隐写术：在萌图里加密

今夏在美国发生的“俄罗斯间谍案”曾轰动一时——FBI 在新泽西州抓获了 10 名俄罗斯特工，并引起了两国外交震荡。FBI 是怎么抓获他们的呢？通过图片。

1、小图片大文章

俄国间谍不是挺牛的吗？怎么会因为一张图片被抓？难道 FBI 探员拍到了他们秘密集会的照片？错了，这些“证据”图片看起来寻常无比——像小猫和冰激凌这些日常之物，并且这些图片并不是藏在什么隐秘之处，而是公开在网上流通的。看似普通的图片其实隐藏了大量的机密。

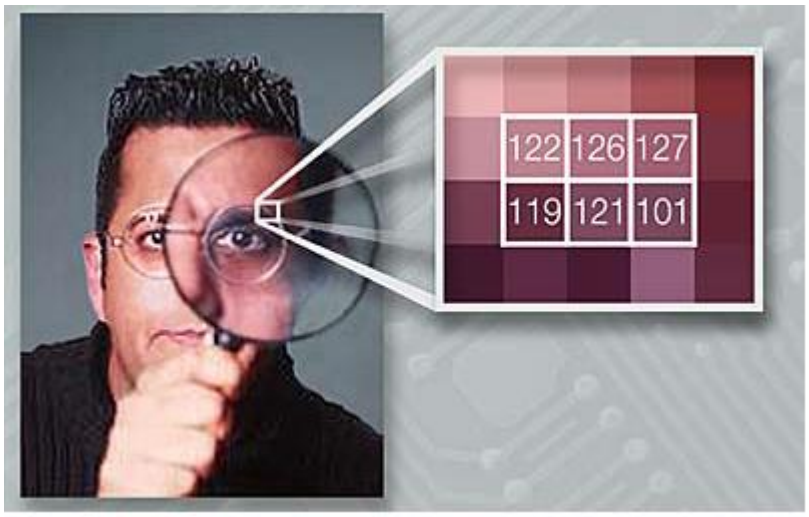
这些机密是怎么隐藏的？难道眼睛使劲盯着图片就能看出来了 就像 Magic Eye（www.magiceye.com）所说的那样？如下面的图片，你能看出隐藏的圣诞老人和雪橇吗？

从这样的 2D 图看出 3D 的图像的确需要一定的技巧，比如你得学会斗鸡眼才行——此处就不赘述观看方法了，有兴趣的同学可以到这儿

http://www.vision3d.com/看看。上图中隐藏的影像如下图。

不过，对于俄罗斯特工的图片，无论你怎么折腾自己的眼睛，也是看不出什么东西的。其实他们将讯息藏到了图片的像素信息中。

电脑上的图片是由一个个像素点组成的，每个像素点可以分解为三个子像素：红，绿和蓝。每个子像素都用一定的值表示。（LINK）只要通过对这些数值做轻微的改变，可以在其中藏匿二进制代码，这些代码可以通过特定软件解析出来。（如果你看了“如何鉴别伪造图像”这篇文章，那一定不会对下面的图陌生）



图中人物为英国著名科学作家 Simon Singh

FBI 根据这个原则，对俄罗斯特工的图片进行了解码，从中发现了这样的信息：

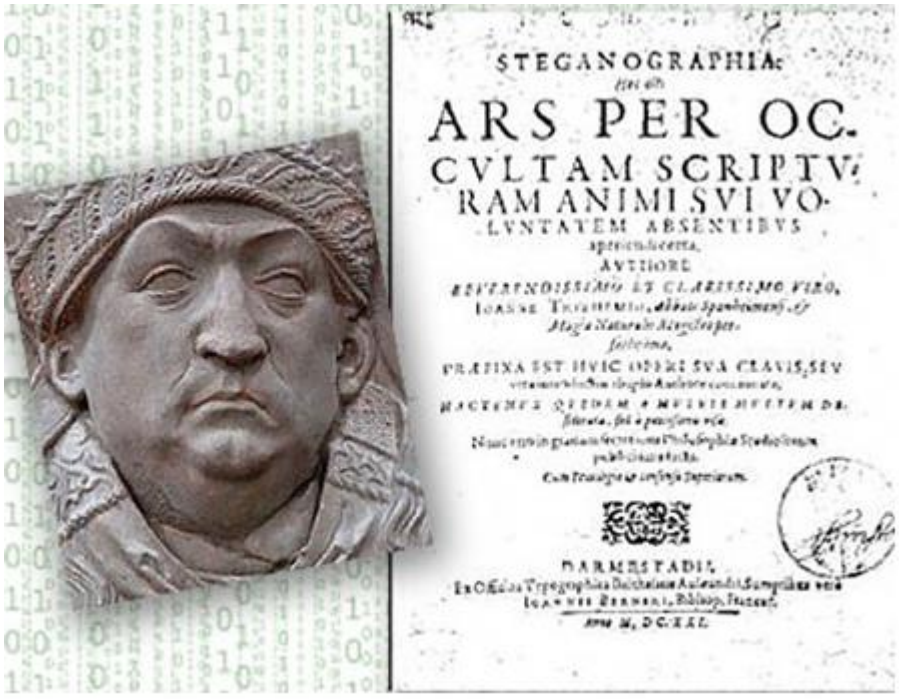
"C plans to conduct a flash meeting w/A to pass him $300K from our experienced field station rep (R). Half of it is for you. Another half is to be

passed to young colleague (known to you) in fall '09-winter '10. . . . "Place: North White Plains train station (Harlem Line), quiet and deserted on weekends. No surveillance cameras. . . . "A and R meet in lower part of staircase, in dead zone. R hands over and A gets pack w/money (A's BN [Barnes and Noble] bag stays in your hands, A hides pack w/money into his tote)."

总之 ,这些信息揭示了俄特工计划在纽约郊区一个火车站进行一个秘密集会以及各种细节。后来通过一系列的钓鱼执法，FBI 终于将他们抓捕归案。

2、隐写术和密码术

这种通过图片像素传递信息正是隐写术的一种。隐写术的英文是 Steganography，来源于 15 世纪一个德国修道士特里特米乌斯（Trithemius）写的一本讲述密码学和隐写术的著作《Steganographia》。该书书名源于希腊语，意为“隐秘书写”。



要注意，隐写术和一般的密码术（cryptography）是不同的。密码术只是对信息进行加密，再发送给接收者。对间谍来说，这个过程可得非常隐蔽——要是被发现在传递一串谁也看不懂的文字，十有八九会被 FBI 盯上。而隐写术则要安全一些。隐写的信息通常藏在图片，购物清单，诗文等事物中。普通人绝不会想到这些东西里其实有大文章。如果说密码术是个隐士，那隐写术看起来就像大街上一个毫不起眼的不会被注意的家伙——所谓小隐隐于野，中隐隐于市，大隐隐于朝也。

换句话说，密码术隐藏的是信息，而隐写术隐藏的则是传递信息的过程。这二者常常结伴出现——将信息加密后再附在图片等载体上发送出去，这样即使他人碰巧截获了图片，也得费一番功夫将信息破解出来。

3、源远流长

早在希腊时代，隐写术就有应用了。有一个名叫 Histaiaeus 的希腊人，他打算策划一场反抗波斯国王的叛乱，需要隐秘地传递信息。于是他将一名奴隶的头发剃光，在头皮上写下信息，等他的头发重新长出来时，就派他出去送信。对方只需再一次剃光奴隶的头发就可获取信息。除了奴隶的头皮，兔子的腹部也是一个传递信息的优良载体。这个方法在那会儿应该算是最先进的加密手段了，不过缺点就是即要找一个头发长得快的，还不能让他洗头。

公元前 480 年，波斯国王薛西斯一世亲率 30 万大军征战希腊。战前，一个被流放的希腊人 Demaratus 想法设法给斯巴达报信，他使用的是书记板。他去掉书记板上的蜡，将消息写在木板上，再用蜡覆盖。据说斯巴达国王的妻子占卜预言出蜡的背后有东西，于是他们将蜡刮掉，得知了波斯的阴谋，从而在温泉关布置了防御以抵抗波斯大军的入侵。温泉关之战是人类史上最残酷的战争之一，在电影《斯巴达 300 勇士》（The 300）里有详细描述。

在二战期间，间谍们常使用微缩照片传递信息。下图手表中的红色小圈被放大后，显示的是几行德国文字。

此外，衣物也可作为传递信息的载体，如电影《风声》最后，那件绣有莫斯密码的旗袍。一篇诗文里面也可藏匿不少信息，如我们常玩的文字游戏藏头诗；此外，也可通过改变某些字母的高度、在特定字上打十分微小的孔、用特殊墨水标记字母以及改变行间距等方法来传递信息。

再谈图片

再回到图片上来——你能想象下面这条鱼的图像中，居然隐藏了一个飞机场的地图吗？

这是计算机取证专家 Gary C. Kessler 做的图片隐写示例。他利用网上即可下载的图片隐写软件，将伯灵顿国际机场的图片藏进了鱼的图片中。接收者拿到图片后使用相似的软件就可提取出飞机场地图。

911 事件后，美国就有传言，基地组织利用色情图片传递秘密信息，不过从来没有被证实过。这次的俄罗斯间谍案是首次被证实利用图片隐写从事间谍活动的案件。

对于 FBI 而言，幸运的是俄罗斯特工使用的软件版本较低——1990 版的，以至于留下了一些蛛丝马迹。新版本的图片隐写软件在接收者拿到图片的信息后，可以抹去对图片曾有过的操作痕迹。这个故事也告诉我们，及时更新软件版本是有多么的重要。

目前图片隐写术软件的数量从 90 年代的少数几个增加到了现在的 250 个左右。利用图片来隐写信息再也不像黑客技术那样高深，而渐渐变得像使用 Microsoft Word 那样简单。