产品调研：

Asirra captcha：broken using a classifier trained to recognize image textures



MintEye captcha：broken by a very simple attack based on Sobel operators that only required 23 lines of Python



论文阅读与笔记：

《The End is Nigh:Generic Solving of Text-based CAPTCHAs》

论文基本是宣告了文本验证码可以成为历史了，甚至说需要重新考虑reverse Turing test。比较重要的是论文在future of captchas中提出的可能设计方案，比如从当前计算机视觉还未解决的问题的角度考虑。

引用：Whether there exist situations where the human brain is definitively able to process information more efficiently than machines remains an open question.

今年计算机视觉领域的比赛ILSVRC今年都宣告结束，也说明在图像物体检测识别领域，计算机也不必人差了。下个还未被ai攻破，但已经被盯上的就是图像理解(从明年正式开始的WebVision比赛就是这一领域的)。

引用：Recently game-based captchas have been developed, however implementing this idea as proven to be difficult, as the game captcha schemes for the leading game captcha provider ”Are you a human” have been broken

给我的感觉是：设计困难，攻破简单。

引用：Human solving time is very predictable for random strings.

不禁想到看到的一个例子：一个验证码是解决复杂的高数问题，评论里有人戏称“看到这种验证码才发现原来自己不是人类”。对这类验证码来说，是不是能快速完成验证的才是机器？但这种方案也出现一个问题：如何衡量和预测人类完成验证的时间？如果依靠实验数据，必然导致设计验证码的人员的负担太大；而如果存在衡量的算法，攻击者又可以利用这些算法设计攻击方式。

引用：Clearly solving time is not a good reverse Turing test since it is easy for machines to fake, but other examples might exist, especially for captcha schemes that require a prolonged user engagement.

这里的有关想法记录在另一篇论文(神经科学与密码学交汇)的笔记里。

《神经科学与密码学交汇:通过密码原语抵御软磨硬泡式攻击》

这篇文章里提到的一个“内隐式学习”的概念，根据这个，可以训练用户在用户自己也不知道密码的情况下完成用户验证。虽然这个方案是基于密码，但是如果映射过来，把人类社会与单个人的交互映射到“用户训练”这一过程的话，验证码其实可以看做只允许人类通过的密码机制。我们需要做的就是验证对象是否是经过内隐式学习获得过某些知识的对象。其实我们设计的方案里，是有一点这个思想的：因为图片是随机截取的，所以我们其实并不能确定用户分组的依据，但是只要正确率到达标准了，就说明这个依据是确实存在并可以被大多数人所认可的。

Asirra: A CAPTCHA that Exploits Interest-Aligned Manual Image Categorization

Machine Learning Attacks Against the Asirra CAPTCHA

Asirra的提出以及被攻破过程，应该说，对如今的计算机视觉技术而言，这样的验证码已经完全无法区分人与机器了。

Video-Passwords: Advertising While Authenticating

提到了视频验证码可以利用的验证方式：Timeline，Click-Based，Tagged。根据这些考虑到我们的方案以随机截图为主，如果利用Timeline，可以选择让用户对乱序的图片排序；Click-Based多半还是需要对图片数据进行标记；Tagged需要考虑在我们方案里，截到的图片不一定会继承视频的Tag。

设计报告：

Part1. 从视频截图并根据tag分类

视频源：

截取方式：

验证方式：是否把标签显示给用户

实验报告：

总结：