DOI:10.6041/j.issn.1000-1298.2012.04.021

水产品追溯码加密算法设计与应用*

李文勇[1]　孙传恒[1,2]　刘学馨[1]　周　超[1]　谢　菁[1]　杨信廷[1]

(1. 国家农业信息化工程技术研究中心, 北京 100097; 2. 中国农业大学信息与电气工程学院, 北京 100083)

【摘要】 为解决当前农产品追溯码安全性不高,难以保证一品一码等问题,以水产品为研究对象,提出了一种水产品追溯码加密算法。在深入分析各种追溯码编码方案和 AES 加密算法的基础上,对水产品监管码进行编码、压缩和十进制等长加密生成水产品追溯码。实验证明算法可行、可靠;密钥的动态变化和追溯码的唯一性,为追溯系统的实际应用提供了安全保障。最后给出了该算法在水产品质量追溯系统中的应用方案。

关键词: 水产品　追溯码　编码压缩　十进制加密　动态密钥

中图分类号: TP391; X954　　**文献标识码**: A　　**文章编号**: 1000-1298(2012)04-0106-07

Design and Implementation of Encryption Algorithm for Aquatic Products Traceability Code

Li Wenyong[1]　Sun Chuanheng[1,2]　Liu Xuexin[1]　Zhou Chao[1]　Xie Jing[1]　Yang Xinting[1]

(1. *National Engineering Research Center for Information Technology in Agriculture*, *Beijing* 100097, *China*
2. *College of Information and Electrical Engineering*, *China Agricultural University*, *Beijing* 100083, *China*)

Abstract

In order to solve such problems as low-level security of traceability code for agricultural products and difficulty to guarantee the traceability code was unique for one product, taking aquatic products as research object, an encryption algorithm of traceability code for aquatic products was put forward. At the base of analysis to coding solution of traceability code and AES encryption algorithm, the aquatic product was coded. Then, this supervision code was compressed and encrypted by an algorithm namely decimal and equal-length to generate the traceability code for aquatic products. The experimental results showed that the proposed algorithm was feasible and reliable. It ensured the deployment security of traceability system owing to the feature of uniqueness and dynamic cipher of traceability code. An example of the application solution of the encryption algorithm in aquatic products traceability system was introduced.

Key words　Aquatic products, Traceability code, Code compression, Decimal encryption, Dynamic key

引言

建立农产品质量追溯系统,促进中国农产品安全体系搭建是保障消费者食用农产品安全和提升农产品竞争力的重要手段[1~2]。统一编码是实现农产品追溯系统的基础,而追溯码的安全性则是农产品追溯系统全面实施的重要保障。

关于追溯码编码的研究,国外多采用 EAN.UCC 系统对农产品的生产过程进行跟踪和溯源,其编码由全球贸易项目代码(GTIN)、属性代码(如批次、有效期、保质期等)、全球位置码(GLN)、物流单元标识代码(SSCC-18)和储运单元标识代码(ITF-14)

收稿日期: 2011-08-22　修回日期: 2011-11-14

*国家高技术研究发展计划(863 计划)资助项目(2011AA100706)

作者简介: 李文勇,工程师,主要从事嵌入式系统、数字信号处理研究,E-mail: liwy@nercita.org.cn

通讯作者: 杨信廷,副研究员,主要从事农业信息化关键技术及农产品质量安全控制研究,E-mail: yangxt@nercita.org.cn

等构成；欧盟等国已采用 EAN. UCC 系统成功地对牛肉、蔬菜等开展了食品跟踪研究[3]。国内在这方面的研究起步较晚，但取得了一定进展。如中国物品编码中心参考国际物品编码协会出版的相关应用指南，并结合中国的实际情况制订了《牛肉产品跟踪与追溯指南》和《水果、蔬菜跟踪与追溯指南》[4~5]等；中国农业部于 2007 年颁布了《NY/T 1431—2007 农产品追溯编码导则》，要求农产品追溯码具有防伪功能，展现形式简单、统一，易于识读，对追溯码的代码结构和表示形式作了说明[6]。除此之外，国内学者也对农产品追溯码的编码进行了研究。如杨信廷等通过对果蔬物流情况的分析以及编码标准的研究，采用全球贸易代码、产品日期、产品产地相结合的条码设计方案，提出了一种产品编码与过程编码相结合的编码方法[7~8]，以及基于地理坐标的农产品追溯码方案[3]；Qu 等采用位置编码、地块编码、生产日期、生产批次、校验码的组合编码方式设计追溯码[9]；邓勋飞等采用以行政区划码和地块编号为主体的方式进行编码[10]。

综合分析目前已有的农产品追溯码编码导则和方式，存在着长度较长、加密较弱甚至没有任何加密，很容易被私自篡改、伪造以及无法做到追溯码唯一性等问题，而且目前国内各省市自治区开发自己的农产品质量追溯系统时，从农产品流通码提取代码的方法也不一致，采用的加密算法不仅不同且互相保密。本文针对上述问题，以水产品为研究对象，以 AES 加密算法为基础，设计与实现水产品追溯编码压缩及其加密算法，不同密钥加密运算的算法不一样，使加密算法具有随机性。提出追溯码动态密钥的概念，实现动态加密的防伪效果，为农产品质量安全追溯的全面实施提供保障。

1　AES 加密算法

1.1　AES 算法原理

AES 加密算法是美国的数据加密国家标准，是由比利时学者 Vincent Rijmen 和 Joan Daemen 设计的 Rijndael 算法，是对称加密算法中加密性能和速度等各项性能指标最好的加密算法[11]。它的原形是 Square 算法，设计策略采用的是宽轨迹策略，从而可以提高算法抗击差分密码分析及线性密码分析的能力[12]。

AES 加密算法的数据分组长度定为 128 位，密钥长度可为 128、192 或 256 位，并由密钥长度决定加密轮变换次数 N_r 为 10、12 或 14[13]。加密算法中的 128 比特的分组信息被分成 16 个字节，按顺序排列成一个 4×4 的矩阵，称为状态(state)。AES 的所有变换都是基于状态的变换，数据处理最小单元是字节。

AES 算法对数据的加密是通过把输入的明文和密钥由轮函数经 N_r+1 轮迭代来实现的，初始轮和结尾轮与中间的 N_r-1 轮不同。初始轮只对明文和密钥进行异或操作；中间的 N_r-1 轮依次进行字节代换、行移位变换、列混合变换和轮密钥加；结尾轮与中间轮相比去掉了列混合变换，以使加密和解密算法在结构上更加接近。

1.2　算法加密与解密

AES 加密算法核心思想是经过多轮置换迭代操作，使数字信息尽可能地散列和混淆。为方便起见，用 C 代表轮密钥控制，B 代表 S 盒置换，S 代表行移位变换，M 代表列混合变换，加密过程如图 1 所示。

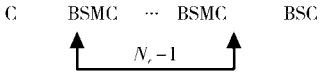

图 1　AES 加密过程代式表示

Fig. 1　Formula of AES encryption

由于该加密运算中采用的每一种运算都是可逆的，所以对于上面的加密过程只需要对每一种运算求逆即可解密。解密过程如图 2 所示。

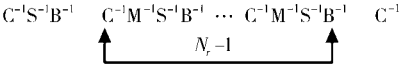

图 2　AES 解密过程代式表示

Fig. 2　Formula of AES decryption

图 2 中，C^{-1} 为轮密钥控制的逆运算，S^{-1} 为行移位逆运算，B^{-1} 为 S 盒逆置换，M^{-1} 为列混合逆运算。

然而计算机适宜处理十六进制数(即二进制)，AES 加密算法是针对十六进制数进行加密[14]。而目前研究的农产品追溯码编码大部分都是由 0~9 之间的十进制数字构成，而且要求追溯码位数和加密后密文位数相对应，即没有密文扩展，基于十六进制的 AES 加密算法就不能满足上述要求。

2　水产品追溯码加密方案

2.1　基于监管模式的水产品追溯编码

水产品监管追溯编码从政府监管的角度出发，以批次作为追溯单元，以同一养殖主体、同一池塘内、同一时间出池、同一品种的产品作为编码单元[15]。水产养殖品追溯监管码由行政区划代码、企业顺序号、产品分类代码、源实体参考代码、生产日期代码和校验码构成，具体结构如表 1 所示。

厂商识别代码 10 位数字：行政区划代码可具体到县级，具体可参考 GB/T 2260—2007 的编码，企业顺序号由 1 位企业类型识别代码和 3 位企业顺序流

表 1 水产养殖品追溯监管码 27 位结构

Tab. 1 Structure of aquatic products traceability and supervision code of 27 bits

厂商识别代码		产品批号代码			校验码
行政区划代码	企业顺序号	产品分类代码	源实体参考代码	生产日期代码	
$N_1 \sim N_6$	$N_7 \sim N_{10}$	$N_{11} \sim N_{16}$	$N_{17} \sim N_{20}$	$N_{21} \sim N_{26}$	N_{27}

水号组成。产品批号代码 16 位数字,由 6 位产品分类代码、4 位源实体参考代码和 6 位生产日期代码组成。产品分类代码按照层次码的设计,详见 SC 3001—1989 水产品名称分类。

2.2 水产品追溯码加密算法

采用上述按水产品、按辖区生成的水产品追溯码编码,对于消费者来说,存在着易于被仿制、安全性低的问题,以及长度过长,不利于产品追溯等缺点。同时为了防止追溯码被私自修改,在设计追溯码时还要采取专用加密算法对水产品追溯码进行压缩、加密。

2.2.1 水产品追溯码压缩

根据上述编码规则,采用分组的方法对每一码段进行重新编码压缩。编码压缩的基本思想是采用穷举法对每一码段按照最大取值范围进行重新编码设计。其中,校验码由厂商识别代码、产品批号代码计算得到,在压缩时可忽略;县级行政区划数量有 2 800个左右,因此,采用 4 个十进制位表示;企业顺序号保持不变;水产品分类代码采用 3 个十进制位表示 1 000 个主流养殖品种完全可满足水产品应用需求;源实体代码即企业池塘编号保持不变;根据《中华人民共和国农产品质量安全法》规定,农产品记录保存时间一般为 2 年,这里生产日期代码时间跨度按 100 年计算,足以满足对农产品质量追溯的要求,以 2000 年 1 月 1 日为基准,采用 5 位十进制数即可表示当前生产日期与基准日期相差的天数。具体编码转换如图 3 所示。

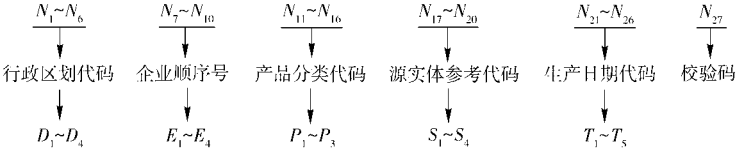

图 3 水产品追溯监管码分组压缩

Fig. 3 Compression of traceability and supervision code of aquatic products by groups

2.2.2 追溯码加密算法过程

经压缩的水产品追溯编码采用分组压缩方法,实现了编码长度的减少,但其安全性和防伪性能较差。需要对其进行加密,而且加密前、后需要保持长度不变。通过对 AES 算法分析可知,AES 加密算法无法满足对十进制数据的加密,在参考刘连浩[14~16]等设计方法基础上,对 AES 算法进行改进,重新设计 AES 算法中的 4 种加密运算,以适应十进制数直接加密的要求。同时为增强加密强度,保证生成追溯码的唯一性,使同一明文生成无规律的密文,实现一次一密防伪效果,采用动态密钥对水产品追溯码进行混沌随机加密。具体的加、解密流程,如图 4、5 所示。

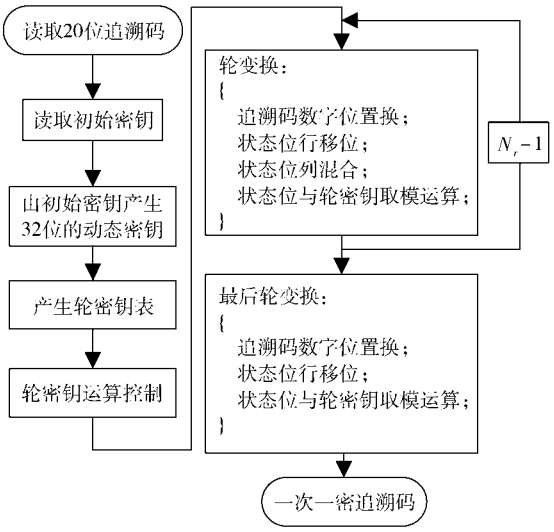

图 4 追溯码加密流程图

Fig. 4 Encryption flow of traceability code

该算法对数据进行分组迭代操作,分组长度和密钥长度可独立指定,密钥轮数可任意,轮数越多,加密程度越高,运算时间越长。本方案采用 12 轮加密策略。每一轮变换由 3 层组成[17]:

(1) 线性混合层:包含追溯码状态位行移位和列混合,目的是为了确保多轮迭代运算的高度扩散。

(2) 非线性层:由一个 10 进制 S 盒组成,起到追溯码数字位置换混淆的作用。

(3) 轮密钥控制层:根据不同的条件,对轮密钥和追溯码状态各个对应的数字进行取模运算,实现密钥和追溯码字的混合。

算法主要包括以下几个关键步骤:

(1) 追溯码动态密钥生成

动态密钥是根据初始密钥、编码生成次数、企业顺序号生成 32 位十进制数密钥。生成过程如图 6 所示。其中 Sbox 运算为 S 盒置换操作。

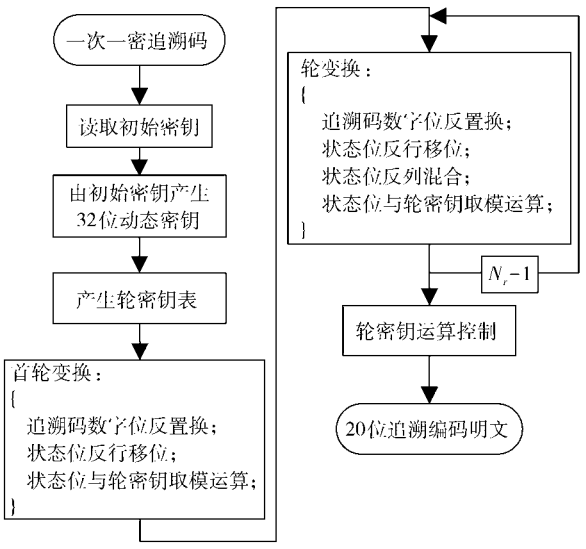

图 5　追溯码解密流程图

Fig. 5　Decryption flow of traceability code

（2）追溯码数字位置换盒

追溯码十进制数字位置换盒，如图 7 所示。反置换盒如图 8 所示。每一轮的数字位置换中，能够达到一半的十进制位发生变化。

（3）追溯码状态位行移位

追溯码状态位是指需要加密的追溯码每位数字，比如 20 位追溯码：26347411750000131203，其状态表如图 9 所示。

状态位行移位规则：第 1 行不移动，第 2 行循环左移 1 位，第 3 行循环左移 2 位，第 4 行循环左移 3 位。图 9 行移位后的结果如图 10 所示。

（4）追溯码状态位列混合

追溯码状态位列混合操作，是用一个可逆正整数矩阵左乘追溯码状态位矩阵，然后对 10 进行取模运算，将得到的结果放回原来的矩阵中。这里的可逆正整数矩阵采用的是刘连浩等[16]设计的矩阵 $\boldsymbol{M}$。

$$\boldsymbol{M}=\begin{bmatrix}5&3&2&1\\1&5&3&2\\2&1&5&3\\3&2&1&5\end{bmatrix}\quad \boldsymbol{M}^{-1}=\begin{bmatrix}5&9&4&3\\3&5&9&4\\4&3&5&9\\9&4&3&5\end{bmatrix}$$

$$\begin{bmatrix}s'_{1c}\\s'_{2c}\\s'_{3c}\\s'_{4c}\end{bmatrix}=\begin{bmatrix}5&3&2&1\\1&5&3&2\\2&1&5&3\\3&2&1&5\end{bmatrix}\begin{bmatrix}s_{1c}\\s_{2c}\\s_{3c}\\s_{4c}\end{bmatrix}\bmod 10 \qquad (1)$$

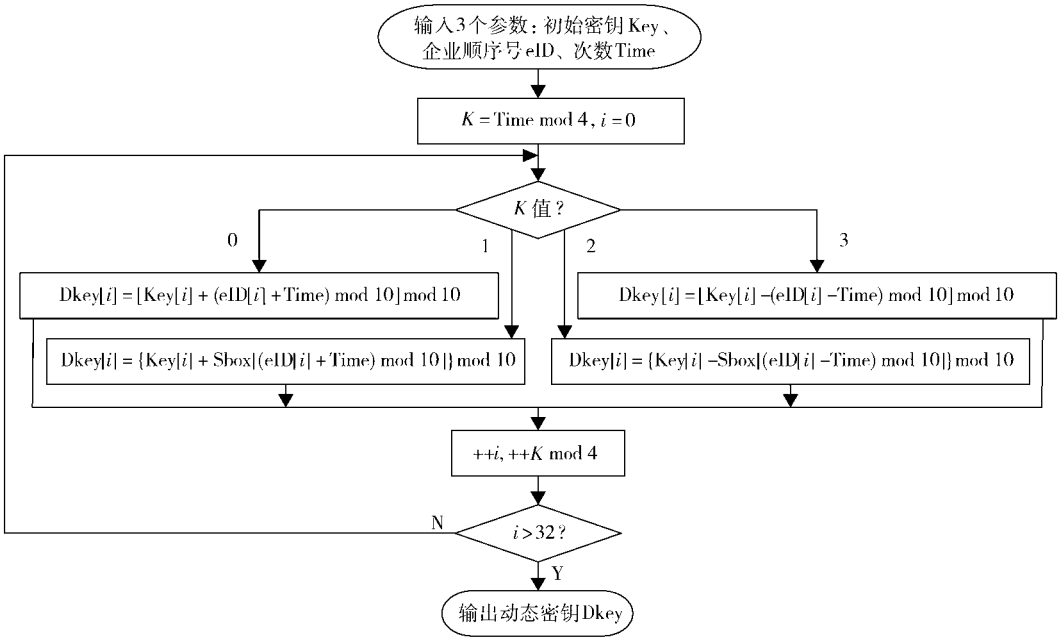

图 6　动态密钥产生算法流程图

Fig. 6　Generation algorithm of dynamic key

0	1	2	3	4	5	6	7	8	9
6	8	4	9	7	2	1	0	5	3

图 7　数字位置换盒

Fig. 7　Table of digital bits substitution

0	1	2	3	4	5	6	7	8	9
7	6	5	9	2	8	0	4	1	3

图 8　数字位反置换盒

Fig. 8　Table of inverse digital bits substitution

2	7	7	0	1
6	4	5	0	2
3	1	0	1	0
4	1	0	3	3

图 9　20 位追溯码状态表

Fig. 9　Table of traceability code states of 20 bits

2	7	7	0	1
4	5	0	2	6
0	1	0	3	1
3	3	4	1	0

图 10　状态位行移位

Fig. 10　Shift row of traceability code states

$$\begin{bmatrix} s_{1c} \\ s_{2c} \\ s_{3c} \\ s_{4c} \end{bmatrix} = \begin{bmatrix} 5 & 9 & 4 & 3 \\ 3 & 5 & 9 & 4 \\ 4 & 3 & 5 & 9 \\ 9 & 4 & 3 & 5 \end{bmatrix} \begin{bmatrix} s'_{1c} \\ s'_{2c} \\ s'_{3c} \\ s'_{4c} \end{bmatrix} \bmod 10 \qquad (2)$$

式(1)为列混合操作的矩阵表示,式(2)为列混合逆操作矩阵表示。

(5) 追溯码状态位与轮密钥取模运算

在 AES 加密算法中,轮密钥加利用密钥与状态对应的字节作异或运算。但是对于十进制数来说异或运算没有可逆性。为了使追溯码状态位与轮密钥混淆,并且具有可逆性,将 AES 算法中的二进制异或改成十进制的轮密钥控制运算,根据每一轮的密钥不同,分别进行 4 种运算中的 1 种。入口由每一轮加密所有使用的密钥各位之和对 4 取模来确定。每一轮运算步骤简述如下:

(1) 32 位动态密钥求和,记为 Sum。

(2) 入口参数 Enter = Sum mod 4。

(3) 根据步骤(2)的结果,进入不同的状态位和轮密钥加减运算。

2.2.3 追溯码加密算法实现

在上述的加、解密算法中,动态密钥是根据初始密钥、编码生成次数、企业顺序号生成的 32 位十进制数密钥,编码生成次数每生成一次加 1,利用密钥对生成次数敏感的特点,产生新的动态密钥和密文,从而实现以编码生成次数为混沌参数的混沌加密。使用 C#语言,在 Visual Studio 2005 开发环境下编程实现,初始密钥为长度小于 32 位的 0 ~9 数字组成,由用户自由设置,以广东省茂名市某企业为例,27 位的追溯码为 44090210010101220001101120 0。压缩、加解密结果如图 11、12 所示。

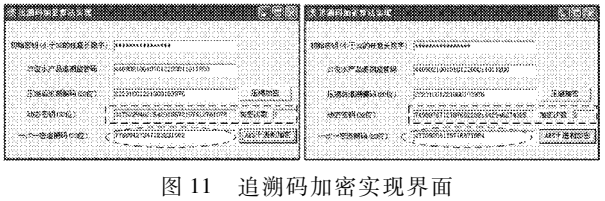

图 11 追溯码加密实现界面

Fig. 11 Implementation of traceability code encryption

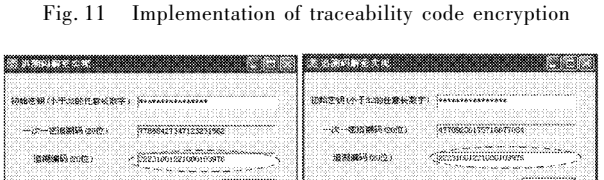

图 12 追溯码解密实现界面

Fig. 12 Implementation of traceability code decryption

从图 11 可以看出,在初始密钥和追溯编码一样的情况下,随着加密次数的不同,密钥也随着变化,得到的追溯码也不同,实现了一次一密和追溯码的唯一性。从图 12 可以看出,实现了在知道初始密钥的情况下,对压缩后的加密追溯码成功解密,得到追溯编码明文。

3 应用示例

将本文的加密、解密算法移植到自主开发的混合条码水产品追溯监管标签打印和追溯系统中,实现了加密标签的打印和追溯码解密追溯[18~19]。以系统在广东省水产品追溯中的应用为例,广东省茂名市广东绿卡实业有限公司 2010 年 11 月 20 日生产的某一批次绿卡牌中华鳖的信息为:企业的行政区划代码:440902;企业类型:养殖企业(1);企业顺序流水号:001;水产品大类:鲜、活品类;水产品种类:淡水鱼;水产品名称:绿卡牌中华鳖;出池日期:2010 年 11 月 20 日。

根据水产养殖品追溯监管码编码规则,计算得到 6 位行政区划代码为 440902;4 位企业顺序号为 1001;6 位产品分类代码为 010122;4 位源实体参考代码,即水产养殖企业产品出池的池塘编号,由企业内部编码,这里假如池塘编号位 0001;6 位生成日期代码为 101120;校验码为 0,综合以上信息,该企业该批次产品的 27 位追溯编码为:44090210010101220 00011011200。当出池日期为 2010 年 11 月 21 日时,该批次产品的 27 位追溯码为:44090210010101220 0011011211。

广东绿卡实业有限公司养殖生产管理系统打印出具有一维条码和二维条码组成的混合标签。其中,一维条码采用 EAN-128 码制,由水产品追溯监管码经本文的加密算法生成,如图 13 所示。例如 2010 年 11 月 20 日出池的中华鳖的 27 位追溯监管码为:44090210010101220001101120 0,经压缩后为:22231001221000103976,加密后为:77888427347123231562。2010 年 11 月 21 日出池的中华鳖的 27 位追溯监管码为:44090210010101220001101121 1,经压缩后为:22231001221000103977,加密后为:09404382050494370518。

经过压缩后,在保证实用和扩展的条件下缩短

图 13 广东省水产品追溯监管标签

Fig. 13 Aquatic products traceability label for supervision of Guangdong province

了码长，满足了编码导则的要求之一；每个产品上的标签，具有不同的追溯码，满足了编码导则的唯一性要求，杜绝了仿制标签的现象。从追溯码数字表面看不出它所包含的任何含义，而且即使在得知追溯码的编码规则后，也无法获取里面的信息，安全性得到了很大的提高。

图 14a 为广东绿卡实业有限公司生产管理软件打印出来加载于中华鳖包装上的追溯标签；图 14b 为广东省省级水产品监管平台，将追溯标签上的追溯码输入该系统，就可以进行产品追溯；图 14c 为经过对追溯码解密后，消费者进行网络追溯的结果，消费者可以追溯出责任主体信息、养殖过程信息等。

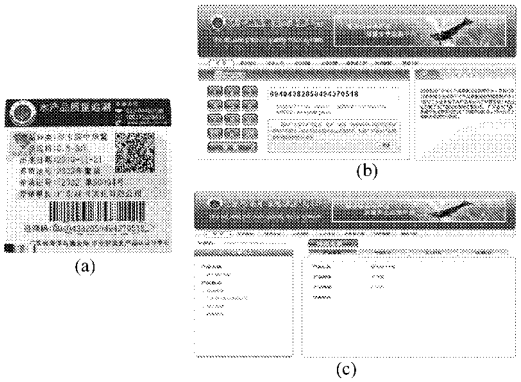

图 14　广东省水产品追溯过程

Fig. 14　Proess of aquatic products traceability of Guangdong province

（a）水产品追溯标签　（b）水产品追溯平台　（c）追溯结果

4　结论

（1）针对目前农产品追溯编码设计以及农业部追溯码编码导则存在的不足和问题，以水产品为研究对象，详述了水产品追溯监管码的设计与压缩方法。

（2）以 AES 加密算法为基础，对压缩后的追溯编码进行了加、解密算法设计与实现，达到了一次一密的防伪效果。

（3）加密生成的追溯码具有一次一码的特点，即每加密一次，生成的追溯码是不同的，做到了追溯码的唯一性，杜绝了仿制同一标签的现象。一方面，当市场上出现大量同一标签时，可以断定是假冒伪劣产品；另一方面，追溯结果会显示追溯码被追溯过的次数和时间，顾客若发现追溯码已被追溯过，就有可能是假货的嫌疑，可以进行举报。

（4）给出了加密算法在水产品追溯系统中的应用，验证了该算法的可行性与安全性。算法的应用增强了追溯系统的安全性，为农产品的可靠追溯提供了保障。

（5）本文加密算法的实现和应用都是在基于 Intel 处理器和微软操作系统的 PC 机上完成的。随着嵌入式系统的发展，利用手持等便携式设备进行水产品追溯监管也有广泛的应用需要，因此在下一步的工作中，将对水产品追溯码加密算法在嵌入式手持设备上的移植进行研究。

参　考　文　献

1　崔洁. 加强农产品安全工作确保百姓餐桌安全[J]. 农业质量标准，2006(2)：18～21.

2　申广荣，赵晓东，黄丹枫. 关于农产品安全体系建设的思考[J]. 上海交通大学学报：农业科学版，2005，23(1)：77～83.
Shen Guangrong，Zhao Xiaodong，Huang Danfeng. Consideration of farm product safety system in China[J]. Journal of Shanghai Jiaotong University：Agricultural Science，2005，23(1)：77～83.（in Chinese）

3　杨信廷，钱建平，张正，等. 基于地理坐标和多重加密的农产品追溯编码设计[J]. 农业工程学报，2009，25 (7)：131～135.
Yang Xinting，Qian Jianping，Zhang Zheng，et al. Design of agricultural product trace coding based on geography coordinate and multi-encrypt[J]. Transactions of the Chinese Society of Agricultural Engineering，2009，25(7)：131～135.（in Chinese）

4　中国物品编码中心. 牛肉产品跟踪与追溯指南[S]. 2005.

5　中国物品编码中心. 水果、蔬菜跟踪与追溯指南[S]. 2005.

6　NY/T 1431—2007　农产品追溯编码导则[S]. 2007.

7　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.
Yang Xinting，Qian Jianping，Sun Chuanheng，et al. Design and application of safe production and quality traceability system for vegetable[J]. Transactions of the Chinese Society of Agricultural Engineering，2008，24(3)：162～166.（in Chinese）

8　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.
Yang Xinting，Sun Chuanheng，Qian Jianping，et al. Construction and implementation of fishery product quality traceability system based on the flow code of aquaculture[J]. Transactions of the Chinese Society of Agricultural Engineering，2008，24(2)：159～164.（in Chinese）

9　Qu Xiaohui，Zhuang Dafang，Qiu Dongsheng. Studies on GIS based tracing and traceability of safe crop product in China[J].

Agricultural Sciences in China, 2007, 6(6): 724 ~ 731.

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(增刊 2):172 ~ 176.
Deng Xunfei, Lü Xiaonan, Zheng Suying, et al. GIS-based traceability system of agricultural product safety [J]. Transactions of the Chinese Society of Agricultural Engineering, 2008, 24(Supp. 2): 172 ~ 176. (in Chinese)

11 Phan R C W. Impossible differential cryptanalysis of 7-round advanced encryption standard (AES) [J]. Information Processing Letters, 2004,91(1): 33 ~ 38.

12 魏凤兰,汤秀芬,米晨. AES 加密算法中的 S 盒及其 C 语言实现[J]. 宁夏工程技术, 2005,4(1): 42 ~ 44.
Wei Fenglan, Tang Xiufen, Mi Chen. S-box in AES encipher algorithm and its C language implementation[J]. Ningxia Engineering Technology, 2005, 4(1):42 ~ 44. (in Chinese)

13 翁小杰,宋中山,杨娜. AES 加密算法及 S-box 改进策略[J]. 电脑知识与技术, 2007, 4(19): 63 ~ 64.
Weng Xiaojie,Song Zhongshan,Yang Na. AES encryption arithmetic and S-box improved strategy[J]. Computer Knowledge and Technology, 2007, 4(19):63 ~ 64. (in Chinese)

14 刘连浩. 基于身份的十进制加密技术研究[J]. 计算机工程与应用, 2005,41(24): 154 ~ 156.
Liu Lianhao. Research of ID-based encryption technology on decimal system[J]. Computer Engineering and Applications, 2005, 41(24):154 ~ 156. (in Chinese)

15 刘学馨,杨信廷,宋怿,等. 基于养殖流程的水产品质量追溯系统编码体系的构建[J]. 农业网络信息, 2008(1): 18 ~ 21.
Liu Xuexin, Yang Xinting, Song Yi, et al. Construction of fishery products coding scheme of quality traceability system based on the aquaculture flow[J]. Agriculture Network Information, 2008(1): 18 ~ 21. (in Chinese)

16 刘连浩,罗安,陈松乔. 基于十进制的加密技术研究[J]. 小型微型计算机系统,2006,27(7): 1 229 ~ 1 231.
Liu Lianhao, Luo An, Chen Songqiao. Research of encryption technology based on decimal system[J]. Mini-Micro Systems, 2006, 27(7): 1 229 ~ 1 231. (in Chinese)

17 孙爱娟,武俊峰. AES 加密算法中的 S-盒及其 MATLAB 实现[J]. 信息技术, 2008(11): 67 ~ 69,73.
Sun Aijuan, Wu Junfeng. The S-box of AES encryption algorithm and its MATLAB implementation [J]. Information Technology, 2008(11):67 ~ 69, 73. (in Chinese)

18 杨信廷,钱建平,范蓓蕾,等. 农产品物流过程追溯中的智能配送系统[J]. 农业机械学报,2011,42(5):125 ~ 130.
Yang Xinting, Qian Jianping, Fan Beilei, et al. Establishment of intelligent distribution system applying in logistics process traceability for agricultural product[J]. Transactions of the Chinese Society for Agricultural Machinery, 2011,42(5):125 ~ 130. (in Chinese)

19 陈长喜,张宏福,飞颉经纬. 肉鸡产业技术体系生产监测与产品质量可追溯平台设计[J]. 农业机械学报,2010, 41(8):100 ~ 106.
Chen Changxi, Zhang Hongfu, Feixie Jingwei. Traceability platform design of production monitoring and products quality for broilers industry technology system[J]. Transactions of the Chinese Society for Agricultural Machinery, 2010,41(8):100 ~ 106. (in Chinese)

(上接第 74 页)

6 Kim H S,Tsai L W. Kinematic synthesis of spatial 3-RPS parallel manipulators[C]// Proc. of DECT'02 ASME 2002 Design Engineering Technical Conference, Canada,2002:978 ~ 986.

7 Jacques Steyn. Fatigue failure of deck support beams on a vibrating screen [J]. International Journal of Pressure Vessels and Piping,1995,61(2 ~ 3):315 ~ 327.

8 徐立章,李耀明,李洪昌,等. 纵轴流脱粒分离-清选试验台设计[J]. 农业机械学报,2009,40(12):76 ~ 79.
Xu Lizhang, Li Yaoming, Li Hongchang, et al. Development on test-bed of longitudinal axial threshing-separating-cleaning unit [J]. Transactions of the Chinese Society for Agricultural Machinery, 2009, 40(12):76 ~ 79. (in Chinese)

9 焦红光. 振动筛分过程解析[M]. 北京:煤炭工业出版社,2008.

10 徐立章,李耀明,张立功,等. 轴流式脱粒-清选装置试验台的设计[J]. 农业机械学报,2007,38(12):85 ~ 88.
Xu Lizhang, Li Yaoming, Zhang Ligong, et al. Development on test-bed of axial threshing and cleaning unit [J]. Transactions of the Chinese Society for Agricultural Machinery, 2007,38(12):85 ~ 88. (in Chinese)