新型三维可操控验证码设计与实现

陆嘉辉 / 上海市上海中学
指导教师　吴奕明

◉ 研究背景

在验证码出现以前，黑客可通过暴力搜索破解账户密码，造成用户的巨大损失；垃圾评论也可轻松通过任何一个网站的注册程序，覆盖有意义的内容使网站瘫痪。许多网站为此设置了发贴时间间隔、同一 IP 地址发贴数、内容不能重复等多种限制防止论坛灌水，但是这些手段都不是非常有效。同时，网站对账号的保护并不能使用上述方法，所以信息安全专家们发明了验证码，以解决此类问题。

虽然验证码已被很多网站使用，它还是存在许多漏洞。随着 OCR 识别技术的不断发展，简单的字符式验证码已经很难起到较好的防护作用；而目前正在开发的非字符式验证码，用户使用起来又有一定的困难。因此，本文提出验证码隐藏概念，将验证码字符旋转至球体任意位置而不直接显示在界面上，在一定程度上降低入侵计算机的识别概率。

◉ 三维验证码的设计

➲ 对当前验证码发展的分析与反思

笔者对目前争议较大的验证码技术进行了分析，发现一些它们误入歧途的原因。

验证码首要的目标是用户能识别并输入，一旦设计过度，就会给用户造成很大的麻烦。比如：字符变形过度，字符全都挤压在一起，让人难以辨别；背景具有干扰性，即所谓的喧宾夺主——用户通常不用的字符很难输入；非常识性验证码问题——用户都不希望仅仅为了输入验证码，还要用纸和笔计算一下。

由此，笔者认为一个好的验证码应当具有以下性质。

◈ 易于用户识别：验证码的前提是用户能识别，否则用户会因不能正确输入验证码而不能登录网站。

◈ 干扰机器识别：验证码如果没有该效果，其用途和功能就形同虚设，反而成为用户上网过程中的障碍。

◈ 随机生成：一旦验证码题目数量有限，入侵计算机就可以通过累积有限的验证码，生成数据库破解。

◈ 实现简单：尽管验证码是网络安全的重要一环，但毕竟不是网页要表现的内容，因此验证码的实现不能过分困难，否则就是安全成本的浪费。

➲ 新型验证码的思路来源及设计思想

如今，验证码已经不只局限于二维形式。一些专家和研究人员对三维形式的验证码已经有所探究。其表现形式主要有以下 2 种。

◈ 动态验证码。Windows 系统中曾经有 1 个屏幕保护程序——三维文字（图 1）。动态验证码也是通过创造 1 组动态式文字，使其在显示界面中进行平移和旋转，攻击者只有在有效解决运动对象识别的难关后才能进行字符识别。然而这种运动并不是随机的，终将有一个循环，破解者就可以选取一个循环并逐帧尝试识别，就会有一定的可能性识别出验证码。

◈ 立体验证码。立体验证码虽然是静态的，但由于目前机器识别单个立体字符的概率仅为 5%，识别整串字符就更困难了。不仅如此，立体验证码可以与普通验证码一样进行拉伸、收缩、扭曲等，而背景的叠加更增加了机器识别验证码的难度，而字符的三维化和立体旋转也在一定程度上增加了用户识别的难度（图 2）。

有没有一种新的方法，既能避免动态验证码无法避免的循环，又能防止静态立体验证码对用户识别的影响呢？笔者从这个问题入手，设法实现自己的新型验证码。

验证码的质量多从机器识别难度和用户识别难度 2 方面进行衡量，评估结



图 1

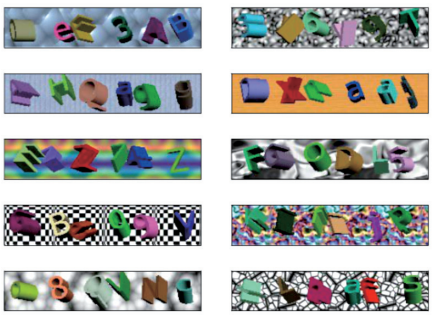


图 2

果通常会偏向一边：不是过分容易被机器识别，就是太不容易被用户识别。因此，本课题设计的验证码必须尽可能地做到两者的平衡。

从机器识别难度方面进行考虑，主要有 2 大因素：机器分析 1 个字符所需时间和机器识别字符的成功率，前者要尽可能长，后者要尽可能低。鉴于如今计算机尚不能很好地识别三维物体及三维验证码，我决定采取三维立体方式呈现验证码。由于图形验证码较难让用户理解自己需要做的事情，且随机性不是很强，所以仍选择传统字符作为输入和输出的内容。

➲ 系统环境

◈ C#（C Sharp）。Microsoft Visual C# 是一种功能强大、使用简单的面向对象语言，主要面向需要使用 Microsoft .NET Framework 创建应用程序的开发者。C# 在保持 C 语言风格的表现力和雅致特征的同时，能够让用户快速开发应用程序。

◈ OpenGL（Open Graphics Library）。OpenGL 图形系统是图形硬件的 1 个软件接口，它允许使用者创建交互性程序，产生移动三维物体的彩色图像。OpenGL 广泛应用于游戏、医学影像、地理信息、气象模拟等领域，是高性能图形和交互性场景处理的行业标准。

➲ 设计路线

◈ 绘制 1 个可由用户控制旋转的三维球体。首先绘制 1 个 20 面体（坐标存放在数组中），然后通过递归算法将 20 面体细分为 80 面体、320 面体，直至近似球体。运用 OpenGL 旋转函数，利用滚轴控件完成对球体的拖动。

◈ 给球面上的每个部分按指定规则随机生成 1 组像素值（图 3）。

◈ 将验证码中的字符投影在该球体上（目前的方法为生成字符坐标库）。

◈ 生成随机噪音线：随机生成 2 个坐标点，连接成线。

◈ 显示在界面上让用户识别，无论是用户输入成功或失败，验证码都会刷新。

➲ 新型验证码的改进方向

◈ 字符不能仅有 1 个，否则识别率太高。

◈ 球体透明化，屏幕内的字符在球面投影时相互叠加，使机器识别难度提高。

◈ 扩大适用范围。仅使用上述 2 种方式并不能做到面向全体用户，主要原因是对球体上的数字识别能力因人而异。所以，可以让用户提前选择自己能够识别的难度，以此减少用户操作时不必要的麻烦。

◈ 如同普通字符式验证码，三维可操控验证码的球体和字符大小也都是随机决定的，能够对机器的识别产生干扰。

◈ 无滚轴操作：用鼠标拖动每个字符的三维旋转的滚轴进行操作，对于用户使用过于麻烦。在此可以实现更简单的方法，即用户可以直接在每个字符上用鼠标拖拽实现球体旋转。

➲ 测试实验

我使用的实验方式非常简单：在用户界面上选择 1 个角度，将验证码转换成 BMP 图像，让识别程序（用 VC 编制）尝试识别，从而得出识别成功率。图 4 为验证码球体相对于验证码（字母和数字）正对屏幕时机器识别的概率（每组 20 个），其中横轴为旋转角之和，纵轴为识别概率。

由图 4 可见，尽管在字符正对屏幕时的识别概率较大，但随着旋转角的增加，验证码的识别率显著减小；而当旋转超过 90° 时，机器几乎不能识别。同时，在仅采用数字的情况下，该验证码的表现已相当不错。

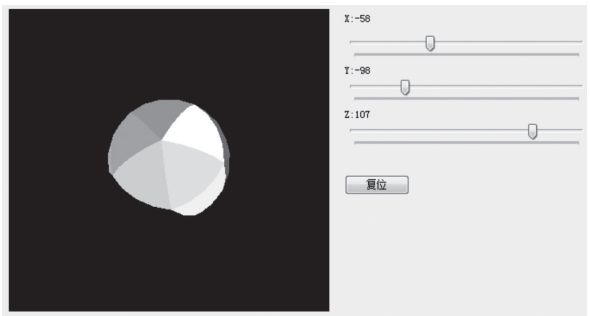


图 3

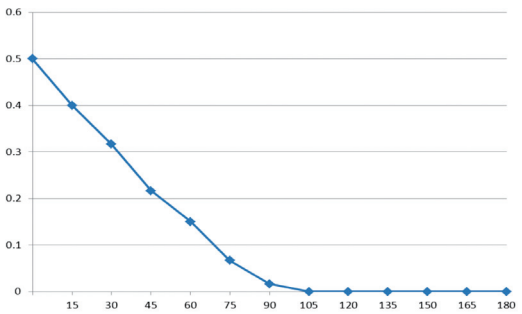


图 4

➲ 新型三维可操控验证码的创新性和实用性

目前，三维图形技术和人机交互技术的发展相当迅速，在验证码中也有了一定的应用。然而，正在使用或最新创造的验证码还没有将这两者整合运用。本课题设计的三维验证码最大的创新点在于它生成的球体能够通过用户的控制旋转，可以大大降低破解者的识别率，主要其主要原因有二：

◈ 由于验证码分布于立体上，使得原来平面形式的字符不一定能同时出现在屏幕视角中，而总是会缺少一些部分，显示残缺的字符，不能对应到机器的字符库；同时，由于投影面为球面，使得平面上的字符会有所扭曲，从而降低了入侵计算机的 OCR 识别率。

◈ 由于球体是可以旋转的，攻击者不知道初始的旋转角度，识别的概率因此进一步降低。破解这种新式验证码的方法仍为 OCR（本质上仍旧是机器对字符的辨识），但由于加入了 1 个新的干扰因素即旋转角度，攻击的时间复杂度必须乘以枚举数（360 的立方），显然大大增加了破解的时间。

在实用性方面，本课题设计的验证码并不因安全性提高而降低便捷度。在生成验证码的时间复杂度上，该验证码与现行的普通二维验证码相差无几，并不会占用太多的运行时间，用户也不会因此而需要增加等待时间。除此之外，该验证码面向各类用户，可以根据用户的识别能力进行适当的调整，降低用户的使用难度。

◉ 改进方向

◈ 字符多样化。将字符的种类从数字、字母拓展到汉字，进一步降低机器的识别成功率。而由于汉字是方块字，投影在球面上能够遮挡更多的文字部分，使破解者更加无从下手。

◈ 纹理贴图。目前，生成字符坐标库的实现方法不够简单，而将计算机中的每一个字符位图直接在立体表面贴图的方法更加便捷。此技术的采用能加快实现汉字验证码的脚步。

◈ 网络应用和人性化改进。“看不清”、“换一张”等人性化元素也是需要添加的。只有这样，才能给用户呈现一个良好的界面，让他们习惯于使用，新型验证码才能被广泛运用。

◉ 结论

应用验证码技术是防止入侵计算机重复攻击、批量注册的有效方法。本文提出了 1 种生成验证码的新方法，具有球面遮挡、投影扭曲和随机旋转等 3 个特点，能够有效地防止攻击者对机器的破解，一定程度上保护，网络安全，具有一定的使用前景。

该项目获得第 27 届全国青少年科技创新大赛创新成果竞赛项目中学组计算机科学一等奖。

专家评语

验证码是防止计算机入侵和恶意程序的一个重要研究领域，近期已有人开始研究自动识别验证码，该项目考虑设计三维验证码，把平面三维码投影到球面上，而且可以用鼠标操控球面的旋转增加验证码的不可识别性。项目想法创新，可以直接使用。■