目录

[游戏 2](#_Toc357067458)

[业务目标 2](#_Toc357067459)

[账号 3](#_Toc357067460)

[可能的实现方法 3](#_Toc357067461)

## 游戏

重返大航海（网页游戏）<http://dhh.txwy.com/>

## 业务目标

进入游戏 -> 点击酒馆 -> 情报打听



* 开始投掷



* 点金币
* 确保金币转，点击鼠标左键，金币为正面。一直7个都是正面。

正面：

背面：骷髅头

如果7次都是正面，则可以得到丰厚的奖励。  
特别是到5个以后的奖励是地图，就可以探索到我需要的造船材料

## 账号

* 账号hchenga2 密码：klmydn12 双线8区（正式账号，测试时不能使用该账号）
* 账号hchenga1 密码 klmydn12 12区（测试时可使用该账号）
* hchenga2 klmydn12 双线8区（测试时可使用该账号）

## 可能的实现方法

时时采样屏幕图象，同时按照鼠标确认的地址附近图象进行一些判断（判断为正面时，就模拟点击鼠标左键）。

## 研究计划、步骤

1. 网上调查实现该功能的方法，确定技术方案。

## 技术方案

1. 使用“按键精灵”软件，通过编写脚本，捕获金币图像，判断为正面时点击鼠标（我使用该技术方案，但是最终没有实现业务目标。详见“按键精灵分析”）
2. 截获包，分析游戏数据，修改游戏数据，发送到服务器。（详见“游戏外挂设计技术探讨4 http://www.hackbase.com/subject/2009-04-09/14341.html”）

## 按键精灵分析

我研究了按键精灵了，它功能确实强大。  
我通过编写脚本，成功识别出了正面，并自动点击鼠标。但是结果并不是每次都一样！比如这次运行脚本，金币停的时候为正面，下次在同样条件下运行脚本，金币停的时候却为背面了！  
  
所以不能通过“捕获金币图像，判断为正面时点击鼠标”的方法来达到您的目的（6次都为正面）。  
我认为可能有两个原因造成这种方法失败：  
（1）金币是随机转动的，一会快一会慢。  
比如对于捕捉同一个图像C:\Users\lr\AppData\Roaming\Tencent\Users\395976266\QQ\WinTemp\RichOle\Q2AB0JB@}ER_{S@`8}19W5O.jpg，第一次点击时金币为正面，第二次点击时金币就为背面了！由于有随机的因素，所以不能通过“捕获金币图像，判断为正面时点击鼠标”的方法来达到您的目的。  
（2）因为脚本运行有延迟。  
从捕捉到图像到点击鼠标中间有延迟，且该延迟在一定范围内波动不固定。所以导致每次脚本运行时，捕捉到图像后鼠标点击的时机都不一样，造成一会正面，一会背面。  
综上所述，想要直接通过软件来“捕获金币图像，判断为正面时点击鼠标”是行不通的。

## 与客户（贺诚-郝老师同学）聊天记录

郝老师同学-贺诚 20:10:45

小杨：现在开始实验了吗？

y 20:10:59

实验了，发现不行。

y 20:11:19

稍后我会把分析报告发给你哈

郝老师同学-贺诚 20:11:25

你可以取图象了

y 20:11:46

取图像不是那么简单的。。。。。。

y 20:11:59

我会在分析报告中说明

郝老师同学-贺诚 20:12:01

也是最关键的

y 20:12:54

取图像需要截获包，还要分析转化，需要很多知识

郝老师同学-贺诚 20:13:08

是呀！

y 20:13:10

模拟鼠标点击很简单

y 20:13:21

我用模拟鼠标点击试了下

y 20:13:41

我发现金币转是随机转的，并不是固定转的

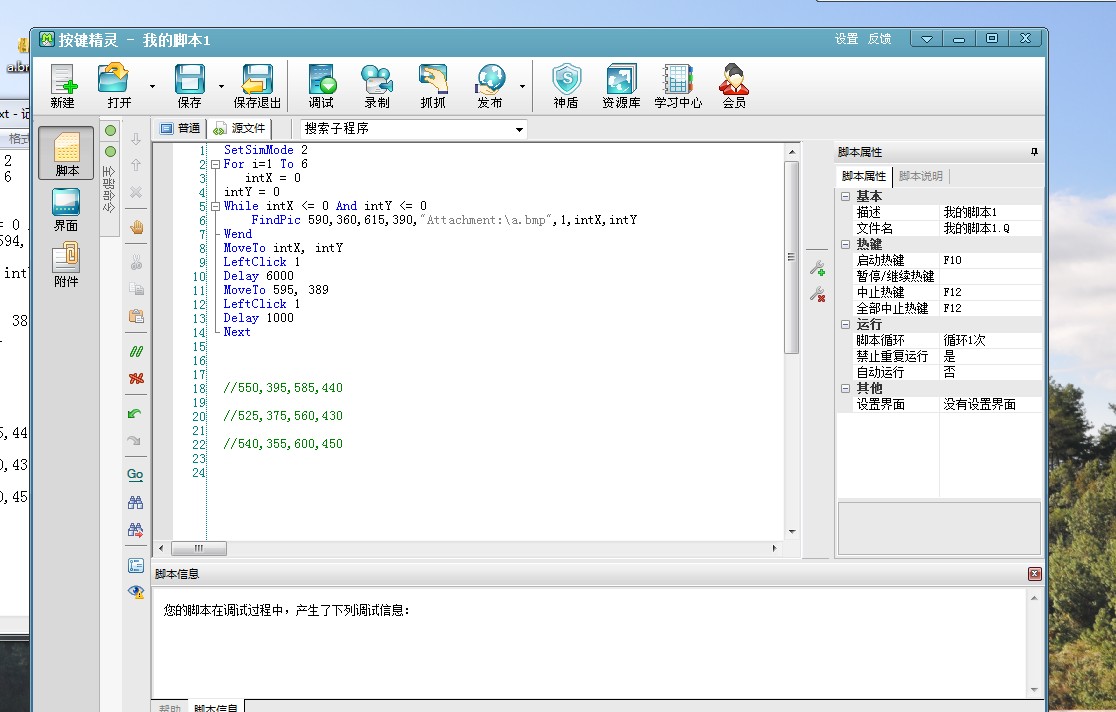
郝老师同学-贺诚 20:14:58

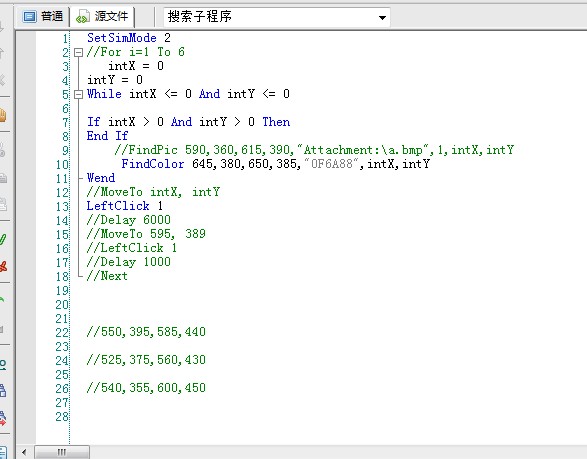
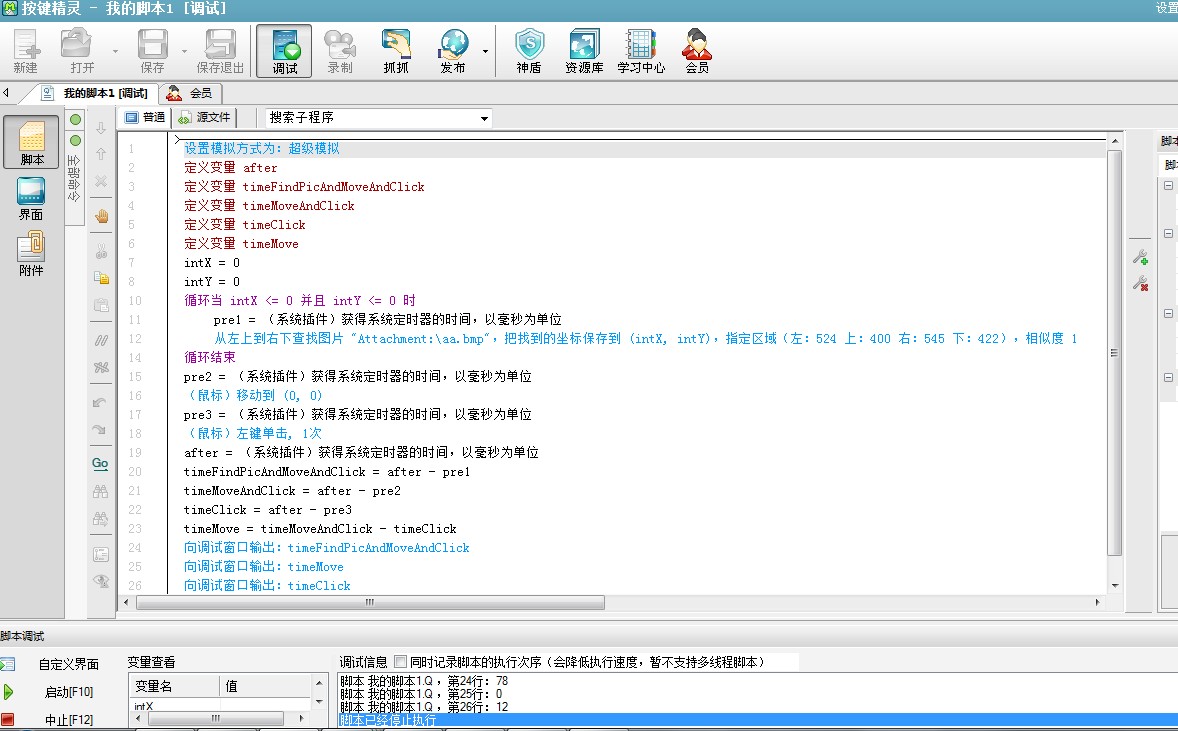
它不是匀速转动

y 20:15:01

当前为第一个金币。点开始后，假设1s后点击鼠标，金币为正面。那么重新开始，也是第一个金币，点开始后，1s后点击鼠标，并不一定是正面。

y 20:15:03   
对  
y 20:15:11   
它不是有规律转动的  
y 20:15:18   
所以必须分析图像  
郝老师同学-贺诚 20:15:23   
所以才需要判断图象  
y 20:15:37   
但是分析图像需要网络编程、汇编等知识  
y 20:15:48   
难度较高  
y 20:16:13   
就跟直接修改游戏数据技术差不多  
y 20:16:47   
先要拦截socket包，拦截游戏图像数据的包  
郝老师同学-贺诚 20:16:58   
我想你是否能直接从显示卡缓存取数据进行判断  
y 20:16:59   
然后分析游戏数据，破解数据  
y 20:17:24   
判断哪个包代表正面，哪个包代表背面  
郝老师同学-贺诚 20:17:31   
不管游戏是什么  
郝老师同学-贺诚 20:17:48   
不要进入游戏软件  
y 20:18:16   
还要在图像为正面时，伪造鼠标点击，并发送到服务器端  
y 20:18:35   
“不要进入游戏软件”什么意思？  
郝老师同学-贺诚 20:18:46   
不管游戏是什么  
郝老师同学-贺诚 20:19:06   
我只管一点显示  
y 20:19:42   
先要截获游戏数据  
郝老师同学-贺诚 20:19:53   
也就是我直接从显示缓充区取数据进行判断  
y 20:20:02   
，，，。。。  
郝老师同学-贺诚 20:20:05   
不管游戏数据  
y 20:20:06   
我知道你的意思  
y 20:20:15   
你说的显示缓充区是客户端  
郝老师同学-贺诚 20:20:21   
对呀  
郝老师同学-贺诚 20:20:32   
就是我们看的屏幕！  
y 20:20:52   
但是是要把数据发到服务器端的  
郝老师同学-贺诚 20:21:01   
这个显示，不管是什么软件  
y 20:21:56   
我们需要先截获服务器端的数据，分析什么数据代表图像正面，什么数据代表鼠标点击。然后伪造图像正面且点击鼠标的数据，发送到服务器端  
郝老师同学-贺诚 20:22:04   
仿一个鼠标按键相好给  
郝老师同学-贺诚 20:24:06   
当然如果取显示数据比较难，可以用摄象头直接摄象，然后仿鼠标从外围给一个鼠标按键信号！  
y 20:27:21   
贺老师，您现在方便说话不？  
郝老师同学-贺诚 20:27:32   
可以呀  
y 20:27:37   
语音哇  
y 20:27:52   
或者您电话是多少？  
y 20:28:03   
电话里说要好说点哈  
郝老师同学-贺诚 20:28:12   
直接在QQ上  
c:\users\lr\appdata\local\temp\53`nwnek$s{2j_kyy37r${m.png20:28:34  
您的麦克风没有声音，请点击查看  
y 20:28:43   
听得到吗、？  
郝老师同学-贺诚 20:28:50   
没有  
y 20:28:56   
听到了吗？  
y 20:29:25   
听得到吗？  
郝老师同学-贺诚 20:29:31   
不能  
y 20:29:34   
等下哈  
y 20:29:52   
我听得到你说明  
y 20:29:53   
说话  
y 20:30:06   
稍等下  
y 20:33:07   
我弄好后联系你哈  
郝老师同学-贺诚 20:33:13   
好  
y 20:33:14   
我弄好后联系你  
y 20:33:20   
先下了  
y 20:33:23   
马上上  
y 20:33:32   
好的  
c:\users\lr\appdata\local\temp\x2d])rzbqveo9yt2]jepj8p.png20:33:37  
您中止了语音通话，通话时长5分13秒。  
C:\Users\lr\AppData\Local\Temp\$7G~6@79V%(@R9VZP(_%QZL.png2013-05-31C:\Users\lr\AppData\Local\Temp\10%FCBQZ]K6Y4$[C~N9XBQO.png  
y 14:28:34   
您好！请问在吗？  
郝老师同学-贺诚 14:28:36   
[自动回复]您好，我现在有事不在，一会再和您联系。  
y 14:31:37   
我研究了按键精灵了，它功能确实强大。  
我通过编写脚本，成功识别出了正面，并自动点击鼠标。但是结果并不是每次都一样！比如这次运行脚本，金币停的时候为正面，下次在同样条件下运行脚本，金币停的时候却为背面了！  
  
y 14:32:24   
所以不能通过“捕获金币图像，判断为正面时点击鼠标”的方法来达到您的目的（6次都为正面）。  
y 14:43:08   
我认为可能有两个原因造成这种方法失败：  
（1）金币是随机转动的，一会快一会慢。  
比如对于捕捉同一个图像c:\users\lr\documents\tencent files\395976266\image\eh`0ho}uh8f8d@hma{p@a`w.jpg，第一次点击时金币为正面，第二次点击时金币就为背面了！由于有随机的因素，所以不能通过“捕获金币图像，判断为正面时点击鼠标”的方法来达到您的目的。  
（2）因为脚本运行有延迟。  
从捕捉到图像到点击鼠标中间有延迟，且该延迟在一定范围内波动不固定。所以导致每次脚本运行时，捕捉到图像后鼠标点击的时机都不一样，造成一会正面，一会背面。  
y 14:44:13   
综上所述，想要直接通过软件来“捕获金币图像，判断为正面时点击鼠标”是行不通的。  
郝老师同学-贺诚 15:53:22   
我在！

看来按键精灵不行！  
郝老师同学-贺诚 15:56:00   
你搞的按键精灵软件，是否可以在晚上8点或者9点使用一下，那个时候金币转的比较慢！  
郝老师同学-贺诚 15:57:53   
还有一个方法就是判断出反面后延时一点时间在给出按键信号  
y 16:39:55   
"还有一个方法就是判断出反面后延时一点时间在给出按键信号“也是不行的  
  
郝老师同学-贺诚 16:41:43   
第一、你先搞一个录象的软件，然后慢放分析一下金币转动情况  
y 16:41:50   
因为金币转动一会快一会慢，也就是说，假设脚本设置判断出反面后延时100毫秒点击鼠标，这样第一次为正面。但是因为因为金币转动一会快一会慢，所以第二次需要延时200毫秒点击鼠标金币才为正面了  
y 16:42:22   
转动是随机的。。。。。。  
y 16:42:36   
只有直接修改数据  
郝老师同学-贺诚 16:42:42   
录象后可以慢放！  
y 16:42:51   
没有规律的  
y 16:42:58   
应该是没有规律的  
y 16:43:28   
我晚上8点过再试下  
y 16:44:00   
  
y 16:44:07   
这个是我写的脚本  
郝老师同学-贺诚 16:44:51   
主要是按键精灵不是可以控制的，如果是自己写的程序，就可以先判断一下金币转速！  
y 16:44:55   
这里的关键是，因为金币转动的时间不是固定的，因此不能把时间写成死时间  
y 16:45:04   
。。。  
郝老师同学-贺诚 16:45:48   
另外不知道按键精灵判断图形需要多少时间  
y 16:46:02   
比较慢  
郝老师同学-贺诚 16:46:33   
如果你要它判断点是否可行  
y 16:46:51   
游戏中金币转得太快了，以至于一般要转个20圈的样子才能匹配到一次图片  
y 16:47:17   
  
郝老师同学-贺诚 16:47:30   
正面和反面不是有些点颜色不一样  
y 16:47:33   
这样脚本你应该就看的懂了  
郝老师同学-贺诚 16:47:47   
不懂！  
y 16:48:07   
你说的是怎样判断图片  
郝老师同学-贺诚 16:48:12   
我现在把软件都给还给老师了  
y 16:48:54   
我能够使用按键精灵”判断图片是否为正面，为正面时则将鼠标移到金币的位置并点击“  
y 16:49:18   
但是因为金币转动是随机的，这种方法并不是每次都成功  
郝老师同学-贺诚 16:49:41   
我记的以前都是判断一个点的颜色，这样就非常快  
y 16:49:56   
你说的是取色  
y 16:50:03   
我用的是取图像  
y 16:50:10   
那我再试下取色  
郝老师同学-贺诚 16:50:44   
还有，你可以先把鼠标放在需要点的地方，这样就直接取那里的点颜色  
y 16:51:00   
好的，我再试下  
郝老师同学-贺诚 16:51:24   
这个你慢慢实验吧！  
郝老师同学-贺诚 16:51:56   
你现在是上博士？  
y 16:52:00   
研究生  
郝老师同学-贺诚 16:52:17   
快毕业了吧！  
y 16:53:13   
还有1年  
郝老师同学-贺诚 16:53:31   
加油！  
y 16:53:45   
C:\Users\lr\AppData\Local\Temp\WML`ZUS$8NCVU(%7M%5VUJI.gif谢谢  
郝老师同学-贺诚 16:54:18   
毕业后是继续上还是已经找好工作了  
y 16:54:34   
找工作哈  
郝老师同学-贺诚 16:55:24   
我以为你还想上学，然后在大学当老师  
y 16:55:55   
不读了哈  
郝老师同学-贺诚 16:57:06   
你先研究，我有正式项目在找你  
y 16:57:14   
嗯，好的  
郝老师同学-贺诚 16:57:22   
886  
y 16:57:28   
嗯，88  
y 17:10:02   
  
y 17:10:28   
我用了找色了，还是不行  
郝老师同学-贺诚 17:10:53   
找色应该多用几个点！  
y 17:11:04   
如果是判断背面的话，找色还要好找点（骷髅的颜色比较特殊），但是正面的话颜色就不是那么特殊了  
y 17:11:17   
多用几个点就相当于去个图像  
y 17:11:28   
找色一次只能找一个点  
y 17:11:38   
找图像就是一次判断一个范围的点  
郝老师同学-贺诚 17:11:46   
3个点，顺序判断  
y 17:12:52   
用”找图像“就是区域判断  
郝老师同学-贺诚 17:13:00   
如果是判断背面就给一定的延时，如果判断正面就不延时

用”找图像“就是区域判断  
郝老师同学-贺诚 17:13:00   
如果是判断背面就给一定的延时，如果判断正面就不延时  
y 17:13:11   
不管取多小的区域，关键时金币转动是随机的  
郝老师同学-贺诚 17:13:30   
区域判断估计是点太多！时间太长  
y 17:13:35   
同一条件第一次为正面，可能下一次同一条件下按就为背面了  
y 17:14:00   
您说的减小延迟，只能减小脚本匹配到正面的时间  
y 17:14:31   
这个是可以优化，关键是匹配的正面后，点击鼠标不一定每次都是正面  
y 17:14:41   
因为有随机的因素  
y 17:14:46   
这是根本问题  
y 17:14:57   
不知道您明白我的意思没  
y 17:15:22   
  
郝老师同学-贺诚 17:15:26   
对呀，本来是判断到正面立即给鼠标信号，但是你说他会出现反面！  
y 17:15:34   
对  
y 17:15:41   
这是游戏里的随机因素  
y 17:15:51   
我怀疑这个是随机出现的  
y 17:16:19   
也就是说，你看到是正面并点击鼠标，那么结果并不是每次金币都是正面  
y 17:16:25   
也有可能是背面  
郝老师同学-贺诚 17:16:46   
我知道，你能不能写一个程序测量一下判断图象到给出鼠标信号用多少时间  
y 17:16:46   
反过来说也一样，看到金币为反面时点击鼠标，结果金币也可能是正面  
y 17:17:02   
这个测试了也没用  
y 17:17:59   
从根本上来说，对于这种随机的图像，只有分析游戏数据  
郝老师同学-贺诚 17:19:45   
这个测试就是能够确认我们在正面的时候给鼠标信号是否一定得到正面图象，比如我们说的那个时间如果只有100毫秒，那一定是你说的不管我们给信号在那里，他都是随机给出正反面  
y 17:22:07   
那我看能不能测试  
郝老师同学-贺诚 17:23:05   
你可以写一个变换颜色的显示程序，然后就可以测试了  
郝老师同学-贺诚 17:24:39   
 比如一种颜色只显示40毫秒，当接受到一个鼠标信号后立即停止颜色变换！  
y 17:25:16   
我先测试下  
郝老师同学-贺诚 17:26:47   
好的！有时间我们好好聊一下，如果我了解你的研究方向！说不一定我在深圳给你找一个好工作  
y 17:27:26   
谢谢  
y 18:02:36   
  
y 18:03:38   
您好！经过我的测试，判断图像时间+鼠标移动时间+鼠标点击时间<80毫秒  
y 18:03:50   
鼠标移动时间约等于0毫秒  
y 18:04:00   
鼠标点击1次的时间小于20毫秒  
郝老师同学-贺诚 18:04:30   
那就是说金币游戏是随机的  
y 18:06:28   
对，这个金币游戏的转动应该是随机的  
y 18:06:40   
  
y 18:07:04   
我又试了下，我是在估计为背面时用手点的  
y 18:07:25   
结果前两次为正面，这次为背面  
郝老师同学-贺诚 18:14:15   
那就没有办法了！我就不玩这个游戏了吧！  
y 18:15:41   
可以用”逆天改命“  
郝老师同学-贺诚 18:17:09   
我玩游戏不充钱！没有多少金币  
y 18:17:35   
嗯  
郝老师同学-贺诚 18:18:00   
你现在玩什么游戏吗？  
y 18:18:26   
四国军棋、连连看、dota  
郝老师同学-贺诚 18:19:08   
不少呀！都是要很费脑力的  
y 18:19:30   
只是偶尔玩下哈  
y 18:25:25   
贺老师，这次没能让您成功刷金币我感到非常遗憾，以后有机会再合作哈！  
郝老师同学-贺诚 18:25:52   
这个也是玩一下！  
郝老师同学-贺诚 18:26:03   
你现在研究方向是什么？  
y 18:27:14   
我现在主要在做网页游戏，用的是web技术  
郝老师同学-贺诚 18:27:39   
不错呀！  
y 18:28:09   
呵呵，我也是才开始做了半年而已哈，之前在做网站  
郝老师同学-贺诚 18:29:33   
你研究没有研究弹出广告的挣钱模式！  
y 18:30:29   
挣钱模式没有研究  
郝老师同学-贺诚 18:31:23   
现在游戏都是卖道具，如果弹出广告也有可能挣钱！  
y 18:31:55   
应该能挣钱  
郝老师同学-贺诚 18:32:35   
对呀！道具和弹出广告同时上比较好！  
y 18:35:10   
嗯  
郝老师同学-贺诚 18:36:24   
现在我看的盗版书网站就是靠弹出广告挣钱！  
郝老师同学-贺诚 18:36:32   
好象还不少  
y 18:37:38   
嗯