https://doi.org/10.1051/e3sconf/202123301082

Research on Two Dimensional Code Encryption Method Based on Embedded Device

Wenchao Xu[1,a,*], Haiyun Gong[1] and Daitao Wang[1]

[1]South China Institute of Software Engineering GU, Department of Electronic Studies, 510990, Guangzhou, China

Abstract. As the carrier of information storage, the generation standard and identification method of two-dimensional code are shared. A set of unified standards used, but without corresponding encryption measures, it is difficult to ensure that the two-dimensional code information will not be attacked and tampered by criminals in the process of transmission, resulting in information security risks. With the intellectualization of embedded devices, two-dimensional code has found an increasingly wide application, but its safety issue is becoming more and more prominent. This paper proposes a two-dimensional code encryption method based on embedded devices. In this paper, AES symmetric encryption algorithm which ensures both encryption and decryption speed and security is selected to encrypt the two-dimensional code. Key expansion with the traditional AES encryption algorithm has some flaws in that once a key in one of the rounds is intercepted, the previous and the following subkeys will be calculated through fixed algorithm. Random function is used to improve the generating algorithm of expanded keys, hence enhancing the anti-attack ability of the encryption algorithm. By putting random function and g function into Cloud for operation, the speed of encryption and decoding QR code of the embedded device is increased. The test results show that the system designed in this paper can effectively hide the information contained in the QR code picture, which shows that this method ensures high security.

1 Introduction

With the popularization of embedded devices, QR code, as a technique of automatic identification and information carrier for digitized information, is widely used in people’s daily life. Typical examples are mobile payment, e-card, ticketing management and product tags, etc. QR code mainly deals with information carrier and error correction, but it does not take information encryption into account. As a consequence, QR code can easily be tampered, carry Trojan or virus, which are indistinguishable to naked eyes. Therefore, fields involving personal sensitive information require encryption of QR code. If encryption technique is added in the generative process of QR code, even if it is tampered, the tampered code cannot be recognized by the terminal because the attacker does not know the encrypted key. For this reason, research on the safety of QR code has become a topic of vital importance.

This paper, based on the characteristics of embedded devices, is devoted to analyzing and studying the process of encryption and decryption of AES encryption algorithm by selecting QR code as information carrier. Then, on the basis of this, according to the needs of the encryption system of QR code, it conducts in-depth analysis on the defects of AES algorithm, and makes optimal design to enhance its safety.

2 Relevant Techniques of QR Code

QR code is a kind of barcode technology. Also called two dimensional bar code, it can store information both horizontally and vertically. From the perspective of components configuration, QR code may be viewed as a picturized matrix. It was first created by the Japanese. It stores data information in a matrix of some geometric pattern by arranging black and white little squares in accordance with different rules. Data information is express with black and white geometrical features corresponding to binary system. Besides, it has error correcting capability[1]. To read QR code information, identification equipment or optoelectronic scanning devices should be used to recognize the information so as to read and process QR code information. Paperless transmission is possible if QR code is used as the carrier of information transmission. With the popularization of smartphones, use of CR code is a frequent occurrence[2]. Thus, it is clear that CR code is very popular among the people.

2.1 Matric QR Code

Matrix two-dimensional code, based on matrix, is formed through permutation and combination of black and white squares. Each square is equal in length and

[a] 253655860@qq.com

width and the whole image is square-shaped. Matrix two-dimensional code adopts the code system of character recognition processing. After data coding, black and white squares are arranged to encode in the interior of the matrix in accordance with some rule. Generally, it has error correcting capacity. A representative matric two-dimensional code is QR(Code Quick Response Code). It is a quick response matrix code, a matric two-dimensional code[3] put forward in 1994 by Denso Wave, a Japanese company. It can be seen from Fig 1 that QR Code has three concentric squares chequered with black and white. It is a shape for position detecting. It is the key identifier of QR code, enabling the device to position and recognize the two-dimensional code in a short period of time. Besides, the code can be read from any angle. It can be recognized at a high rate of speed without adjusting the angle of the geometric figure [4].

QR code has a set of unique mechanism for correcting errors. In addition, supporting Chinese character code with high information density, it may hold 7,089 Chinese characters at most. Therefore, QR code is the most widely used two-dimension code in people's daily life.

Fig. 1 QR Code

3 Two- Dimensional Code Encryption

In the process of two-dimensional code encryption and decryption, we all know that encryption key is required for encryption while decryption key for decryption. Depending on whether the encryption key bears relationship to the decryption key, encryption algorithm may be divided into two categories: symmetric encryption algorithm and asymmetric encryption algorithm. The encryption key of the former and the decryption key are the same or have some relationship. Generally, one key is used to encrypt asymmetric decryption algorithm while another key is used for decryption. Generally, the encryption key is open to the public.

A asymmetric decryption algorithm has some advantages in terms of key distribution and management. It is mainly used in digital signature, identity authentication, and some other fields. As the unipolarity of the whole process of asymmetric decryption algorithm is based on complex maths problems featured by a large amount of operand, it can hardly be cracked. Nevertheless, as it is featured by low arithmetic speed and occupies a large amount of embedded memory, it is unfit for practical use. In contrast, in terms of symmetric encryption algorithm, AES, the next-generation encryption standard, can hardly be cracked. Besides, its encryption and decryption speeds are very fast, reaching tens of megabytes per second, nearly 100 times the speed of asymmetric encryption algorithm[5].If information of the same order of magnitudes is encrypted, symmetric encryption algorithm is, obviously, more applicable to embedded devices. Therefore, in the development process of embedded devices, symmetric encryption algorithm is the best choice when a great amount of data needs to be encrypted.

The QR code produced by embedded devices contains quite a great amount of information. Besides, it requires fast speed of reading. It is inadvisable to affect the use of QR code just for the sake of safety. After careful consideration, symmetric encryption algorithm is selected to encrypt the QR code. In symmetric encryption algorithm, AES Algorithm is characterized by high-level safety, high computing efficiency, simple and flexible algorithm, fast encryption and decryption, and low requirement for memory. Therefore, in this paper, AES is selected to do data encryption in QR code.

3.1 AES Encryption Algorithm

SAES (Advanced Encryption Standard) is a widely used encryption standard. In 1997, National Institute of Standards and Technology (NIST) solicited advanced encryption standards around the world. Later, the contribution of Joan Daem and Vincentive Rijmen, two experts in cryptology in the name of Rijndael, won the final victory after three rounds of selections. In 2000, NIST announced to the world that it took Rijndael encryption algorithm as the new generation encryption algorithm[6]. It was renamed AES Algorithm, so it is also called Rijndael encryption algorithm. AES Algorithm is a kind of block encryption algorithm, formed through repeated iteration of round transformation functions. Its block length can only be 128 bit, but its key length can be any of the three: 128 bit,192 bit, and 256 bit. AES Algorithm is conducted in bytes. The 128-bit data in the block are divided in bytes into 16 sections, and its encryption process is completed on a 4×4 matrix. For different key lengths, different round transformation operations are conducted. Nr (the number of times of round transformation for the key lengths corresponding to 128 bit, 192 bit and 256 bit) is 10 times, 12 times and 14 times respectively. Each round has four different process round AddRoundKey, SubBytes, ShiftRows, and MixColumns. The last round is slightly different in that it does not involve MixColumn transform operation. For each circulation, a subkey will be created by the extended key module[7].As AES is a symmetric encryption algorithm, the decryption process is the inverse process of encryption, so this paper focuses only on encryption process.

3.2 Improvement of Key Expansion

This system generates encrypted two-dimensional pictures for sensitive and confidential data. It supports various character modes such as letters, figures, bytes and Chinese characters. First, the information needs to go through round key addition operation. This process requires expanded keys which are obtained through transformation of the initial key. After that, every round of transformation and reverse-transformation requires expanded keys[8].The expanded keys in the rounds are different from each other. Traditionally, the expanded key in every round is obtained through the transformation of the expanded key in the previous round. In this paper, the expanded keys are optimized so that even if a key for one of the rounds is obtained by attackers, they cannot obtain the keys for the other rounds. This method enhances the safety of AES encryption algorithm.

3.1.1 Traditional Key Expansion[9]

To take samples of music signals, appropriate sampling frequency should be chosen. The higher the sampling frequency is, i.e, the shorter the interval time of sampling is, the more sample data of music signals one will acquire, and the more accurate the waveform of music signals will be. However, more sampling data means greater sampling data size. For this reason, the data size to be calculated will greatly increase.

The keys used in all rounds of QR code encryption and decryption are the same, which indicates that generation of expanded keys are of vital importance. The expanded keys for AES algorithm are used to expand the input 128-bit initial key (4×4 matrix) to 11 128-bit subkeys for the additional transformation of the round secret key in each round. The generating algorithm of AES's expanded keys is conducted in units of characters. One character has four bytes, and each byte has eight bits. One character has 32 bits in all, which is precisely one column of the key matrix. The key matrix has four columns in all. Therefore, AES expanded key means expanding the 4-character (128-bit) key to 11 subkeys (44 characters). Let the initial key be w (w_0, w_1, w_2, w_3),

When j%4=0 ($4 \leq j \leq 43$),

$$w_j = w_{j-4} \oplus g(w_{j-1}) \qquad (1)$$

When j%4≠0 ($4 \leq j \leq 43$),

$$w_j = w_{j-4} \oplus w_{j-1} \qquad (2)$$

g function is to make w ring shift left one byte (RotByte), and then map each byte by pressing the S box (equivalent to byte conversion SubByte). After that, make it have nonequivalence operation with 32-bit constant RCon(RC[$j/4$]). RC is a one-dimensional array, and its value is: RC {00,01,02,04,08,10,20,40,80,1B,36}. As a matter of fact, only 10 RC's values are needed. As j 's minimum value is 4, the minimum value of j/4 is 1. Here, 11 values are used. RC [0] is added to facilitate array representation in the procedure. In fact, RC [0] is not used in the operation. G function may be:

$$g(w_{j-1}) = \mathrm{SubByte}(\mathrm{RotByte}(w_{j-1})) \oplus R(j/4) \qquad (3)$$

3.1.2 Key Improvement

Traditional expanded algorithm is direct and efficient. However, it has some defects. Once a subkey for one round is intercepted and captured by an attacker, he/she may calculate the subkeys for following rounds through fixed algorithm. Then, he/she may obtain the subkeys through reverse thinking. In this sense, the subkeys for all rounds risk being cracked. Therefore, the paper is devoted to improving the algorithm[10] .

Let w (the 128-bit initial key) be w_0, w_1, w_2, w_3; the expanded subkey be w_{40}, w_{41}, w_{42}, w_{43}; In it,

Initial subkey: w_0, w_1, w_2, w_3;

Subkey for the first round: w_4, w_5, w_6, w_7;

Subkey for the second round: w_8, w_9, w_{10}, w_{11};

... ...

Subkey for the tenth round: w_{40}, w_{41}, w_{42}, w_{43};

In the cloud, using random generation function, we generate 128-bit random initial key w_0, w_1, w_2, w_3() and 32-bit random supplementary password (w_{sj}($4 \leq j \leq 43$)). Then, do the first-round expansion to the method when j%4=0 with the traditional key expansion algorithm of AES, and find g function of the subkey for the previous round. Next, do further encryption with the supplementary password. The specific implementation steps are shown as follows:

$$w_4 = w_0 \oplus g(w_3) \oplus w_{s4};$$

$$w_5 = w_1 \oplus g(w_4) \oplus w_{s5};$$

$$w_6 = w_2 \oplus g(w_5) \oplus w_{s6};$$

$$w_7 = w_3 \oplus g(w_6) \oplus w_{s7};$$

The above is the generating algorithm of the subkey for the first round. Namely, it it generated in accordance with the rule of $w_j = w_{j-4} \oplus g(w_{j-1}) \oplus w_{sj}$($4 \leq j \leq 7$). The subkey expansion for the second and the following rounds relies on the initial key, and the subkey in the previous round and the supplementary key are generated at the same time.

$$w_8 = w_0 \oplus g(w_4) \oplus w_{s8};$$

$$w_9 = w_1 \oplus g(w_5) \oplus w_{s9};$$

$$w_{10} = w_2 \oplus g(w_6) \oplus w_{s10};$$

$$w_{11} = w_3 \oplus g(w_7) \oplus w_{s11};$$

From the second round to the end, the subkeys for each round are generated from

$$w_j = w_{j-8} \oplus g(w_{j-4}) \oplus w_{sj}(8 \leq j \leq 43) .$$

We put the randomly generated function and g function into the cloud for operation. As a result, it reduces the computation burden of the embedded devices, improves the efficiency of encryption and decryption and solves the problems like freeze and even system crash of the embedded system due to the too sophisticated encryption. Meanwhile, the generating algorithm of the extended keys is improved. On one hand, a random number is chosen as the initial key to make it have strong variation ability. To this end, there is no other choice but exhaustive attack. For the 128-bit keys, even though the attacker has obtained the key for the first round, he/she, if attempting to acquire the key for the next round, need not only know the key for this round but also make assumption of the four round key characters for the previous round. As each round key has 128 bits, 2128 times of exhaustions have to be done. On the other hand, a 32-bit supplementary key is randomly added to each subkey so that the attacker cannot calculate the subkeys for the previous and following rounds through fixed algorithm. These two methods combined, cracking the key and the initial key become much more difficult.

4 Experiments

To know the differences between QR code before encryption and the code after encryption, an ordinary two-dimensional scanner is used to scan the unencrypted QR code and the encrypted code respectively. According to figure 2, the result is shown as in Table 1. It shows that the information received after scanning is in complete accord with the input raw information, which means that the system program of generating QR code through QR encoding has no problem. However, when the encrypted QR code is scanned with the ordinary two-dimensional scanner or scanning software, messy codes are found. This indicates that the two-dimensional code encryption method we design is a success. Our method helps to protect the data information contained in the symbols of two-dimensional code, thus ensuring its safety in the process of information dissemination.

(a) Unencrypted QR code (b)Encrypted QR code

Fig. 2 QR Code

Table 1. Test of QR Code Encryption

QR Code	Unencrypted QR Code	Encrypted QR Code
Scanning Result	South China Institute of Software Engineering GU	error

To test the effectiveness of this method, four kinds of frequently-used character modes are used: figures, alphanum, 8-bit bytes and Chinese characters to test the identification results and time. It is shown in Table 2.

Table 2. Identifying Test Data with This Method

Original Data	Our Method	
	Identifying Result	Identifying Time /ms
0123456789	0123456789	891
Abcdefghizk	Abcdefghizk	887
567*efg@?	567*efg@?	936
QR Code Encryption Method	QR Code Encryption Method	903

The test data in Table 2 indicates that this method used, the encrypted QR codes can be correctly read. This shows that the two-dimensional code encryption method designed in this paper is reasonable. It is found in the process of testing the time of two-dimensional code decryption that all is completed within one second, hence satisfying the practical needs in real life.

5 Conclusion

This paper proposes a two-dimensional code encryption method based on embedded device. First, the raw information of QR code is encrypted, and QR encoding is done to ensure the safety of the QR code data. Second, according to the requirements for encryption and decryption of QR code, relevant functions are put into the cloud for operation, hence improving the operating efficiency of the device. Next, AES symmetric encryption algorithm, which ensures encryption and decryption speed, is selected to encrypt QR code. On the other hand, expanded key based on the traditional AES encryption algorithm has defects in that once the key for one round is intercepted, the attacker may calculate the keys in the previous and following rounds through fixed algorithm. Therefore, improvement is made in expanded key generating algorithm with random functions. As a result, the anti-attacking ability of encryption algorithm is enhanced. Test results indicate that the system designed in this paper can effectively hide the information contained in QR code pictures. Thus, it is clear that this method boasts high-level safety.

Fund project

Foundation for Young Innovative Talents in Higher Education of Guangdong, China (No.2018KQNCX389).

References

1. Yaojun Shan, Jin Bai, Xiaoqian Ye, Wei Li. Application of QR Two-dimension Code Technology in Credits Certification System[A]. Information Engineering Research Institute, USA. Proceedings of 2013 the Second International Conference on Innovative Computing and Cloud Computing (ICCC 2013) [C]. Information Engineering Research Institute, USA,2013,3.

2. Kuan-Chieh Liao, Wei-Hsun Lee, Min-Hsuan Sung. A One-Time Password Scheme with QR-Code Based on Mobile Phone[J]. IEEE Conference, 2014,24(3): 2069-2071.
3. Huang Zhenjian & Cai Qunying, Application of QR Code Encoding and Decoding Based on Web[J], Computer Knowledge and Technology, 2014, 10(24): 5671-5672.
4. Yong-feng Huang, Zhen Xue, Cai-rong Yan. Research of Localization Algorithm Based on Multi-QR Code[A]. Research Institute of Management Science and Industrial Engineering. Proceedings of 2017 2nd International Conference on Automation, Mechanical Control and Computational Engineering (AMCCE 2017) [C]. Research Institute of Management Science and lndustriai Engineering, 2017, 4.
5. Jia Xu, Saftey Analysis and Its Optimization and Improvement of AES Algorithm [D]. Jilin University, 2010.
6. LiQuan Han, Fang Yuan, ZhengChao Xu. A strong-security protocol based on AES algorithm for passive RFID tags[A]. Information Engineering Research Institute, USA. Proceedings of the 2014 Pacific-Asia Workshop on Computer Science in lndustrial Application (ClIA201 4) [C]. Information Engineering Research Institute, USA, 2014, 7.
7. Zhang Xiaoyu, Chen Kaiyan, Zhang Yang, Gui Weilong, Li Lei. Correlation power analysis for AES encryption device[A]. International Informatization and Engineering Associations, Atlantis Press. Proceedings of 2015 4th National Conference on Electrical, Electronics and Computer Engineering (NCEECE 2015) [C]. International Informatization and Engineering Associations, Atlantis Press,2015,7.
8. Ren Wenping, Zhang Wenyong, He Jiqin, Shen Dongya. An improved method about AES and FPGA high-speed realize[A]. lEEE Computer Society. Proceedings of 2016 IEEE International Conference of Online Analysis and Computing Science (ICOACS 2016) [C].IEEE Computer Society, 2016, 4.
9. Zhou Jiahua, Design and Implementation of QR Code Encryption System Based on ARM [D]. Fuzhou University, 2018.
10. Zhang Xiaomei, Optimization and Implementation of AES Algorithm in the ARM Embedded System [J]. Computer Application and Software, 2012, 29(05): 285-288.