An Optimized Encryption Algorithm of Fruit And Vegetable Product Traceability Code Based on Embedded System

Shile Mu*, Jiamin Wang, Yue Qi, Jianying Tian
ShanDong Institute of Commerce and Technology No.4516, Lvyou Road, Jinan 250103, China

*285997555@qq.com

Abstract. The quality and safety of fruits, vegetables, and other agricultural products is the lifeline of agricultural development. In recent years, the state departments concerned have strengthened the whole process block on the quality of fruits and vegetables, continuously optimized the measures, and continuously improved the quality control level of fruits and vegetable products. Traceability code is the key technology to realize the whole process block and traceability of the whole industry chain. There is a risk that the traceability code will be modified privately in the application process. Once the traceability code is cracked and modified, its important role in the traceability system will be destroyed. In order to prevent the traceability code from being arbitrarily modified, this paper designs and studies an optimization algorithm of traceability encryption based on an embedded system.

Keywords: Intelligent Agent, University Education, New Infrastructure, Man-machine Integration

1. Introduction
The safety of fruit and vegetable products is related to the health and life safety of the broad masses of people, economic development, and social stability. Now it is urgent to build a whole chain of fruit and vegetable product traceability systems to ensure the safety of fruit and vegetable products. Internet of things, sensors, embedded artificial intelligence, and anti-counterfeiting bar code are the key technologies to realize the traceability system of fruits and vegetables. Based on the embedded fruit and vegetable product traceability code as the encoding method, the advanced encryption standard (AES) algorithm is improved, and a fruit and vegetable product traceability code encryption algorithm is designed, and the algorithm is transplanted to the data intelligent acquisition and convenient query equipment, realizing the dynamic change of the key and the uniqueness of the traceability code on the embedded platform, so as to play the anti-counterfeiting function.

2. Algorithm principle
In order to prevent the traceability code from being modified privately, an encryption algorithm should be adopted to compress and encrypt the traceability code of fruits and vegetable products when designing the traceability code. The choice of encryption algorithm should be determined according to the characteristics of use. Because the speed of asymmetric encryption algorithm is much slower than that of a symmetric encryption algorithm, when we need to encrypt a large number of data, we suggest...
using the symmetric encryption algorithm to improve the encryption and decryption speed. Because of the fast speed of the symmetric encryption algorithm, and the AES algorithm is the latest advanced encryption standard. Compared with DES and 3DES in the symmetric encryption algorithm, it has the advantages of fast speed, high security, and low resource consumption, so the traceback code encryption algorithm in this paper is based on the AES encryption algorithm[1].

Advanced Encryption Standard (AES) is the next generation encryption algorithm standard with high speed and high-security level. It is the Rijndael algorithm designed by Belgian scholars Vincent Rijmen and Joan Daemen. It is the encryption algorithm with the best encryption performance and speed in the symmetric encryption algorithm. Its prototype is a square algorithm, and the design strategy is a wide trajectory strategy, which can improve the ability of the algorithm to resist differential cryptanalysis and linear cryptanalysis.

3. Research on grouping encryption technology of fruit and vegetable product traceability code

Because the computer is suitable for processing hexadecimal number (i.e. binary), AES encryption algorithm is for hexadecimal number encryption. At present, most of the agricultural products traceability code codes are composed of decimal numbers between 09, and the number of traceability codes is required to correspond to the encrypted ciphertext bits, that is, there is no ciphertext extension, AES encryption algorithm based on hexadecimal can not meet the above requirements. AES algorithm needs to be improved to meet the encryption requirements of fruit and vegetable product traceability code[2].

3.1. Traceback code packet compression

According to the above coding rules, each code segment is recoded and compressed by the grouping method. The basic idea of coding compression is to redesign each code segment according to the maximum value range by the exhaustive method. Among them, the check code is calculated by the manufacturer identification code and product batch number code, which can be ignored in compression; there are about 2800 county-level administrative divisions, so four decimal digits are used; the enterprise sequence number remains unchanged; the fruit and vegetable product classification code use three decimal digits to represent 1000 mainstream varieties, which can fully meet the application needs of fruit and vegetable products; the source entity code is enterprise base number remains unchanged; according to the law of the people's Republic of China on quality and safety of agricultural products, the storage time of agricultural product records is generally 2 years, and the production date code time span here is calculated as 100 years, which is enough to meet the requirements of agricultural product quality traceability. Based on January 1, 2000, as the benchmark, the difference between the current production date and the base date can be expressed by using 5-digit decimal numbers the number of days. The specific code conversion is shown in Figure 1.

![Fig.1 Grouping compression of fruit and vegetable product traceable block code](image)

3.2. Traceback code encryption technology

The compressed fruit and vegetable product traceability coding adopts the grouping compression method, which reduces the coding length, but its security and anti-counterfeiting performance are poor.
It needs to be encrypted, and it needs to keep the length unchanged before and after encryption. Through the analysis of the AES algorithm, we can see that the AES encryption algorithm can not meet the requirements of decimal data encryption. On the basis of Liu Lianhao's design method, this paper improves the AES algorithm, redesigns four encryption operations in the AES algorithm, namely, ByteSub, shift rows, MixColumn, and add rounds, to adapt to the direct decimal number encryption requirements. At the same time, in order to enhance the encryption strength, ensure the uniqueness of the generated traceability code, make the same plaintext generate irregular ciphertext, and achieve the anti-counterfeiting effect of once secret, the dynamic key is used to encrypt the fruit and vegetable product block code randomly[3].

In this algorithm, the packet length and key length can be specified independently, and the number of key rounds can be arbitrary. The more rounds, the higher the encryption degree, the longer the operation time. The scheme adopts 12 rounds encryption strategy. Each round of transformation consists of three layers

Linear mixing layer: it includes the state bit row shift and column mixing of traceability code, which is to ensure the high diffusion of multi-round iterative operation.
Nonlinear layer: it is composed of a 10 base S-box, which plays the role of confusing the number position of traceability code.

Round key control layer: according to different conditions, the round key and the traceability code state corresponding to the number of modular operations, realize the key and traceability code word mixing.

3.3. Key steps
The algorithm includes the following key steps.

3.3.1. Tracing code dynamic key generation
According to the three factors of device initial key, device ID, and traceability code encryption times time, the dynamic key dkey of a 32-bit decimal number is dynamically generated each time. The introduction of a dynamic key makes the encryption strength higher. Different dynamic keys are used to encrypt each traceback code. The dynamic key random algorithm is controlled by time. The difference of time in binary value makes the dynamic key generated completely different.

Traceability code status bit replacement traceability code status bit replacement is to replace the original traceability code status matrix with a new state matrix through the status bit replacement table. In each round of digital position change, half of the decimal digits can be changed[4].

The state matrix row shift of traceability code here refers to the state matrix replaced by the previous step, and its state bit row shift rules are as follows: the first line does not move, the second line circularly shifts left by 1 bit, the third line circularly shifts left by 2 bits, and the fourth line circularly shifts left by 3 bits.

3.3.2. Column mixing of traceability code state matrix
The mixed operation of the traceability code state matrix column is that a reversible positive integer matrix is used to multiply the traceability code state bit matrix to the left, and then modulus operation is performed on 10, and the result is put back into the original matrix.

3.3.3. Round key operation control
In the AES encryption algorithm, round key addition uses the key and the byte corresponding to the state to do XOR operation. But for decimal numbers, XOR is not reversible. In order to make the status bit of traceability code confused with the round key and have reversibility, the binary XOR in the AES algorithm is changed into the round key operation control based on the decimal number. [5]According to the different keys of each round, one of the four operations is carried out. The entry condition is determined by the sum of all the bits of the key used in each round of encryption and takes the modulus of 4. The operation steps of each round are described as follows:
32 Sum of bit dynamic key, denoted as a sum;
The entry parameter enter = sum mod 4;
According to the result, enter different state bits and round key addition and subtraction operations.

4. Conclusion
The short block encryption algorithm based on AES is the basis of the whole fruit and vegetable product traceability code encryption, and its security has an important impact on the whole application. Through the test of the algorithm, according to the security requirements of practical application, the test scheme is designed and the automatic calculation test of the diffusion ability of the encryption algorithm is realized. The diffusion ability of the algorithm plays an important role in the realization of the fruit and vegetable product traceability system. The 20-bit decimal traceability code is tested for 2 to 16 rounds of encryption and decryption operation. Here are the test results of 20 decimal numbers for encrypted packets.

When the plaintext of the traceability code is changed, the diffusion rate of comparison between ciphertexts of traceability code is changed. That is, the same key encrypts different plaintexts, and the ciphertexts obtained are compared with each other, and the ratio of each bit between ciphertexts is different. The higher the value, the smaller the correlation between ciphertexts, which can effectively prevent the attack of ciphertext correlation analysis.

When the encryption rate changes between cipher codes. In other words, different keys are used to encrypt the same plaintext, and the ratio of each bit between ciphertexts is different. The higher the value, the less correlation between ciphertexts. It can effectively prevent the user from intentionally or unintentionally inputting the ciphertext and solving the correct plaintext.

The diffusion rate of comparison between the plaintexts of traceability codes is changed. In other words, the same key decrypts different ciphertexts, and the plaintext obtained is compared with each other, and the ratio of each bit between plaintexts is different. The higher the value, the smaller the correlation between plaintexts, which can effectively prevent plaintext correlation analysis attacks.

When the encryption key is changed, the diffusion rate of comparison between encoded plaintexts is traced back. In other words, different keys are used to decrypt the same ciphertext, and the ratio of each bit between plaintexts is different. The higher the value, the smaller the correlation between plaintexts, which can effectively prevent plaintext correlation analysis attacks.

References
[1] G A Kabatiansky 2019 Traceability Codes and Their Generalizations 55(3) pp 283-294
[2] Zhou Sh J 2017 Technical specification for coding of food quality and safety traceability code DB 35/T 1711 Interpretation of local standards
[3] Chong SG, Jingxue M and Gennian G. 2018 New upper bounds for parent-identifying codes and traceability codes 86(8) pp 1727-1737
[4] Shahbaz K, Mohd I K and Abid H 2018 Selection of Traceable Technology in Food Supply Chain 404(1)