各位好，我是王国畅，今天给各位介绍的工作是MQRCODE，利用空间频率非线性的**安全**QRCode系统。

我首先从这三个问题介绍一些QRCode的背景知识。什么是QRCode，为什么它不安全，怎么可以使他安全。

QRCode就是我们平常说的二维码，全称是Quick Response Code，如字面意思是一种响应很快的编码，相机一扫就能扫出来，方便快捷。它如今已经在各类移动应用和线下支付中被广泛应用，例如QQ微信，和超市商店的扫码支付。

如果二维码不安全了，随之而来的就是个人信息会泄漏，支付也可能被劫持，造成经济损失。

而二维码恰恰安全性很低，有很多攻击方式都可以用较低成本来窃取你的二维码信息。这张图中描述的过程就是一个攻击流程，小明掏出了手机付款码给店家扫想要付款，这时旁边张三眼疾手快把他的二维码拍下来，拿去买了自己的东西。这样小明就帮张三买了他的东西，自己的钱还没付。

这篇论文的攻击模型就是攻击者会通过一些预先安排的摄像机或者在柜台附近蹲点企图拍到用户的二维码。但是攻击者有两个限制，第一是无法直接获取受害者的手机权限，或者在用户手机上预装木马程序。第二是攻击者没法获取像素级的高质量二维码，因为这需要非常专业大体积镜头的相机才能做到。

然后我们就要说一下QRCode为什么不安全。根本原因之一就在于它是一个过于容易获取的2维编码，可以从任何角度扫，只要你的相机够好，可以从很远的距离扫，同时也不是只有商家才能扫，随便一台智能机都能扫。

原因之二就是扫了以后还能随便解密，QRCode是这样的结构，这里的方块和线涵盖了QRCode用于解析的信息，而灰色部分则是加密的数据，数据通常是冗余的，所以只要相机采集到了这些方块，即使覆盖掉一部分灰色数据区域不影响二维码的解析。这样的设计就导致它极其容易被获取和解密，安全性很差。

从这两个原因出发就可以得到两个很直观的想法，二维码本来很容易获取，就想个法子让他不容易获取，比如只有从一定角度和一定距离扫二维码才能得到二维码；二维码本来很好解析，那就让它变得不好解析，比如将其中的数据用一个灰色的图层覆盖掉，这样相机自带的扫描就无法处理这个二维码，必须先解析这层灰色的图层才能得到原有的二维码，就像给二维码上了个锁。

这就是MQRCode的基本思路。它通过空间频率的非线性来对二维码进行加密，添加一个图层，并且用一个CFA模型来描述它的这种光学伪装。对应加密过程，它提供两种解密方法来还原被加密的二维码。

可以看出在加密时MQRCode提到了两个关键词，空间频率非线性和Color Filter Array，我们就围绕这两个是什么和怎么用来介绍加密过程。

空间频率是纹理在某个空间的周期性特征。对于一个2D空间下，把一个又黑到白渐变的纹理和consine函数进行复合，就可以得到最右侧的纹理。这个纹理就有它的空间频率。复合而成的纹理函数是m，原有的相位函数是phi，周期函数是p，也就是cosine函数。

显然多个纹理可以叠加并复合成一个新的非线性纹理，这种纹理叫莫尔条纹。我们假设之前的纹理是m1，周期函数cosine的频率为f1，在此基础上叠加一个频率为f2的纹理，记为m2。此时，图中仍然有原有的纹理，但由于叠加了一层纹理，原有的纹理不可见，对比度更强的是下方频率为f1-f2的纹理。这是由m1和m2叠加后产生的新纹理，由于他更符合人眼可响应的频率范围，所以更能被人眼所捕捉，原有的纹理就被伪装了。这里的公式表示莫尔条纹和两个叠加纹理的解析器之间的转化关系。如果由f1频率构成的纹理是加密后的图案，f2频率构成的纹理是用于解密的图案，而f1-f2频率构成的莫尔条纹是我们希望获得的图案，那么这时，我们就可以得到一个面向人眼的加密解密系统。其中原图是f1-f2的莫尔条纹，加密后的纹理为f1，只有通过f1和f2的叠加才能得到所需莫尔条纹。

空间频率可以干扰人眼，从而达到对图案进行加密的效果，它同样可以干扰相机，从而对二维码进行加密。

这就要提到相机拍照片的原理。相机想要拍彩色照片不可缺少的就是Color Filter Array 也就是我们之前提到的CFA。CFA实际就是色彩滤镜。就像这张图上插入式滤镜就是相机上常用的滤镜，也就是CFA。每个滤镜实际是由一组按序排列的红绿蓝滤镜组成的，每个小的就是一个Color Filter，他们共同构成了Color Filter Array。比如这个图里最左边就是一个滤镜的微观结构，光打在滤镜上，分别透过红绿蓝滤镜形成三个纹理，结合CFA结构对红色纹理的灰度进行计算就可以得到这种颜色的红光强度，同理可以得知其绿光和蓝光强度，从而复合成RGB颜色，也就让相机看到了色彩。目前最主流的滤镜是Bayer 滤镜，本文的工作也是基于这种滤镜排列来做的。

相机可以被莫尔条纹干扰的原理就在于两点，第一相机和人眼一样，只能捕捉特定频率的光，超出频率范围的光线就不可见，第二相机本身拍到的图形实际是由红色滤镜阵列，蓝色滤镜阵列和绿色滤镜阵列复合而成的结果。三个滤镜得到的纹理相互叠加，根据我们之前的公式，当频率为f1-f2或者f1+f2的光也进入了相机可以捕捉的范围，就会在相机成像里出现莫尔条纹，遮挡住原本图案。具体来讲就是我们拍电脑屏幕的时候相机上出现的这些彩色的纹理。

那么我们可以利用这个原理，假设有一个加密后的二维码，通过相机去扫描它，由于相机滤镜的纹理和加密后的二维码叠加，形成了彩色的莫尔条纹，如果我们调节相机滤镜的纹理，使得这些彩色的莫尔条纹构成了原本的二维码，就可以对加密的二维码进行解密。同样的根据公式，我们在已知相机滤镜纹理和原本二维码的情况下，就可以计算出加密的纹理，也就是加密的二维码，这样就完成了加密的过程。由此我们就可以得到一套完整的工作流。首先生成一个标准的QRcode，我们知道在解密时相机滤镜纹理和加密后的纹理叠加可以形成原本的二维码，在已知相机滤镜纹理和QRcode的情况下我们就可以计算出加密后的纹理，也就是加密后的二维码。用户把加密的二维码展示在手机上，相机就去扫描这个二维码，相机滤镜形成的纹理和加密后的纹理叠加，就出现了由莫尔条纹形成的原二维码。

工作流很简单也很直观，但是为了达到理想的效果，在加密和解密过程中都有一些挑战。接下来我就介绍一下加密和解密的做法以及其中做了哪些特殊的处理。

首先是加密过程，我们目标是得到一个加密过的纹理menc，我们把原本的标准QRcode记为纹理mdec，也就是解密后的纹理，再把用于相机滤镜的纹理记为mcfa。我们希望相机的滤镜纹理和加密后的纹理叠加就可以得到原本的二维码。于是mdec=mcfa叠加menc。

我们的目的是相机滤镜纹理和加密后的纹理叠加后能恰好形成解密的二维码。所以叠加后产生的莫尔条纹必须是两种颜色。相机滤镜包含红绿蓝三种颜色，这里我们只在绿色上进行纹理处理，不对红色和蓝色进行处理。这样原有二维码在展示时，原本的白色部分会编成红蓝复合的紫色，黑色部分会变为绿色滤镜的绿色。选取绿色滤镜是因为在Bayer滤镜的排列中单位面积里绿色滤镜处于对角线位置且占据面积的1/2，确定颜色时受到的干扰相对小，另外绿色和紫色也是对比度较强的两种颜色，有利于二维码解析。我们就可以对相机滤镜的纹理给出这样的解析式。根据之前在空间频率部分呢介绍的公式推导可得加密后的纹理解析式。这样我们就得到了加密后的纹理。

这时回想一下我们的初衷，我们希望被加密的图案只有在一定的距离范围内才能被拍到，使得二维码更难被获取。这里mqrcode给出的控制手段是控制相机滤镜纹理的频率。我们知道频率越大纹理条纹越细，反之条纹越粗，在相机不变焦的情况下近大远小，最终只有在指定距离附近的相机扫描二维码时才能得到纹理合适的二维码。这里我个人觉得这个解决办法有一些争议，后面会具体讲，我这里先抛出来：在知道f的情况下，只要我有足够好的相机，保证我在超远距离也能拍到清晰的二维码图片，或者我离的足够近，什么频率的图片我都可以拍清楚，我完全可以不在规定距离上拍到加密的二维码然后进行解析，这样距离控制是不是就达不到效果了。

我们回到加密过程，在加密的过程中还有一个问题就是在原本二维码黑白分界的位置，即便在加密过后还是可能出现人眼可分辨的线条，为了通过这些线条还原出原本的二维码，我们可以通过添加一些噪声也就是黑点，或者一些虚线来遮盖这些线条，从而达到模糊边界的效果。

加密完成后我们还需要解密。在解密的时候我们理想的情况是这个样子，左上角的方格代表加密后的纹理，它透过相机的滤镜得到了红绿蓝的pattern，通过我们之前设置好的相机纹理来处理这些pattern，就可以将这一格颜色处理为绿色，从而得到原有的二维码图案。

但是可以看到实际相机拍出来的二维码跟理想状态的二维码相差甚远，最右的图片为实际拍到的二维码，在a区域十分模糊，在b1和b2区域颜色都错了。这里论文里没有提它是怎么解决a区域这种模糊问题的，我猜测是因为二维码本身有数据冗余所以部分模糊不影响整体的解析。论文里主要描述并解决的事b1和b2的颜色错误的问题，也就是反相问题，相位的相。

这个问题产生的过程可以通过这四步讲清楚，本来我们期望得到的是一个整整齐齐的黑白格，但是它被拉伸了，可是相机的红绿蓝滤镜排列是整齐的，原本一格红色滤镜和一格白色纹理叠加，就认为这一格是红色，但是实际对应的不是一格红色纹理，是一半红一半黑，那么红色滤镜得到的颜色就不是原本的红色而是暗红色，这样最终这一片区域复合出的颜色就不是均匀的绿色或紫色，而是错误的颜色。

这个问题有两种解决方案，分别对应两种解密方法。

第一个解决方案是补桢。拍一张处理出来的二维码没法用就拍多张，把他们结合起来就能还原出原本的二维码。显然这种解密方式补拍越多张图片，帧数越高，解密效果就越好，帧数过低则可能解密失败。

第二个解决方案论文里命名为快速解密。他的方法是基于这样一个观察。对于一个白色的图片，即使出现反相问题，我们也可以得到一个莫尔纹理。对于对角线上是黑色的图片，在同样出现反相问题的场景下，白色的部分和纯白图片得到的莫尔纹理相同，黑色的部分则明显有区别。也就是说，在同时得到一个b图和d图的情况下，我们就可以分辨d图的原有图案是黑色还是白色。b图和d图一样的部分就是白色，不一样的就是黑色。这样只要我们有一张纯白的图片作为原图片，将它加密以后作为参考图片，在反相的时候就可以通过把参考图片出现的莫尔纹理和实际的二维码图片对比，从而判断原本的颜色。

最后我们来讲一下这个工具的性能评估。

首先对它控制二维码只能在一定角度和距离被拍摄的能力。a，c表示两种解密方法的解密成功率和偏移距离的关系。可以看到离指定距离越远，成功率越低。同样我们从bd图可以看出角度偏移越大成功率越低。而下面的e，f图则显示普通二维码几乎不受距离和角度影响。

然后对补桢解密方法的帧数进行评估，可以看出与我们的猜测一致，帧数越多，成功率越高。

在加密时他们通过加入噪声来控制解密成功率，可以看出噪声的确可以有效降低成功率，而10%的噪声可以起到比较合适的效果，既不会太容易被解密，也不会拍了很多帧也没有办法解密。

在加密时他们还通过f来控制可以解密的距离，我们也可以看出在评估的时候f的确可以控制只有在一定距离范围内才能解密成功。

最后的评估是外界环境，光线和震动对解密的影响，可以看出对于多帧解密而言光线和震动都不会对最终解密成功率有太大影响，而快速解密则对光线和震动更敏感。

报告的最后我们对这份工作的局限做一个讨论，这里先回顾我之前提到的疑问。即使通过这样的伪装，只要我知道了相机滤镜纹理的生成方式mcfa，再获取一张质量足够高的二维码照片，是不是就可以对二维码进行解密了。为了获取质量足够高的照片，我可以很近距离拍二维码，或者找一台很好的相机远远的拍。作者对这两种获取方式的解释是，以他设置的频率从1/4到1，最近距离也是1m左右，一般不假设人在这个距离上还会被偷拍。另一个是再好的相机在焦距调整的时候也会让图片质量下降，从而难以获得可解析的图片。这是作者的解释。

不过，他的实验里是不涉及变焦的，也就是如果指定距离是0.5m，处于1.2m的相机不能通过变焦来获取更大更清晰的二维码，同时我注意到他在加密时mqrcode用了频率f和噪声来控制用户只能在一定距离进行解密。但是在评估时并没有对快速解密方式做相关的评估。我的理解是FAST解密方式是通过对比的方式还原原有的二维码，所以处理反相问题能力其实比多帧方法更强，只要在正确的方向上，即使不在指定距离内，通过伸缩焦距拍到一张反相严重的图片，也能还原出可解析的二维码。也就是说频率f可能没法限制用户必须在指定距离上才能解密，限制用户解密的距离和角度的依然是相机拍照的能力。不知道我的理解是否正确，希望有明白的老师同学讲解一下这个问题。我的报告到这里，谢谢各位。