网络出版时间：2014-04-24 04:01
网络出版地址：http://www.cnki.net/kcms/detail/10.1108.TP.20140424.0414.249.html

基于数字水印技术的 QR 二维码信息保护

文/张晨威　卢濛荻　周彦晖

摘要

二维条码技术和数字水印技术都是防伪领域中的重要技术和研究热点。由于二维码的编码过程是通过公开的数据信息转换方法进行，因此从严格意义上说二维码技术并不是一种可靠的保密技术。本文设计并实现了一整套基于 QR 二维码的信息保护方法。

本文讨论的 QR 二维码信息保护的方法，主要包含生成水印的加密算法和解密水印的提取和解密算法两部分。基于以上思路，采用数字水印技术实现在公开信息中加入秘密的隐私信息，从而实现隐私信息的隐藏保护。本文主要讨论核心信息的混沌序列置乱和置乱图像的嵌入两个步骤。核心信息的混沌序列置乱采用 Logistic 映射的混沌系统对核心信息进行置乱，置乱图像的嵌入采用二维离散余弦变换将置乱后的核心内容图像嵌入到载体图像中。

经过实验验证，该套基于 QR 二维码的信息保护方法能有效的保护储存在二维码中的信息，有效地解决了二维码信息保密性差的问题。

【关键词】QR 二维码　信息保护　混沌序列置乱　离散余弦变换

1 引言

随着信息技术的不断发展，人们对信息载体的容量和便携性有越来越大的要求，对于信息保密和信息安全也有越来越高的要求。QR 二维码和数字水印都是近年来在信息传播和防伪领域中热门的技术，也是研究的热点。但是由于 QR 码的编码过程是通过公开的数据信息转换方法进行，因此 QR 二维码公开传播毫无保密性。数字水印技术是信息隐藏技术的一种，多应用于数字作品的版权保护方面。其基本思想是在数字产品中嵌入加密过的数字信号，在不影响正常读取的情况下将作者、版权信息隐藏在数字产品中。本文中将数字水印技术应用于图像中，将隐私信息嵌入图像。目前对于有特殊防伪要求和较高安全保护的领域，将 QR 二维码技术和数字水印技术结合将成为信息保护的新思路。

本文设计了一个通用的二维码信息保护系统，利用数字水印技术把储存在 QR 二维码中的隐私信息作为数字水印隐藏到载体图像中，成为原数据不可分离的一部分，有效的解决了二维码信息保密性差的问题。

2 系统设计

本系统总共分为两大模块：生成 QR 二维码、生成水印加密图像、解密水印加密图像。生成水印加密图像、解密水印加密图像是两个最核心的模块。

在生成水印加密图像阶段，首先将生成的二维码进行预处理。由于 ISO 标准下的二维码中存在大量关于版本、标示、数据类型等信息，为了保留最核心的信息，只需将二维码核心部分（数据和纠错部分）提取出来，得到核心内容图像。接着，采用混沌序列置乱将核心内容图像进行置乱，使得到的置乱图像满足应用数字水印算法的条件。最后，将置乱图像通过离散余弦变换嵌入到目标图像中完成信息的隐藏。

在解密水印加密图像阶段，首先提取出置乱图像。接着，对置乱图像进行反置乱还原出核心内容图像。最后在核心内容图像上加上相应的格式信息读取出原二维码中的原始信息。

本文主要讨论核心信息的混沌序列置乱和置乱图像的嵌入。

3 核心信息的混沌序列置乱

将核心信息进行置乱的目的是为了将分布不规则的核心内容图像通过矩阵变换的形式进行图像置乱，得到一副杂乱无章的图像。该图像无特殊形状无纹理，因此将这样一副图像嵌入另一幅普通图像中时，被嵌入图像的色彩、形状和纹理均不会产生较大的变化。因此合理的二维码置乱算法不仅分散度较好并且时间复杂度较低。

常见的置乱方法有混沌序列置乱、Hash 置乱、幻方置乱、Arnold 置乱、仿射置乱等。

在混沌系统中，一类非常简单却被广泛研究的就是 Logistic 映射，其定义为：

$$x_{n+1}=\mu x_n(1-x_n) \qquad (3\text{-}1)$$

其中，$0<\mu\le 4$ 称为分支系数，$x_n\in(0,1)$,n=0,1,2,3,…。混沌动力系统的研究工作指出，当分支参数 $3.699456\cdots\le\mu\le 4$ 时，则 Logistic 映射工作于混沌态。由于 Logistic 映射的输入和输出都分布在 (0,1) 上，因此对于一个二维灰度图像 $I_{M\times N}$，利用 Logistic 映射产生实数混沌序列 $\{x_n,n=0,1,2,3,\cdots\}$。将序列 $\{x_n\}$ 升序排列后，得到序列 $\{y_n\}$，并用 num 数组记录 y_n 的值在对应 x_n 上的位置。将序列 $\{y_n\}$ 中的每个元素值依次填入空矩阵 $P_{M\times N}$ 中，得到一个信息量相同的矩阵。根据生成的混沌序列在区间 (0, 1) 具有遍历性可知 $P_{M\times N}$ 必能被填满 $\{x_n\}$，且由于 的混沌特性，填满后的 $P_{M\times N}$ 同样具有混沌特性。

从图像直观的表现上来说即是置乱后的图像杂乱无章像。该图像无特殊形状无纹理，可以作为水印嵌入载体图像。

4 置乱图像的嵌入

将 QR 二维码的核心信息作为水印嵌入到载体图像中利用了二维码储容量大、可以表示汉字图像等复杂信息、无需数据库的支持这些优点。

目前的常见的数字水印算法可以分为空域数字水印算法和频域数字水印算法。空域数字水印算法通过直接改变载体图像某些像素值将水印嵌入，采用这种方法运算简单快捷但鲁棒性较差。频域数字水印算法不直接修改顶点坐标，鲁棒性较好。本文将采用基于二维离散余弦变换的频域数字水印算法，从被嵌图像中选取坐标，进行频域变换，将置乱加密后的信息均匀嵌入到它们的变换系数中，使得加密之后的信息均匀隐藏在普通图像中。

在本文中，先将载体图像 $Q_{M\times N}$ 分成 8×9 互不覆盖的子块，记为 Q(x,y),i=1,2,…,(M×M)/64，置乱得到的水印加密图像 $P_{M\times N}$ 则分为大小为 $(N\times\frac{8}{M})\times(N\times\frac{8}{M})$ 的子块，分别记为 $P_i(j,k)$,i=1,2,…, (M×M)/64，$1\le j\le N$，$1\le k\le N$，M 满足 $M=2^N$。然后对载体图像的每一个子块 $Q_i(x,y)$ 做二维 DCT 变换，变换公式为：

$$O_i'(p,q)=\frac{2}{M}C(p)C(q)\sum_{x=0}^{M-1}\sum_{y=0}^{M-1}O_i(x,y)$$

$$\cos\left(\frac{\pi p(2x+1)}{2M}\right)\cos\left(\frac{\pi q(2y+1)}{2M}\right) \qquad (4\text{-}1)$$

对于载体图像的每一个子块 Q_i，在每个子块的 DCT 系数的低频区域选中一个像素点，把选中的像素点的 DCT 系数记为 $O_i'(p,q)$，利用 $O_i(p,q)=O_i'(p,q)+\alpha P(j,k)$ 嵌入水印，得到嵌入水印的 DCT 系数 $O_i(p,q)$，其中 α 是修正系数，用来确定水印的嵌入比例。对 $O_i(p,q)$ 分块进行反变换得到包含水印的水印加密图 $O''_{M\times M}$。

5 实验结果与分析

实验采用 256*256 的二维码图片储存信息，用 256*256 灰度照片作为载体图像。本文将“西南大学计算机与信息科学学院”的文本信息生成二维码进行实验。经过识别可从二维码图像中提取出格式信息和核心内容信息，如图所示：

图 5-1：二维码

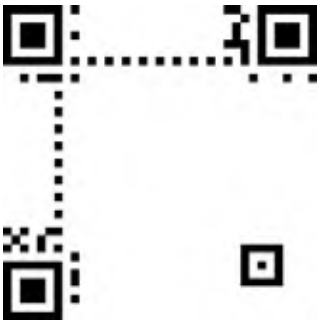

图 5-2：格式信息

图 5-3：核心内容信息

图 5-4：载体图像

在对核心内容信息进行置乱的过程中，主要用两个指标来衡量置乱效果的好坏。

(1) MSE(Mean Square Error)

均方差可以直接反映出评估对象的改变，通过均方差可以分析被评估对象的各种变化特征。对载体图像和嵌入了水印的载体图像比较均方差可以给出置乱变换质量的客观指标。

（2）峰值信噪比 PSNR(Peak Signal-to-Noise Ratio)

针对普通的灰度图像在具体的实际应用中，一般采用峰值信噪比作为衡量尺度，

通过比较两幅图像计算得到的 PSNR，就可以得出一个图像质量的尺度。

利用上述指标对各种置乱方法进行对比试验，结合算法本身的特性和实验结果分析可以发现，Hash 置乱虽然效果好，但是运算时间长。幻方置乱虽然运算时间短，但置乱效果不好。要得到较好的置乱效果比喻要经过多次幻方置乱。Arnold 置乱算法简单易于实现，但也需要多次变换才能达到最好效果。混沌序列置乱虽然在初次图像置乱之前要生成一个图像长乘宽大小的混沌序列，但是对于之后的所有置乱这个混沌序列都不需要再次产生，因此在总体上效率较高且置乱效果较好。所以本文中采用了基于混沌序列的置乱方法。

表 5- 5 置乱方式对比

利用混沌序列进行置乱得到的效果如下：

表 5-5 置乱方式对比

Table 5-5 Comparison of Scrambling

置乱方式	运算时间 (s)	MSE	PSNR(db)
幻方置乱	0.086515	0.1444	56.5364
Arnold 置乱	0.084071	0.3369	52.8561
混沌序列置乱	0.035029	0.3368	52.8570

图 5-6：置乱前

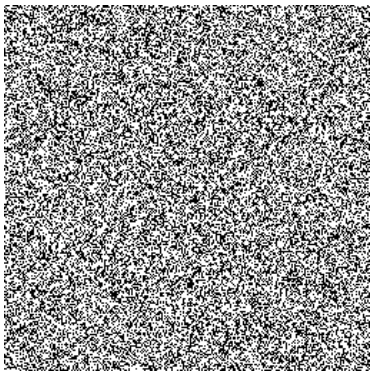

图 5-7：置乱后

将置乱后的核心内容图像利用离散余弦变换嵌入载体图像，与原图像相比，在肉眼上几乎发现不出区别，实验结果如图：

图 5-8：嵌入了水印的载体图像

从载体图像可还原出原二维码，最终还可从还原出的二维码中正确提取出“西南大学计算机与信息科学学院”的信息。

6 总结

实验结果表明，本文所述中应用于 QR 二维码的信息保护技术具有较好的鲁棒性。混沌序列置乱的效果能很好的满足作为水印嵌入载体图像的需要；经过混沌序列置乱和离散余弦变换，嵌入载体图像的信息可以被准确的还原。该方法有效的解决了二维码信息保密性差的问题。

参考文献

[1]Cox, I. J., Kilian, J., & Leighton, T. (1996). A Secure Robust Watermark for Multimedia. Proc. of Workshop on Information Hiding., pp. 185-206.

[2] ISO/IEC. (2006). Information technology-automatic identification and data capture techniques - QR code 2005 bar code symbology specification. ISO.

[3] 范延军，孙燮华，闫晓东，郑林涛．一种基于混合混沌序列的图像置乱加密算法[J]．中国图像图形学报，2006(06).

[4] 侯整风、王国明．基于离散余弦变换的数字水印算法[J]．计算机工程与设计，2008(11).

[5] 黄西娟，& 王冰．一种 DCT 变换域的鲁棒数字水印[J]．计算机工程，2011(10).

[6] 宋海明．基于混沌序列的图像置乱加密算法[J]．荆楚理工学院学报，2009(11).

作者单位

西南大学计算机与信息科学学院　重庆市 400715