

信息安全工程课题研究

|  |  |
| --- | --- |
| 题目： | 文本验证码的设计和攻击 |

|  |  |
| --- | --- |
| 成 员： | 许志鹏 李子康 陈菊芳 |
| 院 系： | 软件与微电子学院 |
| 导师姓名： | 孙惠平 |

二〇一七 年 十 月

# **目录**

[**目录** 1](#_Toc496643262)

[第一章 选题背景 2](#_Toc496643263)

[第二章 产品现状 4](#_Toc496643264)

[第三章 研究现状 6](#_Toc496643265)

[第四章 主要思路 7](#_Toc496643266)

[第五章 项目分工 11](#_Toc496643267)

[第六章 项目计划 12](#_Toc496643268)

# 选题背景

CAPTCHA是“Completely Automated Public Test to tell Computers and Humans”(自动区分计算机和人类的图灵测试)缩写。验证码最初提出的目的是为了解决垃圾邮件问题。作为互联网时代早期最重要的免费邮件提供商，雅虎一方面要解决用户们每天遇到的数以百计的垃圾邮件轰炸，另一方面，他们自己的免费邮箱恰恰又是垃圾邮件的最爱——耗费无数资源所阻止的垃圾邮件，都来自于自己的服务器。这让雅虎开始认真考虑如何解决人机辨识问题。于是雅虎找到一位当时年仅21岁的天Luis vonda Ahn为他们解决这个难题。2002年，路易斯和他的小伙伴在卡内基梅隆第一次提出了CAPTCHA(验证码)这样一个程序概念。这个程序基于这样一个重要假设：提出的问题要容易被人类解答，并且让机器无法解答。在当时的条件下，计算机辨识技术还很落后，识别扭曲的图形，对于机器来说还是一个很艰难的任务，而人类却可以轻松的认出这些文字。这是一个简单而巧妙的设计，计算机先是产生一个随机的字符串，然后用程序把这个字符串的图像进行随机的污染，扭曲，再显示给显示器前的人或者机器。凡是能够辨识这些字符的，即为人类。yahoo在当时第一个应用了图形化验证码这个产品，很快解决了yahoo邮箱上的垃圾邮件问题，因此图形类验证码开始了大发展时期。

验证码能够防止网站恶意注册、防止恶意刷票、防止暴力密码破解、防止论坛垃圾广告信息。有效防止某个黑客对某一个特定注册用户用特定程序暴力破解方式进行不断的登陆尝试，目前验证码是现在很多网站通行的方式（比如招商银行的网上个人银行，腾讯的QQ社区），是当前每一个网站不可回避的设计，随着验证码的普及与发展，最初设计的文本验证码演变处一些新的形式，如目前国内部分商家使用的汉字验证码。验证码主要是运用于登录，注册，评论发帖等网站模块。

1. 防止网站恶意注册。许多机器人程序能自动注册账号，然后发布消息。使用验证码可以使得只有人能够发布信息而阻止机器人程序发布信息，这样保证了互联网正常的生态系统。有效阻止了病毒或垃圾信息横行，让用户能够更有效的利用互联网资源。
2. 防止恶意刷票。一个自动注册程序可以自动批量注册上千万的账号，继而到指定网站上刷票。使用验证码可以有效的防止恶意刷屏，为互联网保持一个更为公平的环境。
3. 防止暴力破解。盗号程序可以利用字典攻击尝试得到密码，若使用验证码，则能大大的降低暴力破解密码的可能性，提高互联网的安全性。
4. 防止论坛垃圾广告信息。机器人能自动登陆论坛发布垃圾信息，使用验证码则可以有效的阻止机器人自动发布垃圾信息。避免造成网络垃圾信息泛滥。

目前为止还没有一个系统的方法来设计或评估验证码。事实上，我们通过研究证明，许多流行网站还在依赖于在自动攻击中易受伤害的模式。由此，对于产生更多强健的验证码的综合设计与测试规则集有一个明确的需求。

全球通行的字母、数字验证码是目前最为广泛使用的一种较为简单的算法，也是相对访客而言较为人性化的简单设计之一。Web安全的攻击与防护技术一直是互相促进的，验证码识别技术的不断发展推动着验证码生成技术的提高。本文将从文本验证码技术的原理出发，介绍文本验证码容易出现的问题以及相关识别技术，以使读者对文本验证码攻防技术有一个了解。

# 产品现状

许多网站使用验证码来试图阻止与它们站点的自动交互，例如网站注册、网上密码找回、投票系统、在线交易、订票系统、信息发布、社交网络登录验证等环节，系统要求登录者必须输入验证码图片上所显示的数字或字母或中文字符才可以完成登录，以防止有人利用计算机机器人程序的自动大量登录社交网站账号或注册网站账号发布病毒或是垃圾广告。这些努力对于这些网站的成功是至关重要的，可以说，互联网处处都存在验证码，我们的互联网生活也离不开验证码。例如，Gmail通过阻止自动垃圾邮件制造者的接入来提高它的服务；eBay通过阻断来自诈骗网站的机器人来改进它的市场；Facebook制用于滥发邮件给诚实用户及在游戏中欺骗的配置文件的产生。最广泛使用的验证码将扭曲的字符与模糊技术相结合，这样人类识别容易但自动识别困难。

基于字符文本的验证码是现今互联网上使用最多的验证码，也是本文研究破解的验证码。这种验证码一般提供一张图片，图片中有数字或者大小写字母，如图2.1所示。为了加大字符提取分割和机器识别难度，往往在图片背景中加入点噪声、线噪声、复杂背景噪声，图片中的字符也可能空心、旋转、扭曲、粘连、坍塌、重叠和干涉线等。（使用此类方式的主要商家有：百度和eBay、qq邮箱、中国工商银行，中国农业银行，中国银行，百度网盘等等）



图2.1 字符文本验证码

也有的字符文本验证码中含有中文字符，目前主要出现在国内，由于中国人的母语是汉语，且汉字验证码对于机器的自动识别的抵抗能力要比普通字母和数字要好的多（常用汉字有3000个，字母只有26个），这使得汉字顺利成章的被应用到验证码中，但是中文验证码往往用户体验较差，因为需要的键盘输入更多，为改善这一状况，许多使用中文验证码的网站在选取中文字符时不再随机选取中文文字，而是选取一个成语，因为这样可以带来较少的键盘输入。图2.2显示了人人网正在使用的中文验证码。



图2.2 人人网中文验证码

文本验证码的特点是验证方式简单，人机交互性较好。

接下来介绍基于文本的验证码机制：

|  |  |  |
| --- | --- | --- |
| 验证码特点 | 举例说明 | 应用商家 |
| 干扰线、背景噪声 |  | 湖南大学教学服务系统网站  北京大学学生网上服务中心网站  交通银行登录验证码 |
| 复杂纹理背景 |  | 这个我还没有找到有哪些网站使用了 |
| 变换字体 |  | 北京大学选课系统（区分大小写） |
| 字符扭曲、旋转 |  | 支付宝网页登陆  Microsoft注册验证码 |
| 字符粘连 |  | 北京大学选课系统  Google注册验证码  Yahoo |
| 空心验证码 |  | 雅虎、腾讯、新浪、中国移动、百度 |
| 中文验证码 |  | 百度的门户网站登录、人人网 |

# 第三章 研究现状

一．验证码的设计

验证码作为一种区分计算机和人类的图灵测试的全自动程序，可以防止恶意破解密码、接收垃圾邮件等攻击者的不合法操作。尽管针对验证码的自动化攻击方式层出不穷，但是验证码仍是比较有效的安全工具。目前应用最广泛的验证码是基于文本将扭曲的字符与模糊技术结合的验证码机制，这种机制的特点就是需要用户来解决文本识别问题以此来区别人和计算机程序。大多数网站的验证码是通过服务器端产生的验证码图片传到客户端。

二．验证码的攻击

验证码识别过程大体上可分为三步：图片预处理，图片分割，图片识别分类。预处理可以移除图片背景干扰元素或是消除图像中可能干扰分割的其他附加元素；分割一般通过聚类算法将连续的验证码字符图片分割成单个字符图片；识别通过机器学习算法如支持向量机（SVM），k近邻（KNN）算法对字符进行分类识别。就准确性而言，分类器的选择不会影响太多，因为现在基于MNIST数据库的分类器表现明显很好（97%~99.5%）。在实践中，分类器的不同在实质上并不会改变系统的性能。相应地，我们选择评估易于使用的分类器而不是最优最佳准确率的。特别地，我们关注于可以快速训练以及需要最小参数调整的分类器。易于参数化以及快速的分类器是最佳选择，因为大多数工作在识别阶段之前完成，所以这一阶段应该尽可能稳定与快速

参考反识别技术和反分割技术来描述图像/文本处理，反识别技术的目的是组织单个字符的识别，反分割技术的目的是阻止解决者将验证码分割成单个字符。许多实验与攻击已经验证大多数确实可分割的验证码是易受损的。因此强健的基于文本的验证码必须使它难以被解决者确定每一个字符在哪里。尽管反分割技术对验证码的安全性来说是必不可少的，但它只有在验证的核心特征以及反识别技术被适当地设计与实现时才有效。

# 第四章 主要思路

一．验证码的生成

验证码的生成与web中的会话相关联，在一个会话开始时，在需要使用验证码的地方会生成一个与当前会话相关的验证码

，用户识别出验证码后通过填写表单将数据提交给服务器，服务器端会验证此次会话中的验证码是否正确，具体步骤如下（如图4.1所示）：

1. 用户请求访问起始页面，通常为登录页面；

2．由服务器端比如servlet随机产生几个字母或者数字，把这些拼接成字符串存储到session域中，同时通过一些图形类库加工处理，生成包含这些随机字符的验证码图片；

3．把验证码图片嵌在起始页面中返回到浏览器上；

4．用户访问起始页面，识别页面中的验证码，输入其他信息和验证码后提交表单；

5．服务器接收到用户提交的验证码值，并与之前存储在此session中的验证码值进行比较，判断客户端是计算机还是真实用户；

6．如果是真实用户，则按照预定流程进入下一步 ，否则将跳转到用户请求的起始页面中，同时刷新验证码。

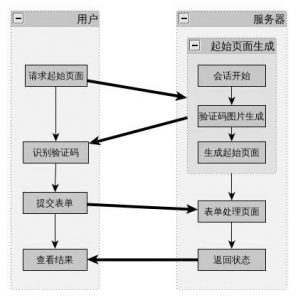


图4.1 生成与验证流程

从目前来看，仅生成固定长度的数字或字母的验证码已经能够很容易辨认出来，安

全性几乎为零，为了能大幅度提高验证码的识别难度，我们需要对验证码图片进行更多的加工处理，具体如下：

1. 验证码字符种类（字母或数字）随机、数量随机、字体种类和大小随机；
2. 验证码字符可以进行适当的伸缩或者旋转；
3. 验证码字符可以设置不同的颜色；
4. 验证码字符间最好都有粘连；
5. 背景颜色最好有一定的干扰性；
6. 图片样式（水纹、鱼眼、阴影等）最好有一定的干扰性；
7. 添加适当的干扰点、干扰线

二．验证码的攻击

验证码的攻击指的是通过计算机来比较准确的识别验证码，主要原理是通过一定的算法预先建立验证码范围内的字符特征库，再将获取到的验证码图片进行一定的预处理和分割，然后将得到的字符通过同样的算法生成特征，与之前保存的特征库进行比较，进而得到验证码的值。

一般地，其识别过程主要有以下的处理流程：

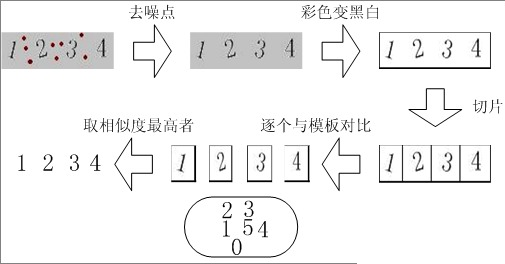


图4.2 大体流程

1. 图片二值化

图片二值化主要是为了将图像与空白区分开来，方便后续步骤的进行。把验证码的部分用1表示，背景部分用0表示，让图片变成2进制点阵。尽管验证码各个字符颜色可能不一样，图片背景颜色也不断变化，但我们还是能够通过RGB值很容易实现二值化。因为在制作验证码的干扰素时，为了使干扰素不影响数字的显示效果，必须使干扰素的 RGB 和数字 RGB 相互独立，互不干扰。

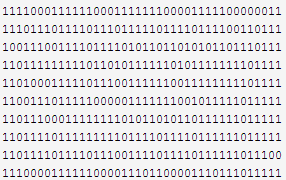


图4.3 图片二值化

1. 去噪处理

在二值化后，会有部分地方出现1，对于验证码上固定位置显示数字，这种干扰没有太大意义。但是对于验证码位置不确定的图片来说，在我们切割字符时，很可能造成干扰。所以，在二值化后要进行去噪处理。去燥处理的原理很简单，就是把这些孤立的1值去掉。如果一个点为 1 则判断这个点的上下左右上左上右下左下右 8 个方位上数字是否为 1 ，如果不为 1 ，就认为是一个燥点，直接设置为 1 即可。有时候的噪点可能是两个连续的 1 ，所以我们计算这个点的 8 个方向上的值之和，最后我们判断他们的和是否小于特定的阈值。

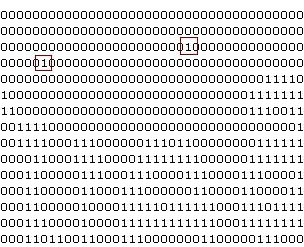


图4.4 去噪处理

1. 字符分割

为了能够识别出字符，需要对识别的字符图片进行分割，把每个字符作为单独的一张图片看待。分割字符的方法有很多种，这里采用最简单的一种，先垂直方向分割成为字符，然后在水平方向去掉多于的 0，如下图：

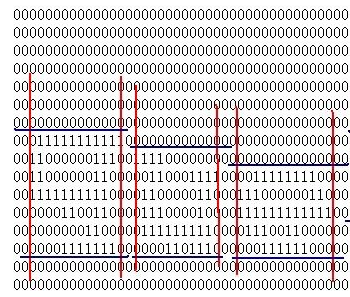


图4.5 字符分割

但是有的时候字符会存在粘连情况，规则字符的粘连比较容易处理。当完成分割操作后，我们不能马上确定分割的部分就是一个字符，要进行验证，验证的关键因素就是，分割下来的字符的宽是否大于阈值，这个阈值的取舍标准是，一个字符无论怎么旋转变形都不会大于这个阈值。所以，如果我们分割的块大于这个阈值，就可以认为这是一个粘连字符；如果大于两个阈值之和，就认为是三个字符粘连，以此类推。

1. 标准化处理

对于部分特殊的验证码，需要对分割后的图片进行标准化处理，也就是说尽量把每个相同的字符都变成一样的格式，减少随机的程度，最简单的比如旋转还原，复杂点的比如扭曲还原等等。

1. 字符匹配

字符的匹配可以有很多种方法，最常用的是模板对比。先建立所有验证码字符的特征库，一开始是人工标记写入特征库，然后通过标记更多的素材，训练出分辨能力和预测能力更强的特征模型，然后把图片处理后生成的字符特征与特征库里的模板特征比较，从中找出最相近的一个字符。

# 第五章 项目分工

许志鹏：负责验证码设计与攻击情况的调研；负责验证码的攻击，图片预处理和分割，探索使用机器学习方法进行验证码识别；参与验证码的设计。

李子康：负责验证码设计与攻击情况的调研；负责验证码的生成，设计验证码以增大识别难度；参与验证码的攻击。

陈菊芳：负责验证码背景和产品现状的调研；参与设计验证码；参与验证码图片预处理和分割。

# 第六章 项目计划

**第一阶段（2017年10月17日 - 2017年10月24日）**

前期准备阶段：阅读项目相关的论文，对目前的背景、产品现状、研究现状、实现方案进行调研，并形成自己的思路。目前已完成。

**第二阶段（2017年10月25日 - 2017年11月10日）**

初步实现阶段：实现基于javaWeb的验证码登录系统，生成验证码并进行识别，测试使用情况。目前已完成。

**第三阶段（2017年11月11日 - 2017年12月20日）**

具体实现阶段：设计改进验证码以增大识别难度，实现对验证码的破解和识别。

**第四阶段（2017年12月21日 - 2018年12月30日）**

后期总结阶段：测试验证码的设计和攻击情况，总结相关的技术问题，撰写论文。