Multiple Encryption-based Algorithm of Agricultural Product Trace Code

YU Hua*, WU Zhen-hua

College of Information and Management Science, Henan Agricultural University, Zhengzhou 450002, China

Abstract To establish a sound traceability system of agricultural products and guarantee security of agricultural products, an algorithm is proposed to encrypt trace code of agricultural products. Original trace code consists of 34 digits indicating such information as place of origin, name of product, date of production and authentication. Area code is used to indicate enterprise information, the encrypted algorithm is designed because of the increasing code length, such coding algorithms as system conversion and section division are applied for the encrypted conversion of code of origin place and production date code, moreover, section identification code and authentication code are permutated and combined to produce check code. Through the multiple encryption and code length compression, 34 digits are compressed to 20 on the basis of ensuring complete coding information, shorter code length and better encryption enable the public to know information about agricultural products without consulting professional database.

Key words Encryption, Trace, Area code, System conversion, Section

China has been again challenged by serious food security problems such as " mercury in Sprite" , " genetically modified staple food" , " poisonous Hainan cowpea" since the milk powder crisis in 2008 and the reappeared milk powder problem at the end of 2010[1]. Security of agricultural products, the fundamental section of food security, directly influences life security of the public and social stability, thus the whole process of food production, especially production of fresh agricultural products, should be supervised, a traceability system of agricultural products should be established to ensure food security[2-4]. Such a traceability system has been well developed in foreign countries, for example, EAN · UCC is the mostly applied system for the unified coding of trace code and defining " identity" of agricultural products. In China, various traceability systems have been invented for supervising security of agricultural products in different provinces (cities and regions)[5-8], especially design of origin place code, for example, code of province and county + code of plot, code of administrative area + code of plot, and code of geographic coordinates. In this way, origin places of agricultural products can be defined fast and precisely, which helps take immediate measures against products with potential security problems[9-12]. However, present coding of agricultural products has also many problems such as poor encryption, overlong code length, non-transparent information about traceability for the public. In view of the above problems, combination of code of administrative area and enterprise name is applied to design code of origin place, because name of enterprise will not be repeatedly registered in the same administrative area, and the enterprise name is indicated by area code. Coding algorithms are used to realize compression of code length and multiple encryptions without breaking completeness of the coding information, specifically, compress the number of digit from 34 to 20.

Received: April 8, 2011 Accepted: June 25, 2012
Supported by National 863 Program (2008AA10Z220); Natural Science Research Program of Education Department of Henan Province (2007520020).
* Corresponding author. E-mail: yuhua_11@126.com

1 Composition of trace code

Original trace code in this study consists of 34 digits as Table 1 shows, including code of origin place, code of product, code of production date and authentication code.

Table 1 Composition of trace code

Code of origin place	Code of product	Code of production date	Authentication code
$O_1O_2O_3\cdots O_{20}O_{21}O_{22}$	$P_1P_2P_3P_4P_5$	YYMMDD	C

1.1 Code of origin place Code of origin place includes 22 digits: positional code occupies 6 of them ($O_1\cdots O_6$) which is designed on the basis of coding laws of administrative area division to locate the administrative area where the enterprise is registered; enterprise code occupies 16 of them ($O_7\cdots O_{22}$), according to the enterprise naming laws, key words of the enterprise name is taken to represent the enterprise, in this case, 4 key words are taken from the enterprise name for the coding of area code, and 1 Chinese character has only 1 set of section code (so there are 16 digits in total, add 0 at right if less than 16). By searching name of enterprise in the administrative area, the production enterprise will be defined. For example, Beijing Glorious Land X X Co., Ltd. was registered in Chaoyang Branch of Beijing Administration for Industry and Commerce, administrative area code of Chaoyang District is 110105, thus location code in the trace code of agricultural products made by this enterprise is 110105. Key words of the enterprise name are " Glorious Land" (Jin Xiu Da Di in Chinese), and correspond-

ing area codes of these 4 Chinese characters are respectively 2985, 4869, 2083 and 2156, thus the 16 digits of enterprise code is 2985486920832156.

1.2 Code of product Code of product consists of 5 digits, among which category occupies 1 digit (P1) because agricultural products are traditionally categorized into 7 categories, there are still numbers left for future expansion besides the 7 numbers for these existing categories (Table 2); Subcategory occupies 2 digits (P2P3), the 2 digits of self-increment serial number have 99 coding combinations which can satisfy needs of future subcategory expansion based on biological and technological development; Type also occupies 2 digits (P4P5), self-increment serial number is used to indicate types of each subcategory and able to meet the needs of future expansion.

Table 2 Category coding of agricultural products

Code	Category
1	Grain and oil
2	Vegetable
3	Fruit
4	Flower
5	Forest products
6	Livestock products
7	Aquatic products
8	Other agricultural and sideline products
9, 0	Standby application

1.3 Code of production date Code of production date consists of 6 digits (YY/MM/DD), and their corresponding coding ranges are given as below: YY covers numbers between 11 and 50, indicating the range from 2011 to 2050; MM between 01 and 12, indicating the range from January to December; DD between 01 and 31, indicating the range from the first day to the 31st day of a month.

1.4 Authentication code Authentication code is an important index for measuring quality of agricultural products, thus it must be taken into the coding, digit 1 – 4 (C) are used to indicate authentication of green agricultural products, organic agricultural products, pollution-free agricultural products and other authentications respectively.

2 Algorithms of multiple encryptions

To ensure security of trace code and also proper length of code, encryption algorithms are needed for the compression and encryption of part of the code, and then the anti-counterfeiting multiple check code is finally generated according to characteristics of overall coding.

2.1 Encrypted algorithms of code of origin place Code of origin place includes 22 digits, it is conversed according to the following algorithms for better encryption and shorter code length.

2.1.1 Conversion of decimal system to quaternary system. The quaternary system uses 4 digits of 0, 1, 2 and 3, and the corresponding relationship between quaternary system and decimal system is shown in Table 3. The quaternary number of 2 digits is able to represent the decimal number 0 – 9. In this study, only the first 21 digits are conversed, thus the 22 digits of original code of origin place are conversed to $21 \times 2 + 1 = 43$ digits.

Table 3 Corresponding relationship between quaternary and decimal coding

Quaternary	Decimal
00	0
01	1
02	2
03	3
10	4
11	5
12	6
13	7
20	8
21	9

2.1.2 Section classification. Original code of origin place (42 digits) before conversion is classified into 3 sets with 14 digits in each, and code conversion of each set is carried out respectively. Each 14 digits are processed as 7 items (each consists of 2 digits, that is, decimal relationship), indicated by A – G. According to the quaternary coding laws in Table 4, each set of 14 digits will find its own section based on the range from A to G in Table 4.

Table 4 Section classification of each set

A – G section range	Corresponding identification code of the section
00 00 00 00 00 00 00 – 03 21 21 21 21 21 21	1
10 00 00 00 00 00 00 – 13 21 21 21 21 21 21	2
20 00 00 00 00 00 00 – 21 21 21 21 21 21 21	3

2.1.3 Defining conversion relationship between items. The conversion relationship indicates something like the multiple relationship among "hour", "minute" and "second", for example, 1 hour is the 3,600 multiples of 1 second, and 1 minute is the 60 multiples of 1 second. In this study, "A" – "F" is supposed respectively as the 13, 11, 9, 7, 5, 3 multiples of "G".

2.1.4 Defining section. When the section is divided, each set should find its own section first before the code matrixing. According to Table 5, if the code section is 1, A should minus 00; if the code section is 2, A should minus 10; if the code section is 3, A should minus 20.

2.1.5 Code conversion. When the section is defined, 14 digits of the code are conversed to numbers indicated by "G" according to multiples of each item, specifically, relative section code of each set (3 digits, add 0 at left if less than 3) plus 1 section identification code, so each set of 14 digits is shortened to 4. Three sets means 12 digits, plus the 22nd digit of original code of origin place, the conversed code of origin place consists of 13 digits.

2.1.6 Check code generation of code of origin place. The conversed code of 13 digits includes 3 section identification codes, they are all numbers between 1 and 3; the first 2 sets of

section identification codes constitute a check code of 1 digit, which shortens the code length and facilitates the encryption. Specifically, the first 2 sets of section identification codes are permutated and combined to 9 codes as Table 5 shows, thus the corresponding check code (1 digit) is obtained and placed before the 3rd set of code. One-digit section identification code of the 3rd set is remained to generate the overall check code. Finally code of origin place (12 digits) is obtained through conversion.

Table 5 Check code combinations of code of origin place

The 1st set of section identification code	The 2nd set of section identification code	Check code
1	1	1
1	2	2
1	3	3
2	1	4
2	2	5
2	3	6
3	1	7
3	2	8
3	3	9

2.1.7 Example. Beijing Glorious Land XX Co., Ltd. is still taken for example, code of origin place of 22 digits is 1101052985486920832156, the first 21 digits is conversed to 01010001001102 21201110201221 02002003020111; taking 01010001001102 for example, this set belongs to section 1 according to 01(A); the conversed code is $(01-00)\times13+01\times11+01\times7+11\times3+02=66$, thus the first set of code is conversed to 066(1).

The code of origin place is obtained as 066(1)559(3)251(1) according to the above method, digits in brackets are section identification codes. The first 2 identification codes are taken as 13, the check code is obtained as 3 according to Table 5, thus the final code of origin place is 0665593251(1)6.

2.2 Encrypted algorithms of production date code Code of production code is obtained by combining relative section code and section identification code, and the specific classification of sections is shown in Table 6.

Table 6 Section classification of production date

Section range	Corresponding identification code
Jan. 1, 2011 – Dec. 31, 2016	1
Jan. 1, 2017 – Dec. 31, 2022	2
Jan. 1, 2023 – Dec. 31, 2028	3
Jan. 1, 2029 – Dec. 31, 2034	4
Jan. 1, 2035 – Dec. 31, 2040	5
Jan. 1, 2041 – Dec. 31, 2046	6
Jan. 1, 2047 – Dec. 31, 2050	7

It is similar to the conversion of code of origin place, the multiple relationship among "year, month and day" is no longer used, but "year" and "month" is supposed as 5 and 3 multiples of "date" respectively, so the conversed relative section code consists of 2 digits (if there is only 1 digit, add 0 in the teft side). Section is defined according to Table 7, if the coding section is 1, the "year" will have to minus 2011; if the coding section is 2, the "year" will have to minus 2017 and so on. For example, April 18, 2011 is defined as section 1 according to the year, its conversed relative section code is $(2011-2011)\times5+04\times3+18=30$, thus the conversed code of production date is 30(1). Based on the above algorithms, the code of production date (6 digits) is conversed to the one of 3 digits.

2.3 Generation and conversion of check code One identification code in the 3rd set of code of origin place is a number between 1 and 3, and that of code of production date is a number between 1 and 7; authentication code is a number between 1 and 4, such 3 numbers have 84 permutations and combinations as Table 7 shows. In the coding, the check code of 2 digits can be figured out according to these combinations, which further encrypts the overall trace code and shortens the code length.

Table 7 Combinations of check code

The 3rd set of identification code of origin place	Identification code of production date	Authentication code	Check code
1	1	1	01
1	1	2	02
1	1	3	03
1	1	4	04
1	2	1	05
1	2	2	06
...	...	...	...
3	7	3	83
3	7	4	84

3 Case study

Basic information about a batch of agricultural products of Beijing Glorious Land XX Co., Ltd. is given as below:

Enterprise name: Beijing Glorious Land XX Co., Ltd.

Administrative area: Chaoyang District

Category of agricultural product: Vegetables

Subcategory of product: Melons

Name of product: Cucumber

Date of production: April 18, 2011

Authentication: Pollution-free agricultural product

According to descriptions in "1", its code of origin place is 1101052985486920832156, and according to the methods in "2.1", the code of origin place can be conversed to 0665593251(1)6; auto-increment serial number is applied for coding, melons take up the first category of vegetables, cucumber is the first category of melons, thus its product code is obtained as 20101 according to descriptions in 1.2; code of production date is 30(1) according to the methods stated in 2.2; authentication code is 3; check code is 03 according to descriptions in 2.3. By combining all the above information, trace code of this batch of agricultural products of this enterprise is obtained as 06655932516201013003, and this code of 20 digits is characterized by shorter code length and better encryption because of the multiple encryptions.

(To page 85)

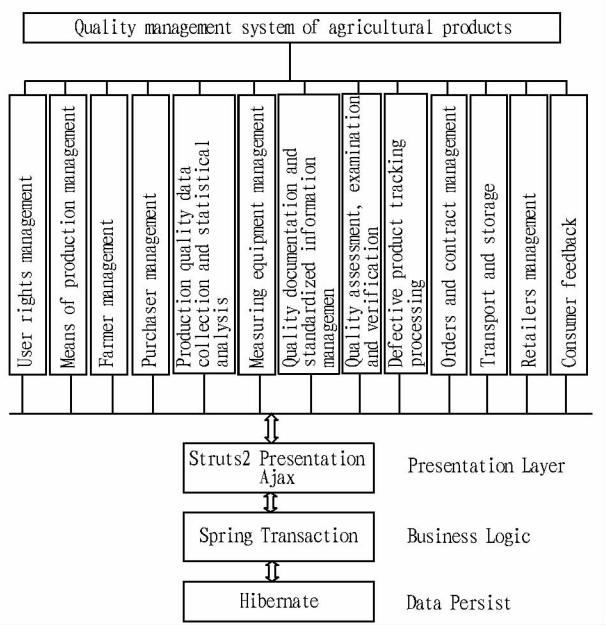

Fig.2 Framework of quality management system of agricultural product based on Spring

tem: Windows 2003; WEB server: Tomcat 6.0; Database system: Oracle 10g.

4 Conclusions

Product quality is directly related to the competitiveness, survival and development of enterprises, and constantly promoting quality management system to adapt to enterprises' daily production and business needs, can greatly enhance the competitiveness of enterprises.

Due to uncertainty in time and technical factors, as well as day-to-day business, there are many shortcomings in the quality management system of agricultural products based on Spring designed by this study. But we can also adopt some measures to continuously improve this system, so as to improve the competitiveness of agricultural enterprises, such as embedding Jfree into the framework to generate the histogram of qualification rate of products, and adding the module of online video training for farmers.

References

[1] TANG XQ. Computer-aided quality management system[J]. China Quality, 2001(3): 34 –37. (in Chinese).
[2] SONG M. The development and research of enterprises quality information software system[J]. Journal of Hefei University of Technology, 2005(5): 72 –73. (in Chinese).
[3] WANG XB. Integration of JavaEE multi-layer frame Struts2 + Spring3 + Hibernate3 + Ajax[J]. Dalian Maritime University, 2009(9): 101 – 104. (in Chinese).

(From page 82)

4 Conclusions

This study by applying algorithms of multiple encryptions converts 22 digits of origin place to 12, 6 digits of production date to 3 through system conversion and sector classification, which can not only improve the encryption but also shorten the code length. Furthermore, 1 identification code of origin place and that of production date code as well as authentication code are permutated and combined to an overall check code of 2 digits, which further compresses and encrypts the trace code.

The trace code of 20 digits proposed in this study provides users key information about enterprises and agricultural products with out the need to consult databases for defining the code, thus production enterprises will be found out quickly and precisely in case of any quality problem, and corresponding measures can be taken timely. Moreover, information of the production enterprise is shown clearly by area code, so the public will know that without consulting databases, they can take preventive measures and will never be left in panic, which to some extent is favorable for the construction of a harmonious society.

References

[1] Cate World. 2010 food safety incident[EB/OL]. (2010 –07 –14). http://www.meishichina.com/News/HangYe/201007/85441.shtml. (in Chinese).
[2] YANG XT, SUN CH, QIAN JP, *et al.* Design and application of bar code traceability label under food safety control[J]. Chinese Agricultural Science Bulletin, 2006, 22(5): 98 –101. (in Chinese).
[3] SHEN GR, ZHAO XD, HUANG DF. Consideration of farm product safety system in China[J]. Journal of Shanghai Jiaotong University: Agricultural Science, 2005, 23(1): 77 –83. (in Chinese).
[4] YANG TH, CHU BJ. Study on control system of food safety from farm to table[J]. Food Science, 2005, 26(3): 264 –268. (in Chinese).
[5] LIN L, ZHOU DY, HUANG QJ. Design of food quality and safety traceability systems based on Internet[J]. Journal of Hefei University of Technology: Natural Science, 2005, 28(5): 546 –549. (in Chinese).
[6] LIU ZG, LING J, HE XT, *et al.* Design and implementation of traceable code for quality and safety of farm product[J]. Computer and Modernization, 2009(9): 125 –128. (in Chinese).
[7] LIU XM, ZHANG HL, LIU YD. Research on farm product quality and security traceability system[J]. Hubei Agricultural Sciences, 2009, 48(8): 2001 –2003. (in Chinese).
[8] MENG M, LIANG WH, SONG QD, *et al.* Coding research of circulation code and back yards of agricultural products[J]. Chinese Journal of Tropical Agriculture, 2010, 30(1): 82 –85. (in Chinese).
[9] QU XH, ZHUANG DF, QIU DS. Studies on GIS based tracing and traceability of safe crop product in China[J]. Agricultural Sciences in China, 2007, 6(6): 724 –731.
[10] DENG XF, LV XN, ZHENG SY, *et al.* GIS-based agricultural products safety traceability system[J]. Transactions of the Chinese Society of Agricultural Engineering, 2008, 24: 172 –176. (in Chinese).
[11] YANG XT, QIAN JP, ZHANG Z, *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).
[12] LING J, XIE R, HE XT. On .net-based food quality and safety tracing technique and its implementation[J]. Computer Applications and Software, 2010, 27(1): 145 –147. (in Chinese).