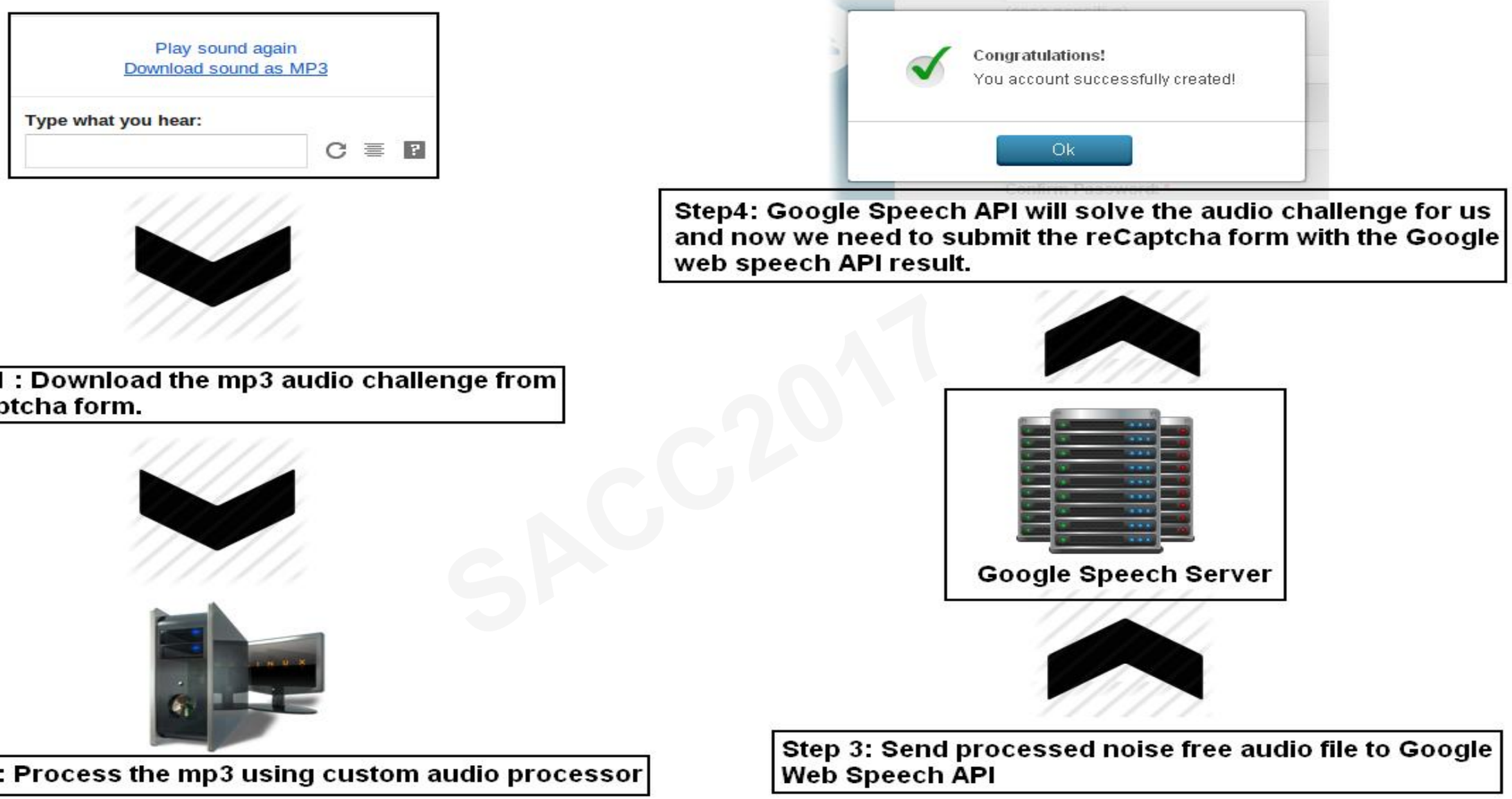
互联网公司每日损失巨大（以腾讯公司为例）

初级验证码识别技术

识别范围

数字验证码、字母验证码、字母加数字验证码、汉字验证码

Google验证码识别技术



用Google的Web Speech API语音识别来破解它自己的reCaptcha声音验证码

语音短信验证码识别技术

猫池□语音识别引擎

传统人机识别技术的破解

（播放12306图片验证码破解视频）

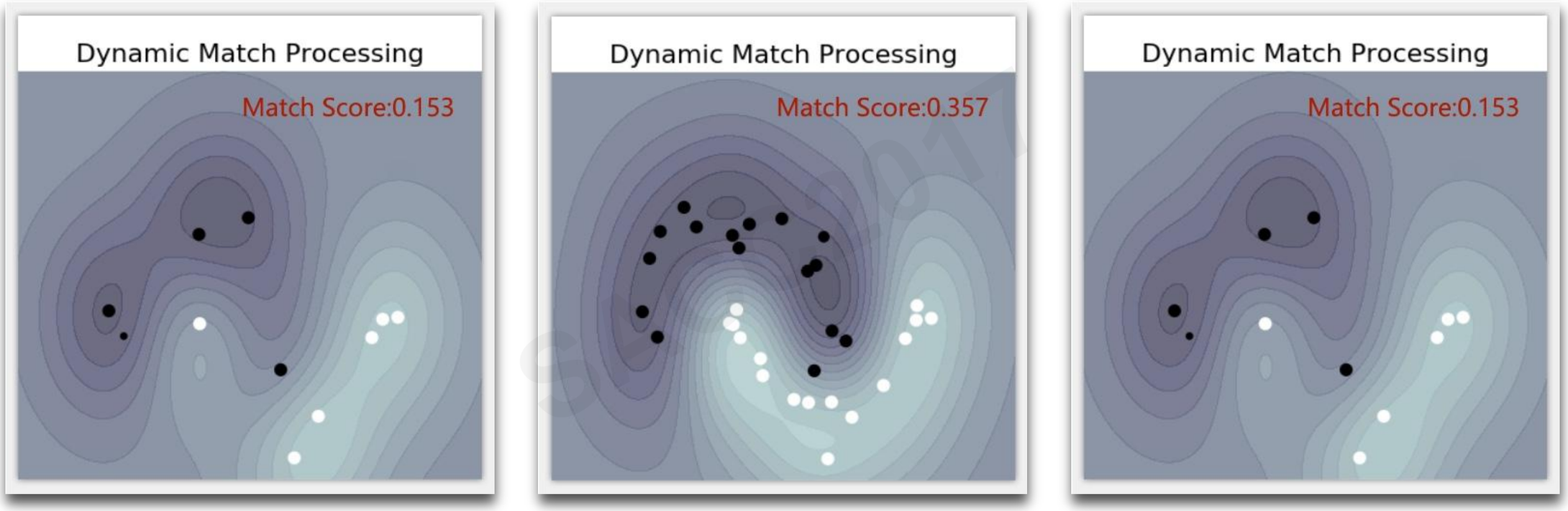
传统人机识别技术的破解

（演示滑动验证破解）

PART3

AI人机识别技术成果与未来

AI人机识别生物体综合特征匹配

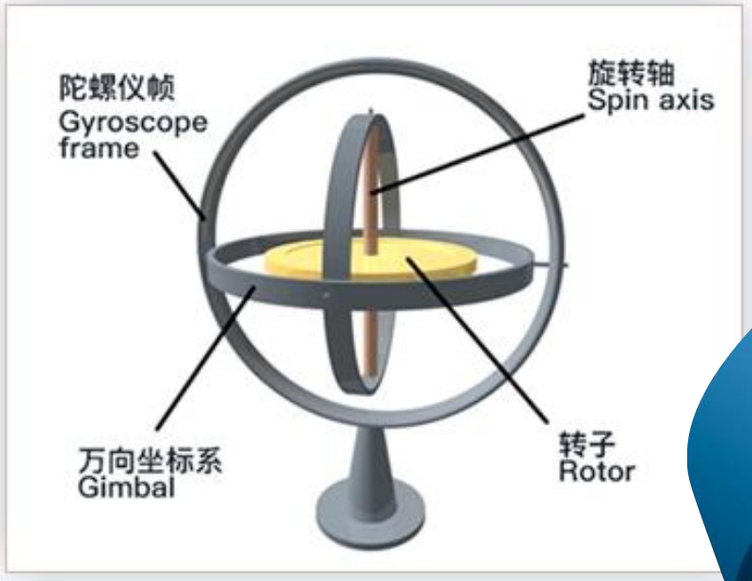


动态数据的实时匹配

AI人机识别技术的未来

AI身份识别

到“他是谁”



AI人机识别

从“他是人”

AI人机识别技术的未来

Callsign®

UNIFYID

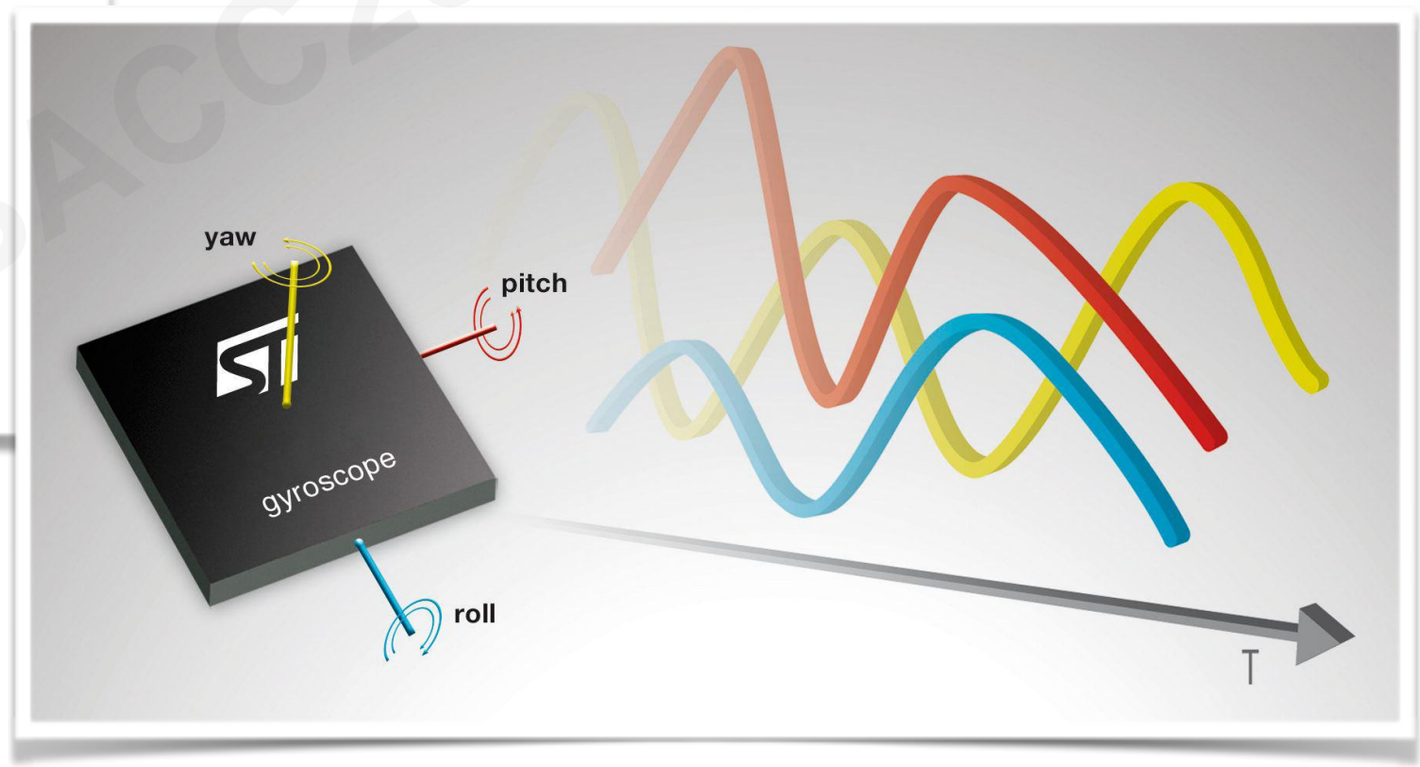
SecID

PART4

AI人机识别技术的原理探讨

AI人机识别技术原理

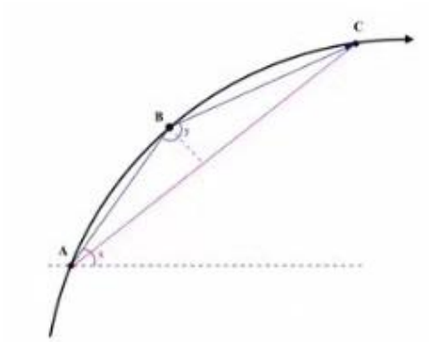
利用大量传感器进行运算
实现精准的生物体感知

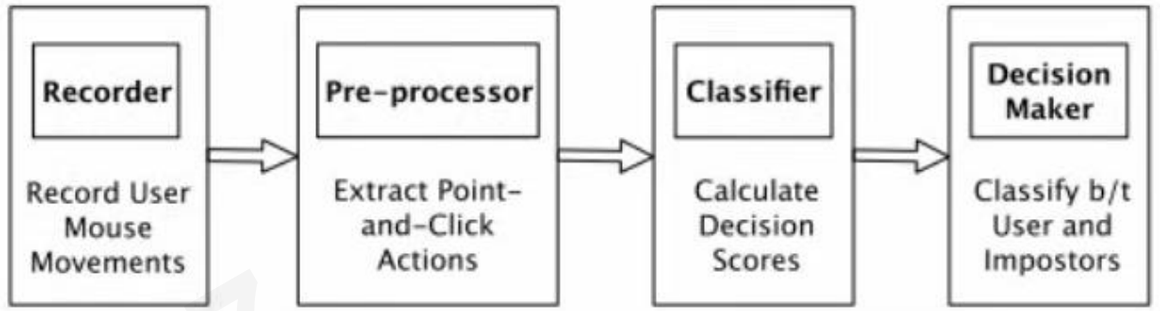


AI动态鼠标行为检测

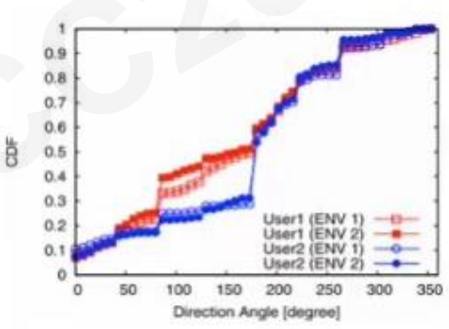
Point-and-click patterns

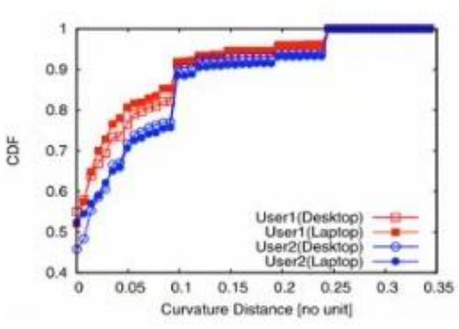
Angle-based features

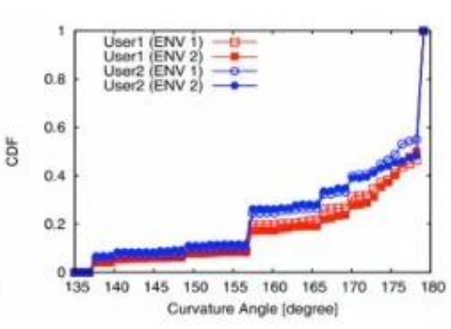




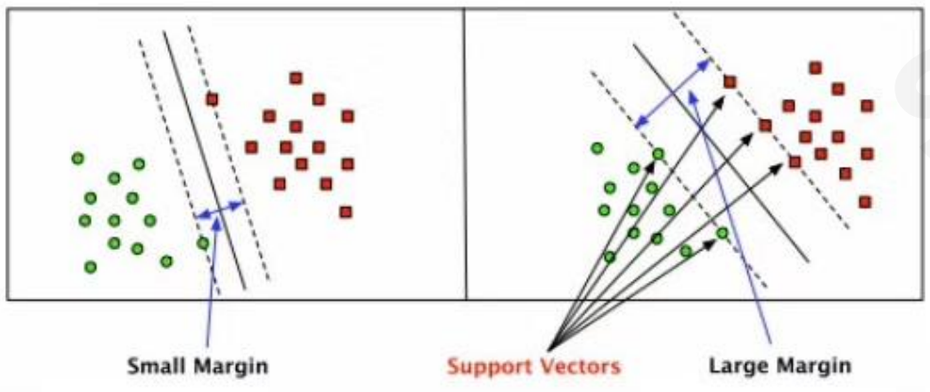
Users are identifiable, even in different environments





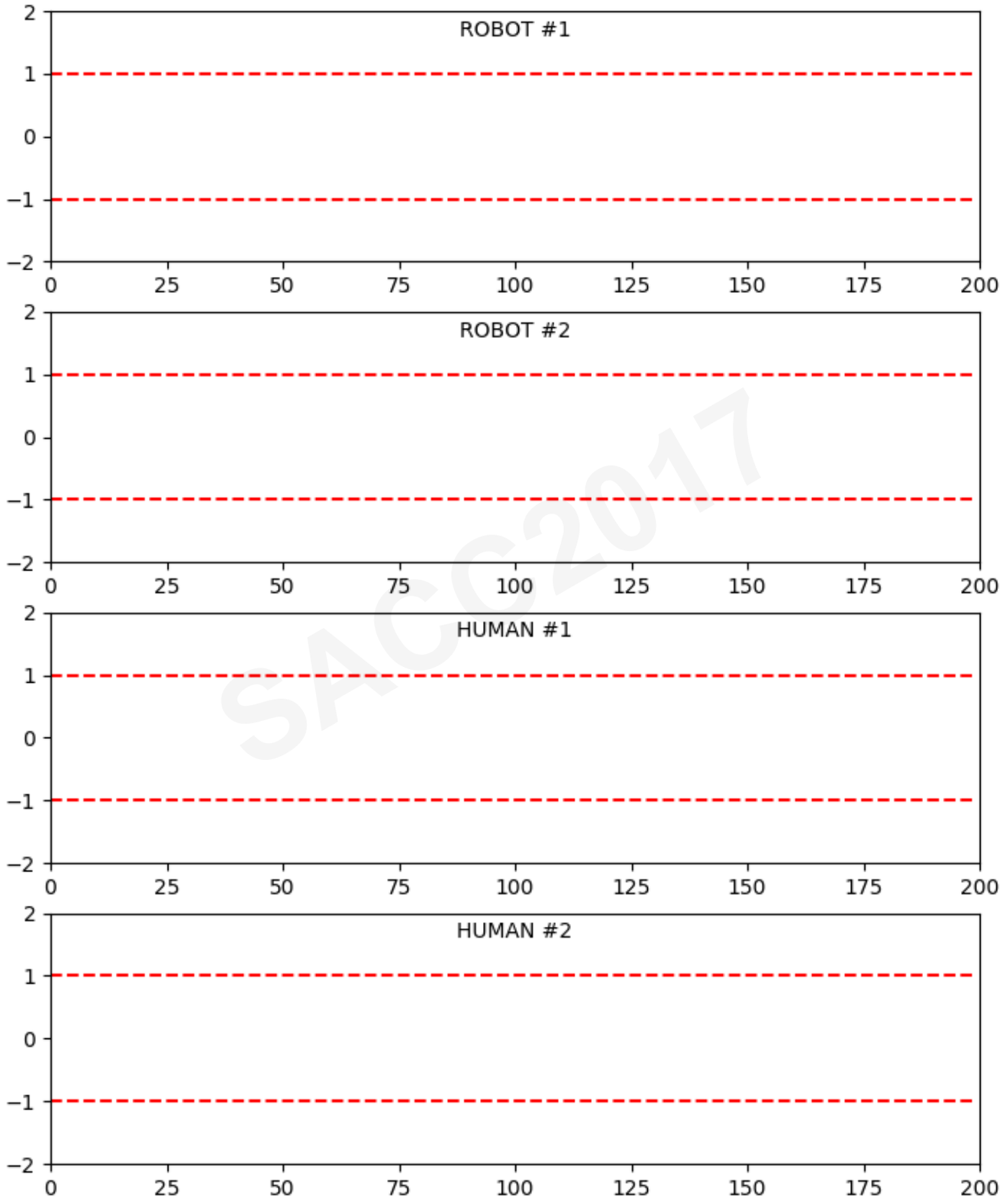


Binary SVM classifier



Zheng, N., Paloski, A. and Wang, H., 2011. An efficient user verification system via mous movements. Proceedings of the 18th ACM conference on Computer and communications security CCS '11., p.139

AI人机识别技术原理


ROBOT #1
ROBOT #2
HUMAN #1
HUMAN #2
2
1
0
−1
−2
0
25
50
75
100
125
150
175
200

PART5

解决传统人机验证隐患新概念

腾讯AI人机识别产品

腾讯智能免验证

网易AI人机识别产品

智能无感知验证码

极致用户体验，多维度收集环境信息，安全用户只需轻点即可通过验证

在线体验>

滑动拼图验证码

创新行为式验证，轻松一滑完成拼图，用户体验极佳，秒速通过验证

在线体验>

点选验证码

顺序点击图中文字，全新行为验证，安全性极高，保障验证安全

在线体验>

短信上行验证码

感知威胁的终极验证方式，需发送随机数字到指定平台方可验证成功

在线体验>

网易“易盾”智能无感知验证码

锦佰安AI人机识别产品

锦佰安“无码”APP人机识别

（“无码”暂时只支持移动端 幸好千亿主流市场在此）

智能验证码技术分析

网易、腾讯智能验证码

智能验证码技术分析

id: 507ffa2bee344d2b9e969caa873c1a5e
version: 2.3.3
token: 41d84910a92c40afa8ded0ba045139b7
type: 5
width: 310
data: {"d":"","m":"RNh4zSVuR0a+oIhL7fkCbX0eN9grcb2DlwbColZswTeC8jMEDIlPR57j9XhWM7R4e6hR5+pnvBaHaPRP1HLbPxuCiA+/eTSt0\\9DIPJgOLkNL
DxocWRFg/bpV+PQOlr9UoqVFy5Ng2dVZe9WDu71W\\+\\8LPQZzmdnvQ6go0vydg5YkamPdH6kjf9DYwOEU9H2czBdNuEbqe59YV5OvBnJh+6\\grs+VydUFAvhsKPgQ
0acZg7wERfZQX4nbyGlvD4Jr89gMrDpt4lTD65/jMuvnQDGUhWisFMj87/1ge+RM75RQiiKYN9js/Q5GAl/w2b7nBr2QbPId5aZyjgH07ZeHX0tAEbcfI6eCNePY92YR
kEj0sK6EjWQrdfTVND5jrhiJBode99CxVyHEjrK+IYfGwhUxjmms\\my8RYPIEVa3","p":"prHBbG5AAv/xx9inxyhqTaVLoAA9PzdVGcBmGWSicGp3","ext":"Fmd

referer: https://dun.163.com/trial/sense
callback: __JSONP_119ymhg_1

aid: 1252020920
asig: M9g-ybEgmq3_IVqFZQdGdJN-BA6TWRC_DdnSlWsYXh5n5SeDHYOZv9vrqlpH5uV7ysBNM9UiC8J3czagKPEPkb9bEpILiPEwmbGIz5sxAarwjgb9q7Ca83Mqzha0_vnzrvaL_B6d3g2WTyrTiChbcQ**
captype:
protocol: http
clientype: 2
disturblevel:
apptype:
curenv: open
uid: 80000105
cap_cd:
height: 45
lang: 2052
fb: 1
theme:
rnd: 637617
collect: OD6q9t0AraWJf+dtq0j8VhGzBTWdaDAZ6Wi4o286rYbE2BepBQSft+dXXvpWZYbqXwO39aIXg1N4ovU7pbceDSbaThrOl5GmukmxzOD9crX7TdqBDBrrbEEjWnb/AtWs0gSe0Hrvq/oFC8nHQg+WGRatIZ
8Focbce3UBTLuK3njYKzr3MTCUnXRzvmgnfILkVVxtRA1p/J563OONxSv3preCtM9ySUYcPB+1LenVpkuvsuwC2FIOIsjorypaIlffOr2//rgjLxiOK0NxJhvTazpA/Fe6vkQLr94X/6Ow114PHzTLWobgjU32cZ0
VYSjIxiuTopLUDU0SaSRjonq7wRJnSx2qDtAm12Au7adK9vNRQaYY/CimzfL0NYR8Ue8q6HORD1YrMuxDiOZSLX2x/1OV3lqkw+FtbriH+1SmAaOK3+reATtCBA2sZKF8+tIJK8mkK04j7w0kffcBVHB5U/1OtNeD
qEasf7zuP9YgT0fvkxritSJ4SZCCOlDtrN1IKppWPIc0wViTnRaPaPD/MMiFmKIyuAvPZcYi/uG0taBElaYqa2+mTrXwUohjqiiwdjPGy3owIaqlLsNcx2F/mL5/oLiw5G7Ol4gcX2LB4IH+Qsg8VYNDkLZu3QHr
90HY0XeNGbXiZmfC5m0OZb0P1sWux7xO/RGBiQgKJTSApG0IBu8USmkq0FxtVZIrzLDuVXfNThYGCaky+hrfOAOndAV0l1V3jH+jsyzEBj5q3GuU1dQVsAvRg+FaRxXXeY4bEUXF1jopMhJvHx+rtCm5GCqnEQ65)
f0zFZhXNCxgBY/X6pItqUAauTDnupHFDs0tADyO54qxlVhYro0rbiSYywx3FPoQiP05L38VTqGdFEnVZLmx+aCEc8y+BBaZ7RhnJ0RzlDaB69MJrj+1zKi5WuvDqGoabDHsRz2mEj3oIhdHxmF7wTjwn/kkz1IM4)
QTCY06jwc9JXqNTO2LjR4nxnlGmQKSwUGx8Od9H2F6lzl7xdPHDv0xhaN6cxvtB5p8sLWxlGebOnyaP/s99T7azTZ8lMBjPNOb10=
firstvrytype: 1
random: 0.8728919132199324

图中点字验证码

请顺序点击大图中的文字

验 证

图中点字技术分析

aid: 1252020920
asig: YjsZfGwRbBJV0jGyCk9Xe9p3MilJvO1i03JRWk5BtdT86ruLNgktWV-M19op6kqLtV1bPD2_Be4N3VQAeZxvTL124RRqJbfm9WzkAiq
captype:
protocol: https
clientype: 2
disturblevel:
apptype:
curenv: open
uid: 1667577568
cap_cd:
height: 45
lang: 2052
fb: 1
theme:
rnd: 529826
rand: 0.07059807561987808
sess: yR0Vhe_S2b-0Agfbzik0WNLVPHGX_5hdJd_5dKr6LSE_yX2dnxBL1eqmf-J9LYpBoyJnJdbAyhR-WcxXT4uO7bc9E18tCz5quz3DCEU
firstvrytype: 1
showtype: point
subcapclass: 7
vsig: b01rmm17S09J7aRTn18_VMYzy-mufv8kFg_Dijt0iDdd2w0ZeDa5lO9nIU4Dx8gPOSjX51DdFTEYQWkzCL2ksknM68ALhpmwdIB0qCE
ans: 104,96;148,206;454,200;104,240;
cdata: 142
bcbafa: OD6q9t0AraWJf+dtq0j8VkNHLoZ//x1V9W7g9BlyuB6Hf5f5JjgT4+w82RyGb3JjuPxj1GTXiCRaNszRQDppm/C6n71JJsaJSjmWk
JgiTgvW0/i+oduSsJaRggXF8EU/5GOmpreWHWrTT8bNAdAlafk8zg2UQ/MjRtHXg7+RPH+85ckZy1VCpTW9TAQqknzcKsNHaZSfSzt4y00U9
yWOUnf7Ewq/MdYgHZEdxUvl68fx6HilCAxyMZcvr2pzsM17LZ4INW3HhJHrSPGfpu9d/Dk85DYDuEbEiv3ovWhWouLzt+6Pi+4jp278r6ehK
nHjpZMM55UtWbI9naXL5LaOwx8o6IqCn4WQWJ6YM+K3gphBM2O+IHd2U2hFL+r2Ix5IpJQHXqmGF1J6toWrqunZlVtTpxVI12WEcVQj8/XsR
k7KLRzrikvXpxmAlHQ7zVqmNBlqOo7RvnnGXYIfwVXTOG1XM61WgJjBdr7/YymRvrNJ9FvPp7806eSVIDyK+UMgQHG51mTpI/aXRgV0BaX7R
oZiECXZ6RAWb1yGbn9WpK19mPdVEMDsmBnhm1Sztg0RVViixWZYAueBl9MAzPt6Qdq0ZCti6/JnCa6Fj+a8vIj+0xu5mjSY3sc7Z1otlaFPr
o26fiSgC7OEEkmNNhlyhSHxRVOagvoulOdJ7QGUQSv5IsCseLWY86oCV1N7YwW/9kQqtbFaw/z9ztbVMyDFV+jvoU7dOBulmiOhxrCMiT+OW
vsofzvZfRkzkjCyhjOAXpYa9uHzUZndjWuBBnQxGvHENPJF5Y24MuAOosYa8LrketeduWyxTsanSPeb3k6mOe/fRvKysoZRdd8H3Ps63huwU
roTBn1VBPu9OdaEm/L1xJK9WeL+kE3kdKgvevs+AEDrUXhUEKCpFyLv5uOJk8pjiE0BEXPEHPMHLB9fawYIRVZ1hGmsUSFxUs79lwJswyH54

没有绝对的安全

没有一劳永逸的防护

攻与防的对抗永无止境！

Thanks !