doi: 10.3969/j.issn.1006-1576.2012.11.008

基于视觉加密的军事物联网应用

杜轶焜，严承华，冯剑川，廖巍
（海军工程大学电子工程学院，武汉 430033）

摘要：针对现有二维码技术保密性较弱的问题，提出一种应用于军事物联网中的图像加密技术。采用视觉加密手段，将传统的 QR 码图像生成 2 幅像素随机分布的共享图像，通过 2 幅共享图像的矩阵值的或运算，利用图像像素矩阵中的汉明重量 w 判断 QR 码原始图形中的黑白值，生成原 QR 码图像，达到 QR 码在授权设备中被还原并读取的目的。分析结果证明：该方法能克服传统 QR 码扫描技术的安全漏洞，加密后的 QR 码图像恢复效果好，并且保密性较强，在军事物联网的应用中有着广阔的前景。

关键词：军事物联网；二维码；视觉密码；QR 码；随机加密规则
中图分类号：TJ02 **文献标志码：**A

Application of Military Internet of Things Based on Visual Cryptography

Du Yikun, Yan Chenghua, Feng Jianchuan, Liao Wei
(*School of Electronic Engineering*, *Naval University of Engineering*, *Wuhan* 430033, *China*)

Abstract: The 2 dimension code is hard to keep secret, introduced an image cryptography technology for military internet of things. Adopt visual cryptography method, and transmit traditional QR code image to create 2 pixels random distribution share images. Through exclusive disjunction of 2 share image matrix value, use Hamming weight w of image pixels matrix to judge QR code primitive image judge black and white value, create original QR code image, then the QR code can be reverted and read in authorization equipment. The analysis results shows that the method can overcomes the security shortages of traditional QR code scanning technology, the cryptography QR code image can be resumed well with better security in military internet of things.

Key words: military internet of things; two dimension code; visual cryptography; QR code; random encryption rules

0 引言

随着国务院发布物联网“十二五”规划，军事物联网的发展再次受到关注。二维码业务作为物联网感知层应用中的技术手段之一，在物联网发展应用中起着不可替代的作用，一定程度上优于射频识别(radio frequency IDentification，RFID)技术，实现了低碳环保、节约的目的，目前网上支付、身份识别、购物等功能均在二维码应用中得以实现[1]。由于构成二维码的QR Code(quick response code)编码技术的公开性，传统的 QR 码直接公开存在于可接触的场合中，存在非法者试图篡改、修改信息的安全漏洞[2]，在军事装备信息存储、交互等保密性较强的军事物联网业务中显得及其脆弱。

视觉密码由 Naor 和 Shamir[3]提出，将(k,n)门限方案扩展到了二值图像秘密分享的领域。Blundo[4]等人从理论上得出了(2,n) VCS 相对差的极大值，以及此时像素扩展度所满足的条件。通常视觉密码对图像进行加密的方法有：基于像素不扩展、基于存取结构等方法，但上述方法在对 QR 码扫描应用上效果不够好。笔者基于视觉密码的图像算法，通过对 QR 码图像进行视觉上的加密并共享图片，而不单纯直接依靠设备对 QR 码进行扫描，再将共享图像通过重叠研究具体的汉明重量值，最后生成原 QR 码图像，达到 QR 码在授权设备中被还原并读取的目的。

1 相关工作

通常二维码是由特定的几何图形按制定的规则水平分布在黑白相间的图形中，并用来记录数据符号信息。在汇编代码中，巧妙地利用计算机内部逻辑的‘0’、‘1’比特流的概念，将与二进制相关的图像特征来表示二维码中的信息，并通过光电扫描等设备自动识读。目前国际 150 标准已经有多种条形码，其中应用最广泛的有 PDF417、DateMatrix、QR 码等[5]。表 1 为常用二维码的性能比较和说明。

收稿日期：2012-06-02；**修回日期：**2012-07-03
基金项目：全军军事学研究生课题(2011JY002-435)；中国博士后基金特别项目(201003757)；大学自然科学基金项目(HGDYDJJ11008)
作者简介：杜轶焜(1988—)，男，四川人，羌族，在读硕士，从事网络对抗与安全研究。

表 1 二维条码性能比较

码制	编码形式	最大数据容量
PDF417	堆迭式	1 108 B
CM	矩阵式	32 768 B
GM	矩阵式	1 143 B
汉信码	矩阵式	7 829 个数字或 2 174 个汉字
QR	矩阵式	2 953 B
Data Matrix	矩阵式	2 000 B
Max icode	矩阵式	93 个字符或 138 个数字

QR Code 是日本 Denso 公司在 1994 年 9 月研制的一种矩阵二维条码，除了具有一维条码及其他二维条码所具有的信息容量大、可靠性高等特点以外，还具有超高速识度、全方位识读、纠错能力强、能有效表示汉字等特点，在我国具有广泛的应用前景；因此笔者对 QR 码作为二维码的研究对象具有深远的意义。图 1 为一个常见的 QR 二维码[6]。

图 1 国内最为常见的二维 QR 码

QR 码作为矩阵式二维条码，优点在于其输入输出的数据流均可用“0”、“1”分别表示图像中的白、黑像素，由于其灰度值为较低，所以可用设备易扫描 QR 码中的图形值。在物联网的应用管理中，二维码的图形特征必须符合一定的机密性和完整性，但由于 QR 码技术已公开多年，必须寻找出一种不让 QR 原码图像直接暴露在可视的场合里，尤其运用于机密性较强的物流管理、军事管理、政府保密办公等业务中显得极其重要。

笔者提出利用视觉加密手段将传统的 QR 码图像生成 2 幅像素随机分布的共享图像，一幅图像作为二维码扫描应用公布于扫描所需位置，扫描设备根据 QR 二维码图形特征值提取所对应的随机矩阵，根据视觉密码算法得出另一幅共享图像。通过 2 幅共享图像的矩阵值的或运算，得出秘密图像，利用图像像素矩阵中的汉明重量 w 判断 QR 码原始图形中的黑白值。

2 QR 码的视觉密码研究

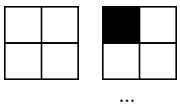
2.1 基本概念

笔者采用的视觉密码方案是基于(2,2)的门限方案实现的，改变了图像像素分布的规则，利用随机加密规则将原 QR 码图像的像素进行分解无序优化。

定义 1 通过对 QR 码图形特征值的研究得出能用信息编码将定义 QR 码中黑像素(白像素)的值为“1”(“0”)，并产生与 QR 码的图像 M(像素为 $m\times n$)相对应的 $i\times j$ 的矩阵 $\boldsymbol{M}$，M_{ij} 表示 QR 码图像中第 i 行、第 j 列所对应的像素编码值[7]。

定义 2 将子像素矩阵 T_{ij} 的汉明重量定义为 w，通过对扫描设备的识别处理能力的研究，定义在共享图像 $\boldsymbol{R}_{ij}$、$\boldsymbol{Y}_{ij}$ 子像素的模块矩阵中，白色子像素满足：$0\leqslant w\leqslant 3$ 的模块矩阵；黑色子像素满足：$w=4$ 的模块矩阵。$\boldsymbol{R}_{ij}$、$\boldsymbol{Y}_{ij}$ 经过或运算得到矩阵 $\boldsymbol{T}_{ij}$，由表 2 关于 $\boldsymbol{M}$ 图中黑、白色子像素扩展图可知，满足白像素的矩阵共有 15 个，满足黑像素的矩阵有 1 个。

表 2 关于 $\boldsymbol{M}$ 图中黑、白色子像素扩展图与对应的矩阵关系

QR 码中的子像素	子像素扩展图 T	对应的矩阵 $\boldsymbol{T}$
白像素		$\begin{bmatrix}0&0\\0&0\end{bmatrix}$ $\begin{bmatrix}1&0\\0&0\end{bmatrix}$ … $\begin{bmatrix}1&0\\0&1\end{bmatrix}$ $\begin{bmatrix}1&1\\1&0\end{bmatrix}$
黑像素		$\begin{bmatrix}1&1\\1&1\end{bmatrix}$

由表 2 可知，可将每个模块矩阵按照 4 位二进制表示 4 个子像素，比如 $\begin{bmatrix}1&0\\0&0\end{bmatrix}$ 表示为 0001，根据定义 2 中对 $\boldsymbol{R}_{ij}$，$\boldsymbol{Y}_{ij}$ 模块重叠的或运算，可将 0001 分解为 0001|0001，0001|0000，0000|0001 三种共享组合方案，关于随机加密矩阵的定义如下。

定义 3 记随机加密矩阵 $\boldsymbol{S}(m\times n)$中每个随机值 s_{ij} 对应的一个随机加密规则 J_{ij}，记以每个随机加密规则 J_{ij} 所组成的 2×2 矩阵[6]为

$$\boldsymbol{K}_{ij}=\left[s_{ij}\right]_{2\times 2} \tag{1}$$

定义 4 将随机加密规则矩阵 $\boldsymbol{S}$ 中每个值 s_{ij} 扩展为 2×2 的子矩阵 $\boldsymbol{K}_{ij}$ 模块，目的是对子像素 $M_{i,j}$ 进行像素扩展处理，生成 $2m\times 2n$ 的扩展矩阵 $\boldsymbol{T}$，并依据指定的随机加密规则产生 2 个共享的子像素 $\boldsymbol{R}_{ij}$、$\boldsymbol{Y}_{ij}$，定义子像素矩阵[8]

$$\boldsymbol{R}_{ij}=\begin{bmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix},\ \boldsymbol{Y}_{ij}=\begin{bmatrix}a_{11}'&a_{12}'\\a_{21}'&a_{22}'\end{bmatrix}。 \tag{2}$$

2.2　方案设计

在制作加密 QR 码过程中，先利用扫描设备对待加密的 QR 码进行扫描，将扫描出的数据编码流转化为矩阵 $\boldsymbol{M}(i\times j)$，在视觉加密程序中依据对原始值（“0”或“1”）判断，对相应的 M_{ij} 进行赋值，在设计中，依据具体的 M_{ij} 对产生随机加密矩阵 $\boldsymbol{S}$，其中 s_{ij} 随机值与原 QR 码图像 $M_{i,j}$、黑白子像素扩展 $T_{i,j}$、随机加密规则 J_{ij}、和 $\boldsymbol{R}_{ij}$、$\boldsymbol{Y}_{ij}$ 的对应关系如表 3，为了便于计算研究，将矩阵定义为 4 位二进制数值。

表 3　s_{ij} 与 $\boldsymbol{M}$、J_{ij} 和 $\boldsymbol{R}_{ij}$、$\boldsymbol{Y}_{ij}$ 对应关系

$M_{i,j}$	$T_{i,j}$	J_{ij}	$\boldsymbol{R}_{ij}$、$\boldsymbol{Y}_{ij}$ 的组合关系
0	0000	0000	0000 0001|0000，0000|0001，0001|0001 … 0000|1101, 0001|1100…1101|1100 共有 27 种组合
	0001	0001	
	…	…	
	1101	1101	
1	1111	1111	0000|1111, 0011|1101，0011|1101…1111|0000 共有 81 种组合

笔者依据 QR 码扫描设备对原始 QR 码扫描，对编码进行信息编码和生成矩阵 $\boldsymbol{M}$，通过遍历判断矩阵中的每个值，定义某个值具体位置为 $i\times j$，具体流程如图 2。

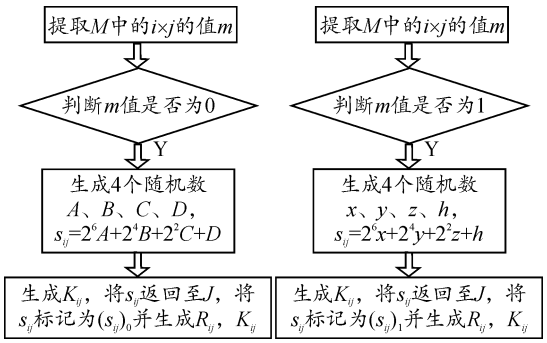


图 2　生成随机数 s_{ij} 的具体流程

由表 3 中的对应关系可知，原码图像中白像素对应于视觉密码共享的扩展像素共有 175 种组合，原码图像中黑像素对应于视觉密码共享的扩展像素共有 81 种组合，在 R、Y 2 个共享图中，扩展像素均是随机扩展分布的，与 QR 码比较达到了视觉上的保密效果。

依据流程图中第 3 步生成 4 个随机数的关系，为了满足表 3 中黑白像素的关系，黑白像素所对应的 4 个随机值分别必须满足以下的条件：

1) $\{A,B,C,D\}\in\{00,01,10,11\}$，且必须满足 4 个数中至少有一个值为 00；

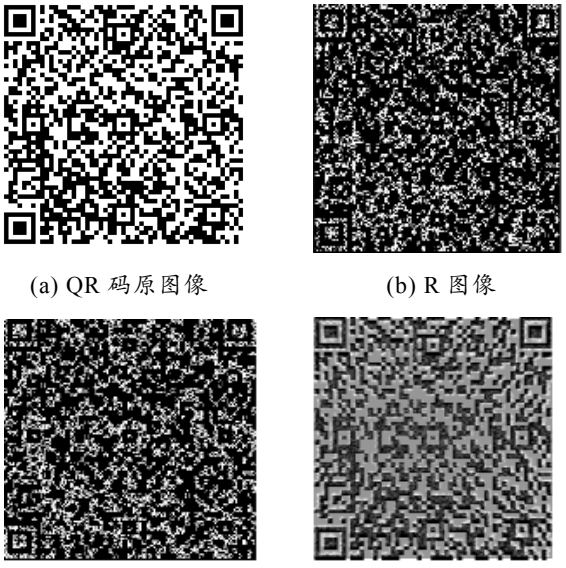
2) $\{x,y,z,h\}\in\{01,10,11\}$。

2.3　方案实验和分析

笔者生成一个包含信息的 QR 码，并通过实验生成共享图像 R、Y，如图 3 所示，概率视觉密码共享方案不能保证原始 QR 码中的每个白像素（黑像素），只能通过一块图像区域来检测黑白差异，提出的方案是一个基于随机概率的方案。

图 3　生成 QR 码原图像

本方案的优势在于对视觉对比度要求不高，依据程序试验中 R、Y 图像中像素重叠后所对应的汉明重量生成原 QR 码，并能解码读出信息，在应用过程中，只需要在设备检测后台中，提取 R 图像中的随机矩阵值，就能在程序中生成 Y 图像，并对 R、Y 做“或”运算，依据汉明重量值 w 的定义判断 QR 码中所对应的像素，从而提取 QR 码中的原始信息[9]，如图 4 所示。



(a) QR 码原图像　(b) R 图像

(c) Y 图像　(d) R、Y 重叠图像

图 4　各个图像的像素对比

（下转第 37 页）