基于演化加密的二维码生成技术及在农产品质量安全溯源系统中的应用

钟小军[1]，赖志杰[2]，陈 琰[1]，钱键新[1]，洪晓聪[1]，李彩仪[1]
（1.广东村村通科技有限公司，广东 广州 510045；2.广东省科技信息中心，广东 广州 510045）

摘 要：二维码技术作为一种电子标签技术，是以计算机和光电技术发展为基础的一项综合性科学技术，是信息采集、输入的重要方法和手段。二维码技术在物流，生产自动化，电子商务各领域被广泛应用的同时，产生了一系列的安全问题。本文基于演化加密技术，对传统的二维码生成算法进行改进，以提高二维码的防伪性能。并将其在农产品质量安全溯源系统中进行应用，结果表明改进的算法可以进一步提高二维码的安全性。

关键词：二维码技术；演化加密；溯源系统
中图分类号：TP391 文献标识码：A 文章编号：1004-874X(2013)24-0153-05

The two-dimensional code generation technology based on evolution encryption and application in the traceability system of quality of agricultural products

ZHONG Xiao-jun[1], LAI Zhi-jie[1], CHEN Dan[1], QIAN Jian-xin[1], HONG Xiao-cong[1], LI Cai-yi[1]
(1.*Guangdong Cuncuntong Technology Co. Ltd., Guangzhou* 510045, *China*;
2.*Guangdong Science and Technology Information Center, Guangzhou* 510045, *China*)

Abstract: Two-dimensional code technology is an electronic tagging technology of combination of computer and optical technology. It is an important way for information collection and input. Two-dimensional code technology produced a series of safety problems. At the same time, it has been widely used in various fields of logistics, production automation, e-commerce. This paper improved the security of traditional two-dimensional code generation algorithm based on evolution encryption. This algorithm was applied to agricultural products quality and safety traceability system, and the results showed that improvements were effective.

Key words: two-dimensional code; evolution encryption; traceability system

二维条码/二维码(2D barcode)是用某种特定的几何图形按一定规律在平面(二维方向上)分布的黑白相间的图形记录数据符号的信息。二维条码技术的研究始于 20 世纪 80 年代末。在二维条码符号表示技术研究方面，已研制出多种码制，常见的有 PDF417、QR Code、Data Matrix、Aztec、Maxicode、Code 49、Code 16K、Code One、Vericode、Ultracode、PhilipsDot Code、Softstrip 等。其中 QR Code 码(图 1)是 1994 年由日本 Denso-Wave 公司发明、最为常用的一种二维码。

二维码作为一种全新的信息存储、传递和识别技术，自诞生之日起就得到了世界上许多国家的关注。

图 1 QR 码

1 二维码加密及演化算法原理

1.1 二维码加密方法

二维码在被广泛应用的同时，产生了一系列的安全问题。由于数据的敏感性，因此对安全的需求也比较

收稿日期：2013-08-27
基金项目：国家科技支撑计划项目(2012BAD35B04)
作者简介：钟小军(1961-)，男，高级工程师，E-mail:zhongxiaojun@gdcct.gov.cn
通讯作者：赖志杰(1975-)，男，硕士，副研究员，E-mail:524619 5@qq.com

高。在这一背景下，研究二维码技术的安全应用问题相当有必要。目前，已有的二维码加密技术主要有基于DES算法的加密和基于Logistic混沌算法的加密两种方法[1-3]。

（1）基于DES算法的QR Code二维码加密方法。该方法首先对QR Code图像的数据进行读取，然后运用DES加密算法以64bit为单位对二维码图像中间黑白相间的区域进行加密操作；最后将加密前的二维码四周未加密的白色区间数据与加密后的二维码中间区域黑白相间数据组合以二值数字图像格式进行存储，存储后的图像文件就是加密后的图像数据。

（2）基于Logistic混沌算法的QR Code二维码加密方法。该方法与基于DES算法的QR Code二维码加密方法相同，首先对QR Code图像的数据进行读取，然后任意指定初始值和能够产生混沌序列的参数，利用 $X_{n+1}=\mu X_n(1-X_n)$，$n\in(0,1)$ 和 $Y_n=\begin{cases}0, 0<X_n\leqslant 0.5\\ 1, 0.5<X_n\leqslant 1\end{cases}$ 产生长度为N×N的Logistic二值混沌序列；最后将QRCode二维码的二值图像像素进行亦或操作，转化成BMP图像格式实现加密。

1.2 演化算法原理

演化算法(Evolutionary Algorithm，EA)是在生物进化优胜劣汰过程中得到启示，采用模拟生物进化策略所产生的一种方法。使用简单的编码来表示某种复杂问题，使种群在解空间进行搜索，采用交叉变异操作控制下一代种群的生成，最后采用适应度函数对种群进行选择，具有自组织、自适应、自学习等特征。这些特征使得演化算法具有简单、易于操作和通用的特性[4]。演化算法解决实际问题有以下几个基本步骤：

(1) 确定编码方案：首先根据实际问题，采用解的某种编码表示，产生种群。

(2) 确定交叉变异策略：采用某种交叉变异策略，实现种群的进化。

(3) 确定适应值函数：适应值是对解质量的一种度量，通常根据实际问题构造，一般以目标函数或代价函数的形式表示。适应值是对种群进行优胜劣汰选择的决定因素。

(4) 控制参数的选取：控制参数主要包括种群的规模、算法执行的最大代数以及其他一些辅助性的控制参数。

(5)算法的终止准则确定：演化算法是在解空间不断寻找最优解的过程，因此在演化过程中很有可能陷入局部最优解而无法找到真正的最优解导致算法无限循环下去。因此，常用的办法是预先定义一个最大的演化代数或算法在连续多少代以后解的适应值没有什么明显的改进时即终止的条件。

(6) 编程上机运行：使用某种编程语言实现具体演化算法过程。

2 基于演化算法的二维码生成算法

2.1 算法思想

本研究基于演化加密的思想，结合图像加密的评定策略，通过设定相应的判断阈值来控制加密过程，既增强了二维码加密的安全性，又使得加密和解密具有可控性。

2.2 算法实现

2.2.1 基于演化算法的二维码图像加密过程 基于演化算法的二维码生成算法加密过程的输入参数为二维码图像、初始加密参数和判断阈值，输出为加密后的二维码图像以及加密经过的迭代次数，具体流程如图2所示。

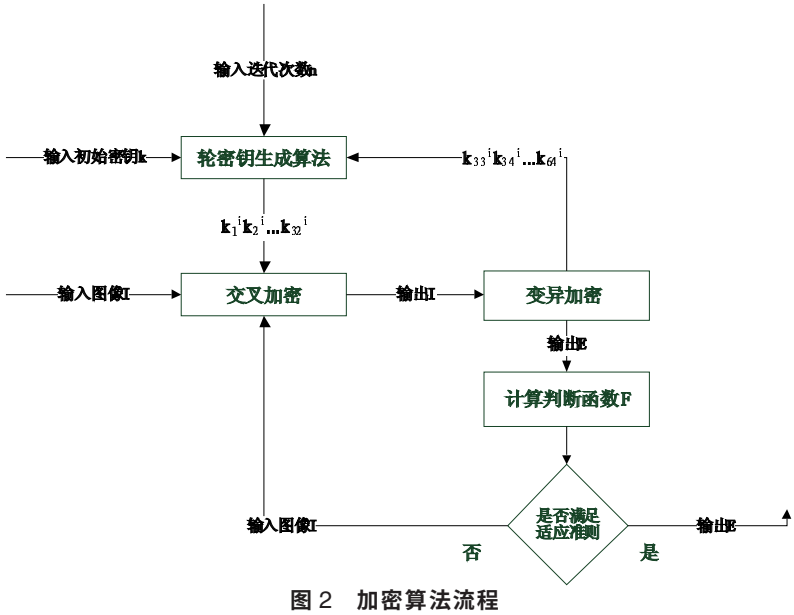

图2 加密算法流程

(1)输入加密前的二维码明文图像 I 和 64bit 的初始加密参数 k,以及相应的判断阈值 F0,并将迭代加密次数初始化为零,即 n=0。

(2)根据 64bit 的初始加密参数生成加密所需的轮密钥 $k_1^i k_2^i k_3^i \cdots k_{64}^i$。

(3)对加密前的二维码图像 I 首先使用交叉加密方法进行处理,将交叉加密后得到的二维码图像记为 I。

(4) 针对上一步骤后得到的已进行过交叉加密操作的二维码图像 I 再进行变异加密操作。这样,算完成整个一轮的演化加密过程, 将如此得到的加密二维码图像记为 E,同时将加密迭代次数加一,即 n=n+1;

(5) 针对上一步骤后得到的已加密二维码图像 E,依据相应的评价指标值 F,判断 F 是否满足判断阈值条件。如果满足条件,则判定加密过程完成,结果图像为最终的二维码加密图像;如果不满足判定条件,那么将经过本轮演化加密后的二维码图像 E 赋值给 I,返回第 2 步,继续进行下一轮加密。

在上述加密过程中, 算法的加密密钥包括了初始参数 k、判断阈值 F0 等。在每一轮演化加密迭代完成后,都需要进行条件判断,当满足条件时,加密过程结束, 这样就可以保证经过演化加密后的二维码图像在效果满足评价准则。

2.2.2 基于演化算法的二维码图像解密过程 首先根据演化加密过程的迭代次数 n 生成 n 组解密的轮密钥, 然后依照与演化加密过程正好相反的顺序使用轮密钥,最后按照与加密过程相同的步骤进行解密过程,解密流程见图 3。

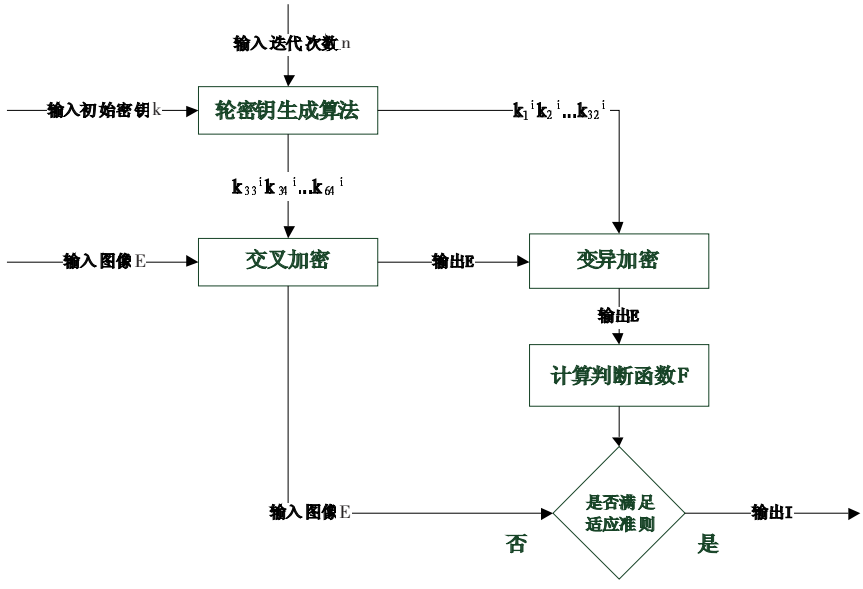

图 3 解密算法流程

基于演化算法的二维码生成算法解码过程的输人参数包括待解密的二维码图像 E、初始解密参数 k 和加密过程的加密迭代次数,解密过程如下:

(1)输入需要解密的二维码图像 E、初始解密参数 k 和加密过程的加密迭代次数 n。

(2)根据解密参数 k 和由加密迭代次数 n 产生的 n 组轮密钥 $k_1^1 k_2^1 k_3^1 \cdots k_{64}^1$, $k_1^2 k_2^2 k_3^2 \cdots k_{64}^2$,…, $k_1^n k_2^n k_3^n \cdots k_{64}^n$,并将这组轮密钥按照相反的顺序来使用。

(3) 对需要解密的二维码图像 E 首先进行变异操作,将经过变异解密得到的二维码图像记为 E。

(4) 对经过变异解密操作得到的二维码图像 E 再进行交叉操作,完成一轮的演化解密,将得到的二维码图像记为 E。

(5)根据加密过程的迭代次数 n,重复第三、第四步骤,计算得到最终的解密二维码图像 I。

2.3 算法分析

本研究基于演化算法的二维码生成算法,算法的密钥包括了初始参数 k、判断阈值 F0 等。根据上文所述,由于初始参数采用 64bit,因此能够生成 64 组不同的轮密钥,保证了二维码生成过程的安全性。判断阈值是另一个二维码图像生成过程的密钥,因为判断阈值的取值范围为一个在某一范围内的实数,要使加密迭代次数随着判断阈值取值而改变,判断阈值的取值精度一般不小于 0.01,因此加密算法的密钥空间会远大于 2^{64} ,更进一步保证了二维码生成过程的的安全性能。

3 基于演化加密的二维码在农产品质量安全溯源系统中的应用

3.1 二维码在农产品质量安全溯源系统中的应用

众所周知,农业是我国国民经济的基础。近年来,频发的农产品安全问题一次次考验着我们的生活。2005 年爆发的“苏丹红一号”,2008 年影响较广的“三聚氰胺”,以及近几年发生的“瘦肉精”、“牛肉膏”、“染色馒头”等危害人体安全的事件,不断威胁着普通老百姓的日常生活和身体健康。因此,如何有效实现对农产品的跟踪和追溯,已经迫在眉睫[5-9]。

“农产品质量安全溯源系统”是一个能够无缝连接农产品生产过程、检验检疫部门检验过程、政府监管部门监管过程和消费者各个环节,让消费者了解农产品从生产到销售是否符合卫生安全等方面信息,提高消费者权益的信息管理系统,该系统实现“从农田到餐桌”的追溯模式。一旦发现问题,能够根据溯源过程进行有效地召回,从源头上保障消费者的合法权益。

伴随着二维码技术的不断应用与提高,结合二维码技术的溯源系统已被广泛应用,并应用于农产品溯源系统中[10-14]。传统的二维码只能进行信息的标示,不能保证其安全性,二维码中的信息很容易被破译并进行仿造。因此,为了保证溯源系统的安全性,溯源过程中二维码的安全性如何保证成为了一个重要的问题。因此,本研究基于演化算法实现二维码的加密,并将加密后的二维码应用于农产品质量溯源系统中,进一步提高农产品溯源系统的安全性。

3.2 基于演化加密的二维码在农产品质量安全溯源系统中的应用实例

本研究选择了村村通商城的广州市农业科学研究院、广州市日月鲜农产品贸易有限公司、深圳市众健蔬菜产业供应链管理有限公司等 11 家农业企业安全农产品品牌网店示范应用,实现了从安全农产品生产层面开始溯源跟踪,保证产品流通到消费者餐桌之间的食品安全。具体包含以下模块:(1)基于演化加密的二维码的发行。包括二维码的加密生成、加密二维码粘贴。(2)农产品溯源信息管理。包括二维码的信息查询、农产品生产商信息查询、农产品生产基地环境检测信息查询、农产品质量安全检测信息查询、农产品流通环节查询。

由于该平台二维码图像进行了加密操作,因此无法通过一般的二维码读取软件进行解码,必须使用专门的二维码读取设备或登陆安全农产品溯源系统平台才能够正确进行解码。该溯源平台的正确解码操作过程如下:

(1)通过手机查询。首先下载溯源系统手机客户端,安装完成后,打开软件会看到 1 个按钮,如图 4A 所示。通过手机扫描农产品的二维码,手机客户端通过将该二维码上传至溯源平台后台查询系统,然后将查询结果反馈回用户手机客户端,如图 4B 所示。

图 4 手机客户端二维码查询系统

(2)通过网站查询。通过网站查询的方式为首先登陆安全农产品溯源系统平台,如图 5A 所示。在二维码图像上传区域单机上传待查询二维码图像,网站后台通过输入的二维码图像数据并进行解码操作,返回查询结果给用户,结果如图 5B 所示。

4 结论及应用前景分析

本文主要针对传统 QR 二维码的生成方法难以保证二维码信息的安全进行研究,将演化加密方法应用于二维码的生成中,在一定程度上有效避免了因为人

图 5　网站客户端查询系统

为因素而导致的数据泄漏，大幅度提升了二维码的安全系数，保证了二维码的安全性和防伪性。并将该算法应用于实际的农产品安全溯源系统中，证明了基于演化加密技术生成二维码的可行性和有效性。

信息技术在农产品安全领域中具有不可替代的重要影响，信息技术的广泛应用会将中国的农产品质量安全体系带入信息化时代。可以预计，通过本研究基于演化加密算法对二维码进行安全控制，并在农产品质量安全溯源系统中应用，监管部门和消费者可以方便有效地了解农产品的生产环境以及农药、化肥等的使用情况。对实现农产品从生产到消费的全程监控、实现农产品流通环节的信息采集与发布，保护消费者权益具有重要作用，对于实现农产品供应链的优化整合、农民增收和产业发展具有重要的推进作用。

参考文献：

[1] 张定会，单俊涛，江平.QR 码 DES 加密与解密[J].数据通信，2011(3):40–42.

[2] 张定会，郭静波，江平，等.QR 码二值图像混沌加密与解密[J].移动通讯，2011,35(3)：131–134.

[3] 韦宝典，刘东苏，王新梅.AES 算法 Rijndael 的原来、实现和攻击[J].通信技术，2002(12):65–68.

[4] Zhao F，Jiao L C，Liu H Q，et a1.A novel fuzzy clustering algorithm with non local adaptive spatial constraint for image segmentation[J].Signal Processing，2011，91(4)：988–999.

[5] 陈蕾蕾，祝清俊，王未名，等.中国农产品安全问题的现状与对策[J].农产品加工，2010(3):58–59,64.

[6] 邢文英.美国的农产品质量安全可追溯制度[J].世界农业，2006(4):39–41.

[7] 戚亚梅，李祥洲，郭林宇.国外农产品安全管理信息体系建设及运用研究[J].世界农业，2009(5):10–13.

[7] 谢菊芳，陆昌华，李保明，等.基于 NET 构架的安全猪肉全程可追溯系统实现[J].农业工程学报，2006,22(6):218–220.

[8] 杨信廷，钱建平，孙传恒，等.蔬菜安全生产管理及质量追溯系统设计与实现[J].农业工程学报，2008,24(3):162–166.

[9] 杨信廷，孙传恒，钱建平，等.基于流程编码的水产养殖产品质量追溯系统的构建与实现[J].农业工程学报，2008,24(2):159–164.

[10] 邓勋飞，吕晓男，郑素英，等.基于 GIS 的农产品安全溯源体系[J].农业工程学报，2008,24(2):172–176.

[11] Balvay L M B. Traceability of beef production and industry in France in Computer and Computing Technologies in Agriculture II, Volume 3 [A].The Second IFIP International Conference on Computer and Computing Technologies in Agriculture (CCTA2008)[C].Beijing, China. Springer–Verlag New York Inc,2009:896–899.

[12] De–an Z T, Cui–feng ,W Xian–wang. Design of Traceability System for Pork Safety Production Based on RFID[A]. in 2009 Second International Conference on Intelligent computation Technology and Automation[C]. IEEE,2009.

[13] Chen R S. Using RFID Technology in Food Produce Traceability [J]. WSEAS Transactions on Information Science and Applications,2008,5(11):1551–1560.

[14] Liu S. Study on quality safety traceability systems for cereal and oil products[A].In World Congress on Software Engineering [C].IEEE,2009.

（责任编辑　苏柱华）