图形CAPTCHA设计

刘艳伟 1801210863

何家乐 1801210829

目 录

C O N T E N T S

- ✓ CAPTCHA设计准则
- ✓ 图形CAPTCHA的引入
- ✓ 3种参考设计方式
- ✓ 图形CAPTCHA设计小DEMO

设计一个成功的CAPTCHA的准则

可用性

可扩展性

稳健性

CAPTCHA：反向图灵测试，区分人机，防止机器人滥用为人类用户制作的网络服务和在线表格。其中最大的挑战是管理**可用性，可扩展性和设计稳健性**的竞争要求之间的贸易关系。

图形CAPTCHA

图形：更加自动化，抗机器识别率远远高于其他。

传统文本：易被机器滥用；扭曲失真难以辨认，准确率低。

图形CAPTCHA

随着图像处理和计算机视觉算法的发展，那些在传统上很复杂的问题，如对象和文本识别，（包括场景的识别和图像中包含的上下文信息的识别等）都可以新的技术和方式解决。

即，基于标准文本的CAPTCHA不再那么安全，它们被新的方式所替代：一种*依赖强大的图形识别或物体识别的验证方式*。

设计方式参考之①：reCAPTCHA

谷歌推出的一款基于图形验证码的reCAPTCHA，它要求用户在几张图片中选择出所有某一特定种类或主题的图片。（比如：要求用户在9张图片中找出所有包含“红酒”的图片）

设计方式参考之②：PiSHi

PiSHi，基于图形的验证码，通过利用人类的三种感知能力来区分人和机器：

一是方向的感知，人类能够轻松识别图像的直立方向;

二是人类大脑能够通过部分可见的图片内容来识别整体内容;

Cognitives

三是人类在遇到图像挑战时无意识决策的能力

设计方式参考之②：PiSHi

PiSHi的实现机制

- PiSHi向用户呈现一组扭曲的图片，并要求用户以任意顺序点击图片的竖直方向；
- PiSHi捕获用户的交互模式，将它们与模式数据库中保存的模式进行比较，并授予她相应的信用。基于该信用，用户通过或未通过测试，并参与更新图片数据库。我们的实验表明，人类用户可以有效地解决我们提出的验证码，准确度为99.44%。

NOTE: 此种PiSH设计i还可以抵抗好几种类型的攻击，包括随机猜测和反向图像搜索引擎。
（攻击设计，我们不做具体介绍）

设计方式参考之③：EmojiCAPTCHA

EmojCAPTCHA，这是一种利用在线工具、开源软件和emoji表情生成的验证码，它要求用户根据给定的emoji表情来从一系列真人表情中选择出相同的那个。利用微软提供的EmotionAPI，能够从图像中自动判别出人脸所表示的感情。

为了防止这种工具和其他类似服务被用于对抗CAPTCHA服务，于是又引入了*图像变形、噪声和失真*三种方式增加安全性。(攻击)

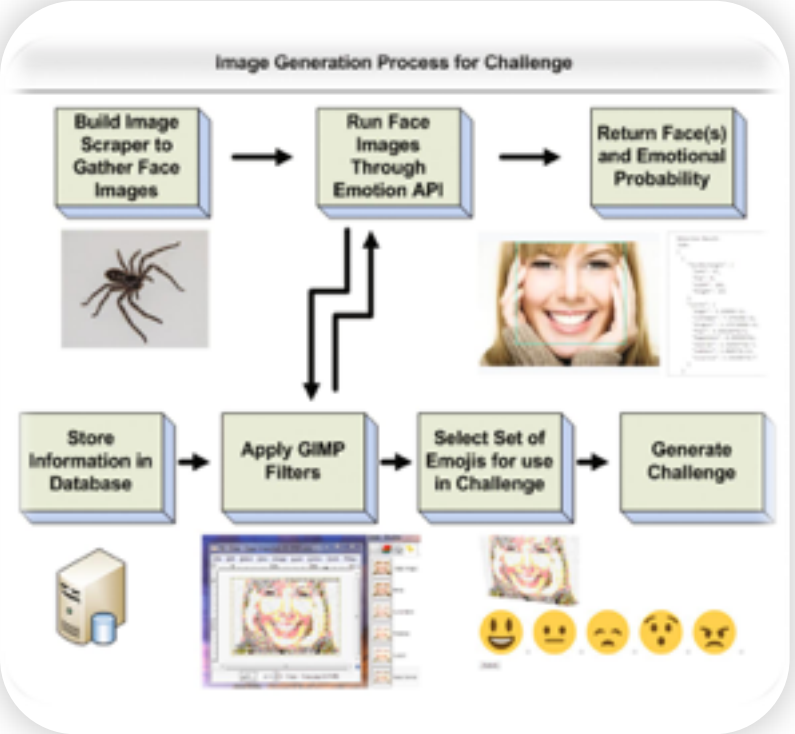
NOTE:

这是一种基于人工智能的API，可通过云访问，并可由开发人员在应用程序中使用。Emotion API将图像作为输入，并使用Face API为图像中的每个面部以及面部的边界框返回一组情感的置信度分数。检测到的情绪有愤怒，蔑视，厌恶，恐惧，快乐，中立，悲伤和惊讶，支持用自动化方法准确一致地识别和标记包含人脸的图像中的情感。

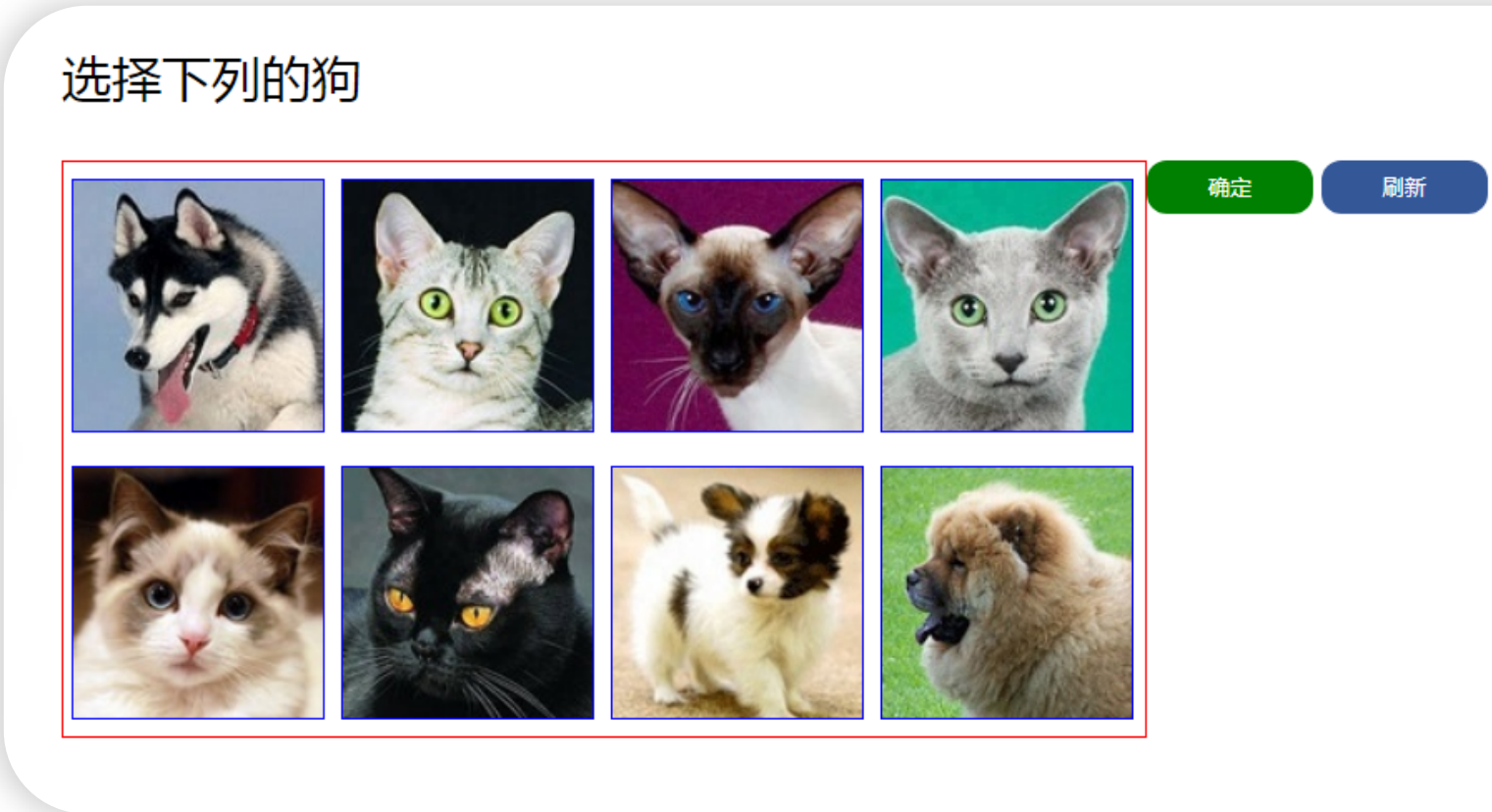
设计方式参考之③：EmojiCAPTCHA

收集过程

- 爬虫爬数据（不需要手动打标签）；
- 利用EmotionAPI运行测试找出符合条件的样本；
- 输出结果存储在数据库中；
- 通过过滤器和GIMP来变形图像，对抗反转图形搜查攻击和基于计算机视觉的其他攻击（攻击）；
- 得到一系列和EmotionAPI相匹配的被标记的打好标签的人脸表情并存入数据库；
- 可以使用。



存储若干猫的图片、若干狗的图片，每次生成随机数随机选择图片各若干张，用户进行选择判断，成功则通过验证，否则不能通过：



设计准则

引　　入

参考设计

设计实现

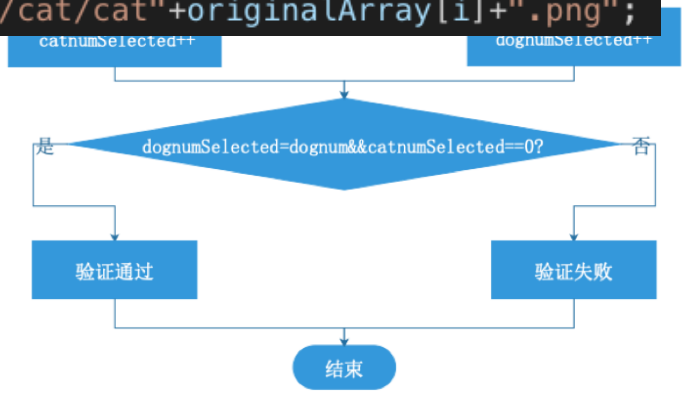
存储若干猫的图片、若干狗的图片，每次生成随机数随机选择图片各若干张，用户进行选择判断，成功则通过验证，否则不能通过：

```
m_div.addEventListener("click",function(){
    var img_m=$(this).children(".tip");

    if(img_m.hasClass("hide")){
        img_m.removeClass("hide");
        dognumSelected++;
    }else{
        img_m.addClass("hide");
        dognumSelected--;
    }
})
```

```
rray = [1, 2, 3, 4, 5,6,7,8,9];
.sort(function () {//将数组内容打乱
5 - Math.random();

g/cat/cat"+originalArray[i]+".png";
```



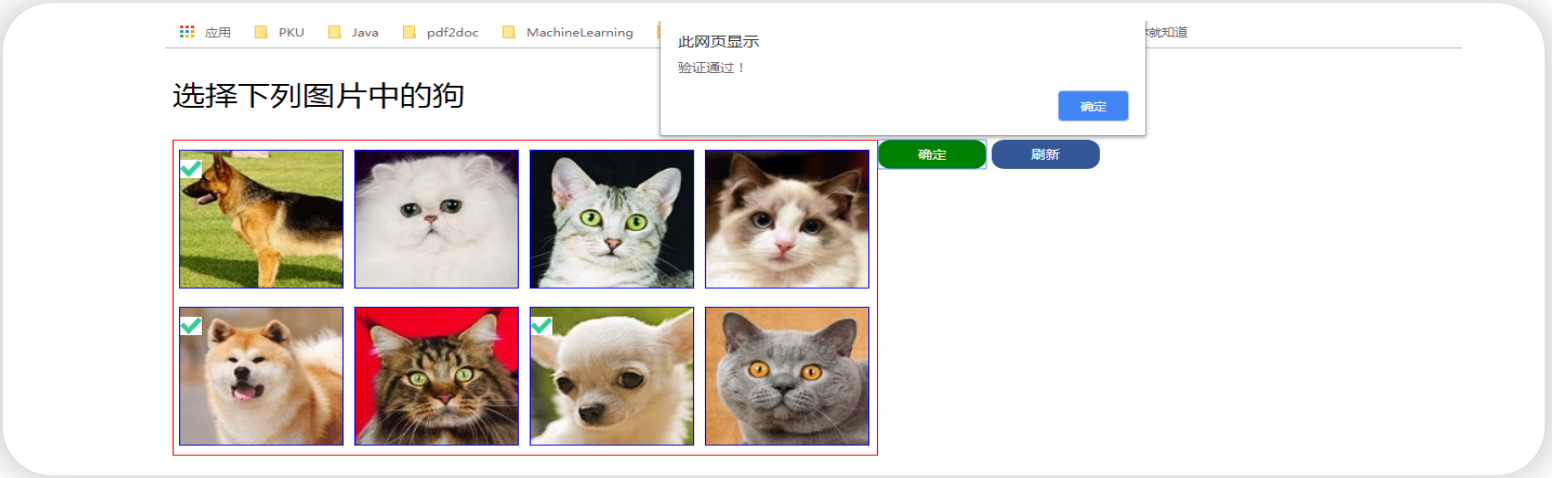
设计准则

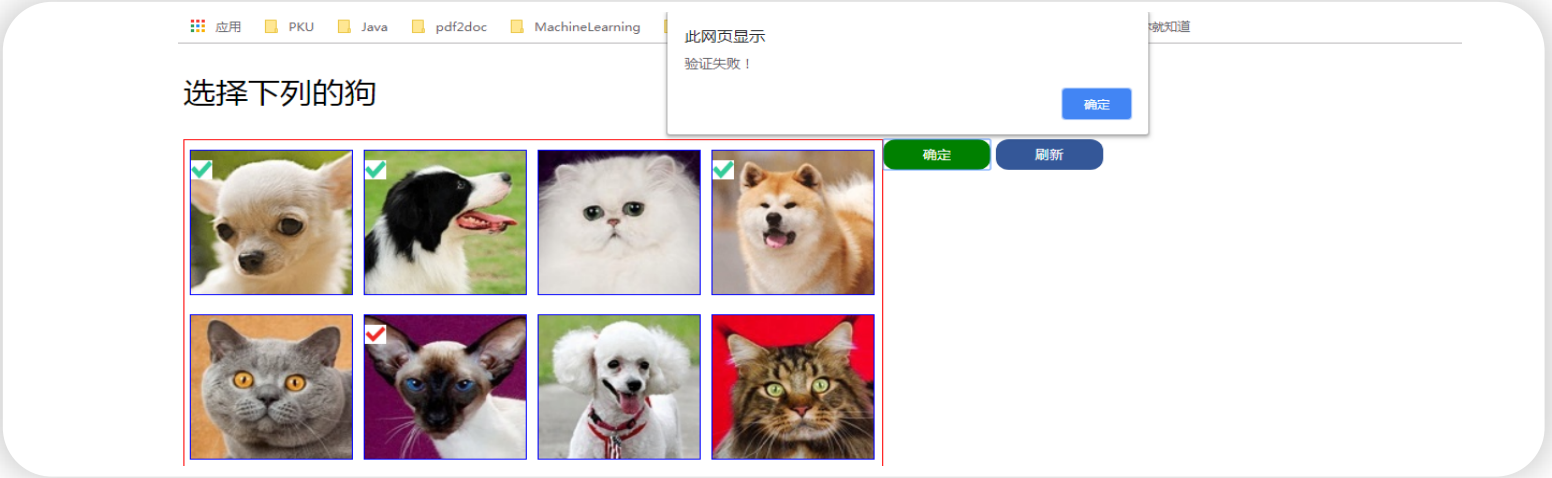
引　　入

参考设计

设计实现

通过验证和不能通过验证分别如下图：





北京大学

THANKS

FOR LISTENING