重庆大学本科学生毕业设计（论文）

重庆大学LaTeX学位论文模板 CQU 使用说明

学　　生：张乐

学　　号：**20121892**

指导教师：葛永新

专　　业：软件工程

重庆大学软件学院

二 O 一六年六月

Graduation Design(Thesis) of Chongqing University

An Instruction of the LaTeX Templet for Chongqing University Thesis

Undergraduate：Le Zhang

Supervisor：Prof. Yongxin Ge

Major：Software Engineering

College of Software

Chongqing University

June 2016

摘　要

摘要是设计或论文内容不加注释和评论的简短陈述，应以第三人称陈述。它应具有独立性和自含性，即不阅读设计或论文的全文，就能获得必要的信息，摘要的内容应包含与设计或论文同等量的主要信息，供读者确定有无必要阅读全文，也供文摘等二次文献采用。

摘要一般应说明研究工作目的、实验研究方法、结果和最终结论等，而重点是结果和结论。摘要中一般不用图、表、化学结构式、计算机程序，不用非公知公用的符号、术语和非法定的计量单位。

摘要页置于英文题名页后。

中文摘要一般为 400 汉字左右，用小四号宋体。

关键词是为了文献标引工作从设计（论文）中选取出来用以表示全文主题内容信息款目的单词或术语。一般每篇设计（论文）应选取 3 5 个词作为关键词，关键词间用逗号隔开，最后一个词后不打标点符号。以显著的字符排在同种语言摘要的下方。如有可能，尽量用《汉语主题词表》等词表提供的规范词。

本文介绍重庆大学论文模板 cqu 的使用方法。本模板符合学校的本科论文格式基本要求，而硕博模板有待完善。本文的创新点主要有:

- 用例子来解释模板的使用方法;
- 用废话来填充无关紧要的部分;
- 一边学习摸索一边编写新代码。

(模板作者注:中文关键词定义 cnkeywords 应在使用中文摘要环境之前。英文关键词同理。)

关键词：模板，摘要，论文，LaTeX

ABSTRACT

An abstract of a dissertation is a summary and extraction of research work and contributions. Included in an abstract should be description of research topic and research objective, brief introduction to methodology and research process, and summarization of conclusion and contributions of the research. An abstract should be characterized by independence and clarity and carry identical information with the dissertation. It should be such that the general idea and major contributions of the dissertation are conveyed without reading the dissertation.

An abstract should be concise and to the point. It is a misunderstanding to make an abstract an outline of the dissertation and words “the first chapter”, “the second chapter” and the like should be avoided in the abstract.

Key words are terms used in a dissertation for indexing, reflecting core information of the dissertation. An abstract may contain a maximum of 5 key words, with semicolons used in between to separate one another.

Keywords: template, LaTeX, abstract, paper

目　录

插 图 清 单

附 表 清 单

主要符号对照表

cluster	集群
Itanium	安腾
SMP	对称多处理
API	应用程序编程接口
PI	聚酰亚胺
劝学	君子曰：学不可以已。青，取之于蓝，而青于蓝；冰，水为之，而寒于水。木直中绳。（车柔）以为轮，其曲中规。虽有槁暴，不复挺者，（车柔）使之然也。故木受绳则直，金就砺则利，君子博学而日参省乎己，则知明而行无过矣。吾尝终日而思矣，不如须臾之所学也；吾尝（足齐）而望矣，不如登高之博见也。登高而招，臂非加长也，而见者远；顺风而呼，声非加疾也，而闻者彰。假舆马者，非利足也，而致千里；假舟楫者，非能水也，而绝江河，君子生非异也，善假于物也。积土成山，风雨兴焉；积水成渊，蛟龙生焉；积善成德，而神明自得，圣心备焉。故不积跬步，无以至千里；不积小流，无以成江海。骐骥一跃，不能十步；驽马十驾，功在不舍。锲而舍之，朽木不折；锲而不舍，金石可镂。蚓无爪牙之利，筋骨之强，上食埃土，下饮黄泉，用心一也。蟹六跪而二螯，非蛇鳝之穴无可寄托者，用心躁也。—— 荀况

1 前言

当今人们越来越依赖 Web 服务，如查看 E-mail，淘宝购物，百度搜索，这些 Web 服务已经和我们息息相关，我们很难想象没有他们的生活。而对于这些服务的提供者来说，确保服务资源能真正被用户使用，而不是被恶意机器人使用，是至关重要的。如使用机器人注册账户[1]，不仅会占用宝贵服务器资源，还为发布恶意信息埋下伏笔。所以区分访问来自人类还是机器人是十分重要的，验证码正是因为这个原因而被广泛使用。验证码（CAPTCHA）是“Completely Automated Public Tests to tell Computers and Humans Apart”[1–5]。的缩写。其主要思想是通过电脑向人类提问，通过回答来区分人和机器人。这个问题需要对人来说简单，而对电脑来说很难（或是需要很长时间）解决。

2 背景

目前在互联网上最流行的 CAPTCHA 系统，是基于文本的。但是，由于计算机视觉技术的提高，基于文本的系统很容易被攻击成功[6–8]。所以越来越多的研究者考虑如何替换掉基于文本的系统，于是有基于图像的[9–14] 和基于声音的[15,16] 系统。

2.1 文本验证码系统

总的来说，基于文本的验证码系统让用户识别字母或数字，GIMPY 是一个经典的例子[17]。攻击基于文本的使用大多使用 OCR(optical character recognition)。这个技术讲图片分割成晓得区域，每个区域只有一个字母，然后使用模式识别技术使用字母模板匹配每一个区块[6–8]。最后一步是一个比较成熟的 AI 问题。为了防止这样的攻击，基于文本的系统使用如下技术来增强鲁棒性[2,18]：

- 增加噪音：向图片中增加线和点，来干扰区域分割算法。
- 字符扭曲：对字符使用扭曲变换，或 3D 变换来增加文字识别难度。
- 字符连接或重叠：将两个或者多个字母连接或者重叠起来，使得攻击算法无法正确划分图片。

如图 2.1 ，a 很容易被 OCR 破解，b 引入了字符的重叠，c 引入了噪声，d 和 e 同时引入噪声和字符扭曲。

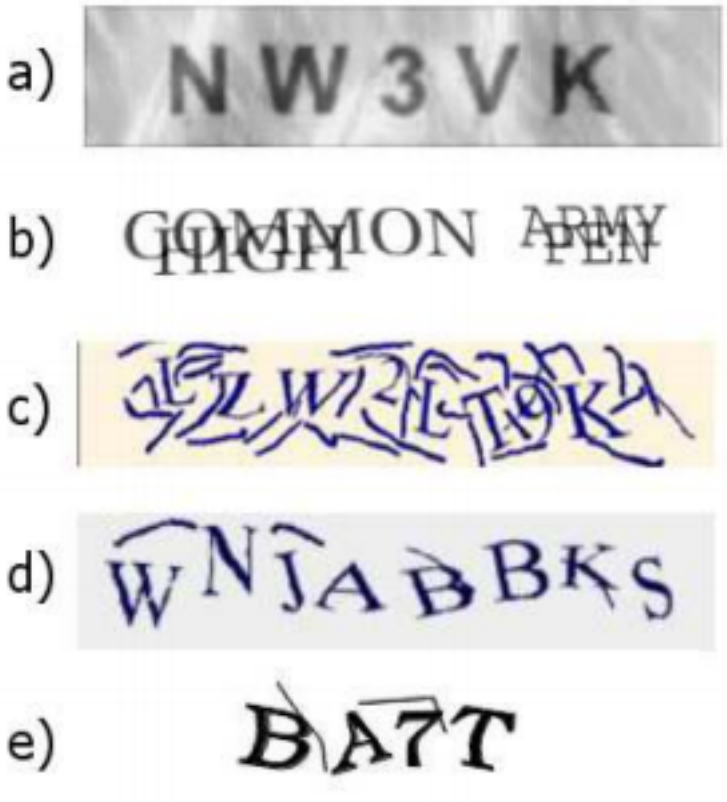

图 2.1 一些文本 CAPTCHA 的例子

然而，以上方法在提高系统鲁棒性的同时，也提高了人类识别的难度，特别是字符的连接。如字符“r”和“n”连接起来，看起来就像是字符“m”。字符扭曲也有可能增加用户识别的难度，如扭曲的后的”S“和”5“就很难分辨。还有些系统使用不同的颜色来标示每个字符，而这些都能很容易的被自动化的程序所移除，并没有给机器识别带来任何的难度[19]。而 reCAPTCHA[20] 提供了一种比较好的解决思路：使用两个单词来验证用户，其中一个是确定答案的，另外一个是不确定的。不确定答案的单词来自古籍中无法被自动化 OCR 程序识别的单词，确定答案的单词是机器生成的或者多个用户的答案是一致的来自古籍中的单词。这个过程既可以起到验证作用又可以数字化图书，是一个非常好的解决方案。但是还是这个解决方案还是有如下缺点：

- 对移动用户不友好：移动设备通常屏幕较小，输入困难，输入较长的单词对用户来说是一个极大的负担。
- 无法防御基于机器学习的攻击：基于机器学习的攻击，能比较容易的识别文本，此方法对与基于机器学习的攻击没有很好的鲁棒性。
- 易导致用户多次刷新：由于一个单词来自古籍，可能出现用户多次刷新来获得

清晰可读的验证码，而这对热门 Web 服务器来说，是一个极大的负担。

正是由于基于文本的系统固有的缺点，有了声音验证系统和图像验证码系统。

2.2 声音验证码系统

声音验证码系统弥补来了视觉障碍用户的可用性需求。一般的声音验证码系统让字母和数字被随机的声音间隔隔开，并向其中添加背景噪声。用户只有很少的时间去确定每个单词。某种意义上说，声音验证码系统仅仅是文本验证码系统的听觉版本，用声音替代可视化的东西，并没有明显的增加破解的难度。构成攻击的基础是相似的——特征提取和字符分类。对机器和人的难度曲线是相似的[21]。所以声音验证码系统既没有提供更加用户友好的接口，也没有更好的防范自动化程序的破解。这也就是它没有被广泛使用的根本原因。

2.3 图像验证码系统

图像验证码系统逐渐替代了越来越复杂的文本验证码系统，图像验证码有很好的用户接口，它主要利用人类对图片超乎想象的处理能力来区分人和机器。ESP-PIX[22] 让用户从一系列词中选择能描述素有图片的。SQ-PIX[23] 让用户标示出物品的所在位置，这对图片候选库提出很大要求，大部分图片可能需要人工处理。Google 的图片验证码“what’s up”[10] 让用户旋转图片，把图片旋转至正确方向。这个过程需要比较精确的鼠标移动，并且有些图片的方向可能是模棱两可的。Microsoft 的 Asirra[9] 使用 petfinder.com 上已有的数据库，让用户在 12 张图片中找到所有有猫的图片（其他图片都为狗）。而这些图片可能是模棱两可的，如图 2.2 中，左图中既有猫也有狗，右图中有一只长得像狗一样的猫。这样的验证码这个对于机器来说，难度只有区分狗和猫，而对于人来说，却可能花费很长时间解决。

12306 火车购票[24] 让用户从所有图片中选择系统指定内容的图片，如图 2.3 。但是同样也存在一个致命的问题：图片需要人工导入，并手动指定标签。有如下缺点：

- 人工失误：人工指定标签时给出错误标签
- 易遭受穷举攻击：因为人工指定，图片库不可能太大，穷举所有图片，并自动或手动指定标签即可很好的破解此类验证码
- 手工录入的标签信息很难复用：花费大量人力物力输入的信息除了验证码，并不能用在其他地方。

正是由于图片验证码系统普遍有需要手动录入图片的缺点，本文提出了一种**图片数据库自动增长**的方案来解决这个问题。

图 2.2 petfinder.com 中模棱两可的图片

图 2.3 12306 验证码

3 图片验证码自增长系统设计

不同于文本验证码系统，文本验证码系统可以生成问题图片，而图片验证码系统生成问题的过程很依赖图片数据库。这就决定图片数据库是图片验证码系统中至关重要的角色。图片数据库的的数据量大小和质量好坏，直接影响图片验证码系统的鲁棒性和用户友好性。数据量大能很好的避免穷举攻击，而数据质量高，能很好提升系统的用户友好性。如何提高图片数据库的数据量和数据质量，成了现在大多数验证码系统亟待解决的问题[11]。本文创新性的提出了一种图片验证码系统图片数据库自增长策略，能很好的解决这个问题。同时，本系统在设计之初就考虑到图片数据库复用问题：利用海量数据，服务于图片语义化搜索。这使得本系统合理利用用户完成验证码过程中输入，为搜索引擎的图片语义化搜索做出贡献。

3.1 思路

reCAPTCHA 系统是基于文本的验证码系统，是借助于人类大脑对难以识别的字符的辨别能力，进行对古旧书籍中难以被 OCR 识别的字符进行辨别的技术。这是一个很好的”增长“思路。本系统参考了 reCAPTCHA 系统，将其改进以适应图片验证码系统。

3.1.1 reCAPTCHA 系统

每次验证码会显示两个单词让人来识别，其中一个是需要用户识别的难认词，另外一个是答案已知的词。软件将能够正确识别答案已知词的用户看作是人类，当答案已知的词被正确识别出来后，程序会记录用户对无法阅读的词的回答并将其添加到它的数据库中。这样就完成了一次人工的 OCR 识别。为了改善软件的精确性，reCAPTCHA 会将最困难的词发送给多个用户并挑选其中有相同答案的作为正确的答案，确率能够达到 99%。用户每使用一次这个程序，实际上就是在帮助数字重现古籍。这项技术已经被 Google 广泛使用。

reCAPTCHA 系统提供了很好的利用用户输入来完成某种目的的思路。即利用用户对 OCR 无法识别单词的输入，完成古籍数字化工作。相思的思想可以用在图片验证码系统上吗？答案是肯定的。我们可以让**用户选择两种物体，其中一个的答案是确定的，起验证作用；另外答案一个是不确定的，起增长作用**。但是在实施的时候，任然需要对 reCAPTCHA 系统进行很多改进，才能使之很好的用在图片验证码系统上。

3.1.2 图片验证码的自学习与 reCAPTCHA 系统差异

图片验证码的自学习策略并不能直接把 reCAPTCHA 系统思路方案拿来使用，这由于图片验证码系统和文本验证码系统有着本质的区别：

- 验证问题生成：图片验证码依赖图像数据库，而 reCAPTCHA 系统一般是由系统随机选择一个单词，然后由系统生成一张包含单词图片交由用户识别。
- 用户输入类型：图片验证码一般是让用户点击选择图片，而 reCAPTCHA 系统是让用户输入图片中的文本。
- 图像分割：图片验证码需要预先将一张图片上物体分离出来，而 reCAPTCHA 系统只需要讲古籍上的单个字体提取出来，这个二者的难度完全不在一个量级。
- 预识别：图片验证码需要预先对图片加上描述标签，而 reCAPTCHA 系统并不需要任何预识别。

正是由于以上差异，图片验证码系统自学习系统要比 reCAPTCHA 复杂得多。其中特别是图像分割[25–28] 和预识别[29–31] 部分，涉及计算机视觉以及人工智能领域。

3.1.3 自增长策略

不同与 reCPATHCHA，我们可以讲古籍中的单词抠出后，经过少许处理即可交由用户。图片自学习系统不太可能设计成让用户输入图片中物体的名称，因为多个用户输入的图片名称可能是多个近义词或同义词的集合，如：土豆和马铃薯，这样就没有办法很好的规约图片中主体的名称。正是考虑到这个因素，我们需要对图片进行预识别，然后通过用户选择图片这一过程来验证机器的识别。即：需要用户选择带有两种标签的全部图片，其中带有确信标签（确信标签为`true`）图片起到真正的验证作用，而用户是否选择非确信标签（确信标签为`false`）的图片作为验证机器识别的依据。

大体过程如下：

1. 将Visual Dictionary 中带有标签图片的数据输入数据库中，并将他们的确信标签置为`true`
2. 使用预先有标签的图片数据集训练深度神经网络，使其具备初级的图片识别能力
3. 通过爬虫从网络上爬取图片
4. 将爬取图片筛选，初步处理

5. 将图片分割（image segmentation）成带有物体的子图（称为**主体**）
6. 使用具有初级图片识别能力的深度神经网络对图片标定预标签（标定多个标签，按置信度排序）
7. 将识别结果存入图片数据库中，并置确信标签为`false`
8. 按一定比例使用确信标签为`true` 和`false` 的主体生成图片验证码问题
9. 将用户验证成功的问题中是否选中确信标签为`false` 的主体信息记录到数据库中
10. 当确信标签为`fasle` 的主体验证次数和准确率都超过预先设定的阈值时，将确信标签置为`true`；当确信标签为`fasle` 的主体验证码次数超过，而准确率低于预先设定的阈值时，将标签置换为下一标签（置信度仅此与当前标签的标签），重置验证次数和准确率
11. 按一定时间时间或者按由`false` 转为`true` 的标签数量达到预先设定的值时，使用主体继续训练深度神经网络

顶级流程图如下：

3.2 设计

3.2.1 适应人类

3.2.2 图片爬虫

3.2.3 图片分割（image segmentation）

3.2.4 深度学习网络

3.2.5 验证码生成

3.2.6 置信标签修改

3.2.7 大数据处理

3.2.8 Web 服务

模型

授权与数字签名

4 图片验证码自增长系统分析

4.1 可用性
4.2 安全性
4.3 稳定性

5 图片验证码自增长系统评估

5.1 实现例子
5.2 用户研究
5.2.1 研究方案
5.2.2 时间统计
5.2.3 精确度统计
5.2.4 自学习策略

6 存在问题和改进空间

7 总结

参 考 文 献

[1] BAIRD H S, POPAT K. Human interactive proofs and document image analysis[G]//Document Analysis Systems V. Springer, 2002: 507–518.

[2] CHELLAPILLA K, LARSON K, SIMARD P, 等. Designing human friendly human interaction proofs (HIPs)[C]//Proceedings of the SIGCHI conference on Human factors in computing systems. ACM, 2005: 711–720.

[3] RUI Y, LIU Z. Excuse me, but are you human?[C]//Proceedings of the eleventh ACM international conference on Multimedia. ACM, 2003: 462–463.

[4] VON AHN L, BLUM M, HOPPER N J, 等. CAPTCHA: Using hard AI problems for security[G]// Advances in Cryptology—EUROCRYPT 2003. Springer, 2003: 294–311.

[5] VON AHN L, BLUM M, LANGFORD J. Telling humans and computers apart automatically[J]. Communications of the ACM, ACM, 2004, 47(2): 56–60.

[6] YAN J, EL AHMAD A S. A Low-cost Attack on a Microsoft CAPTCHA[C]// Proceedings of the 15th ACM conference on Computer and communications security. ACM, 2008: 543–554.

[7] MORI G, MALIK J. Recognizing objects in adversarial clutter: Breaking a visual CAPTCHA[C]// Computer Vision and Pattern Recognition, 2003. Proceedings. 2003 IEEE Computer Society Conference on. IEEE, 2003, 1: I–134.

[8] SIMARD P. Using machine learning to break visual human interaction proofs (hips[J]. Advances in neural information processing systems, 2005, 17: 265–272.

[9] ELSON J, DOUCEUR J R, HOWELL J, 等. Asirra: a CAPTCHA that exploits interest-aligned manual image categorization.[C]//2007.

[10] GOSSWEILER R, KAMVAR M, BALUJA S. What's up CAPTCHA?: a CAPTCHA based on image orientation[C]// Proceedings of the 18th international conference on World wide web. ACM, 2009: 841–850.

[11] CHEW M, TYGAR J D. Image recognition captchas[M]. Springer, 2004.

[12] DATTA R, LI J, WANG J Z. IMAGINATION: a robust image-based CAPTCHA generation system[C]// Proceedings of the 13th annual ACM international conference on Multimedia. ACM, 2005: 331–334.

[13] MATTHEWS P, MANTEL A, ZOU C C. Scene tagging: image-based CAPTCHA using image composition and object relationships[C]//Proceedings of the 5th

ACM Symposium on Information, Computer and Communications Security. ACM, 2010: 345–350.

[14] ZHU B B, YAN J, LI Q, 等. Attacks and design of image recognition CAPTCHAs[C]// Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010: 187–200.

[15] CHAN T-Y. Using a test-to-speech synthesizer to generate a reverse Turing test[C]//Tools with Artificial Intelligence, 2003. Proceedings. 15th IEEE International Conference on. IEEE, 2003: 226–232.

[16] BIGHAM J P, CAVENDER A C. Evaluating existing audio CAPTCHAs and an interface optimized for non-visual use[C]//Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2009: 1829–1838.

[17] Gimpy 项目[J]. http://www.captcha.net/captchas/gimpy/.

[18] EL AHMAD A S, YAN J, MARSHALL L. The robustness of a new CAPTCHA[C]//Proceedings of the Third European Workshop on System Security. ACM, 2010: 36–41.

[19] YAN J, EL AHMAD A S. Usability of CAPTCHAs or usability issues in CAPTCHA design[C]//Proceedings of the 4th symposium on Usable privacy and security. ACM, 2008: 44–52.

[20] Google reCAPTCHA 项 目[J]. https://www.google.com/recaptcha/intro/index.html.

[21] BURSZTEIN E, BEAUXIS R, PASKOV H, 等. The failure of noise-based non-continuous audio captchas[C]// Security and Privacy (SP), 2011 IEEE Symposium on. IEEE, 2011: 19–31.

[22] Esp-pix[J]. http://server251.theory.cs.cmu.edu/cgi-bin/esp-pix/esp-pix.

[23] Sq-pix[J]. http://server251.theory.cs.cmu.edu/cgi-bin/sq-pix.

[24] 12306 验证码[J]. https://kyfw.12306.cn/otn/login/init.

[25] 许新征, 丁世飞, 史忠植, 等. 图像分割的新理论和新方法[J]. 2015.

[26] 林开颜, 吴军辉, 徐立鸿, 等. 彩色图像分割方法综述[J]. 中国图象图形学报, 2005, 10(1): 1–10.

[27] 丁亮, 张永平, 张雪英. 图像分割方法及性能评价综述[J]. 软件, 2010, 31(12): 78–83.

[28] FELZENSZWALB P F, HUTTENLOCHER D P. Efficient graph-based image

segmentation[J]. International Journal of Computer Vision, 2004, 59(2): 167–181.

[29] LE D Q T, TIWARI S N, MERIALDO B. Deep Learning Image Recognition[J]. 2015.

[30] SIMONYAN K, ZISSERMAN A. Very deep convolutional networks for large-scale image recognition[J]. arXiv preprint arXiv:1409.1556, 2014.

[31] CIRESAN D, MEIER U, SCHMIDHUBER J. Multi-column deep neural networks for image classification[C]// Computer Vision and Pattern Recognition (CVPR), 2012 IEEE Conference on. IEEE, 2012: 3642–3649.