information

Article

Implementation and Performance of Face Recognition Payment System Securely Encrypted by SM4 Algorithm

Yukun Zhou [1], Ningsheng Wu [1], Baidong Hu [2], Yitao Zhang [3], Jingyun Qiu [1] and Weiming Cai [4,*]

[1] Applied Engineering College, Zhejiang Business College, Hangzhou 310053, China; zhouyukun06@sina.com (Y.Z.); wns_zjbc@163.com (N.W.); qjy870125@163.com (J.Q.)
[2] Hangzhou Sunyard Technology Co., Ltd., Hangzhou 310053, China; hbd128@126.com
[3] College of Control Science and Engineering, Zhejiang University, Hangzhou 310058, China; yitz@zju.edu.cn
[4] School of Information Science and Engineering, NingboTech University, Ningbo 315100, China
* Correspondence: caiwm@nit.zju.edu.cn

Abstract: Face recognition payment is a new type of payment method, with AI face recognition technology as the core, and its speed and convenience are more in line with the users' payment habits. However, the face is a biological feature with weak privacy, and the protection of user information security is particularly important. At present, face payment technology still has security risks, and the data transmitted during the transaction process are vulnerable to attacks. Aiming at the security problems in the payment process, a payment system that is jointly encrypted by the SM4 algorithm and the face liveness detection algorithm was proposed in this paper, which supports a variety of communication methods. The hardware platform adopts an octa-core 64-bit ARM processor with a main frequency of 1.8 GHz, which has powerful computing and processing capabilities. Based on the Android intelligent operating system, the development environment is more secure and convenient. It is also equipped with a liveness detection 3D structured light camera, which dynamically collects face information and accurately analyzes the characteristics of living bodies. Through the data encryption and decryption test and face performance index detection, the expected effect of the system was achieved, which greatly improved the performance of the face payment system currently studied. The SM4 encryption algorithm improved the running rate of encrypted data and the security of face transaction data transmission, the face detection algorithm improved the accuracy of living body feature recognition, and the payment system effectively improved the accuracy and security of face payment.

Keywords: SM4 algorithm; data security; face recognition; cryptographic protocols; product codes; embedded software

Citation: Zhou, Y.; Wu, N.; Hu, B.; Zhang, Y.; Qiu, J.; Cai, W. Implementation and Performance of Face Recognition Payment System Securely Encrypted by SM4 Algorithm. *Information* **2022**, *13*, 316. https://doi.org/10.3390/info13070316

Academic Editor: Gholamreza Anbarjafari (Shahab)

Received: 27 May 2022
Accepted: 26 June 2022
Published: 28 June 2022

1. Introduction

Face recognition technology is the fastest growing technology in the biometric field, and is widely used in the field of mobile payment. At present, there are three representative payment institutions: Alipay, WeChat, and UnionPay [1]. For users, whether it is the current mainstream Alipay, WeChat scan code payment, or NFC payment such as Apple Pay and Cloud QuickPass, as long as it is convenient way to pay, it is very popular. Face payment uses biometric technology to replace traditional passwords by "scanning your face" in the payment stage, optimizing the payment process, effectively improving the daily consumption experience of users, improving the transaction efficiency of merchants, and driving the development of various industries. Face payment application involves the direction of capital flow and so on, to ensure the security of user data transmission, which requires a payment system to have a high security performance guarantee. The SM4 algorithm is a dedicated block cipher algorithm used in wireless local area networks and trusted computing systems, and is a commercial cipher algorithm issued by the State Cryptography Administration [2]. It has the same key block length as the AES algorithm,

and the security is higher than that of the 3DES algorithm. Compared with other encryption algorithms, the SM4 encryption algorithm is more efficient and convenient in resource saving and design implementation. It is more resistant to related key linear cryptanalysis and has higher security [3]. Therefore, the SM4 algorithm is used in the encryption module of the payment system, which can effectively improve the overall encryption level.

In recent years, there have been many studies on face detection algorithms such as the algorithms based on deep learning, convolutional neural network multi-feature fusion, and the hybrid feature extraction algorithm based on wavelet transform, and improved principal component analysis, these were mentioned in [4–6] to ensure the security of face recognition. However, when face recognition is applied to payment systems, it is not only necessary to ensure the security of face detection, but also the security of the data transmission and transactions in payment systems. At present, there are few such studies such as in [7]. The improvement in the network, host, etc. and binocular liveness recognition algorithm can improve the security of the payment system. However, the SM4 algorithm encryption system is more convenient and secure than the improvement in the hardware physical facilities. The security encryption algorithm was applied in [8], but was mainly used to encrypt face data to ensure the security of image recognition, and the encryption algorithm was not used in payment. As the systems studied in our paper are more specific and efficient than those studied in [7,8], this not only ensures the security of face data detection, but also ensures the security of transaction data transmission, realizes various performances of the payment system, and presents customers with a new interactive experience of face recognition and intelligent payment.

This paper expounds the system performance and advantages from the aspects of the overall system architecture, hardware design, software design, key management mechanism, SM4 algorithm performance, running rate, face system architecture, and detection pass rate. In the research plan, the system development environment, storage space, and core processor were upgraded, the main frequency and performance were improved, and the power consumption and cost were reduced, making it suitable for multi-scenario applications. The built-in security encryption module of the system makes the transmitted data resistant to linear attacks and differential attacks, and has the characteristics of preventing the use of the exhaustive detection of payment passwords. The peripheral driver software can be rapidly developed and transplanted, and each module of the hardware platform can be operated through the function interface. The storage system has a load balancing mechanism to prevent frequent erasing and writing operations. The security module encrypts and stores the internal EEPROM data of the chip in ciphertext so that sensitive data cannot be externally obtained. The hardware adopts the technology of "disassembly and self-destruction" (when the cover is detected, all keys will be destroyed) to ensure the security of the system. In terms of resisting side channel attacks and preventing fault injection, the system adopts hardware encryption [9–11]. The hardware true random number generator generates the key or the key seed, which overcomes the disadvantages of the data encryption system using the general algorithm and software pseudo-random numbers. The M-sequence scrambling mechanism is used to process the true random sequence to ensure that the quality of random numbers is not affected by physical noise sources. The software adopts "firmware encryption and self-checking" (any data that modifies the firmware cannot be updated) technology to ensure the security of the system. The key design part uses a secure key management mechanism and key distribution mechanism to ensure the integrity, authenticity, and tamper-proof modification of transaction data during the transmission process, and prevent keys from being illegally injected, replaced, and used. The face recognition of the payment system includes a living body detection algorithm and a quality assessment algorithm. The living body detection algorithm can prevent prosthetic attacks such as two-dimensional image attacks and three-dimensional mask and head mold attacks. The quality assessment algorithm evaluates the data quality of face recognition and the processing module selects face data for face recognition according to the quality requirements [12]. The HD intelligent 3D camera is adopted in the system and is designed

based on the principle of speckle structured light, which can quickly and accurately obtain the depth information of the target; the recognition accuracy is high [13,14]. In the detection of 5000 face database data provided by the Bank Card Test Center, the pass rate met the performance index of face recognition, and the encryption algorithm passed the test of the State Cryptography Administration, which verified the algorithm performance such as high encryption and decryption efficiency and the fast speed of the system. Compared with the existing research, the safety performance was greatly improved, and the expected effect of the system was achieved.

2. Principles and Methods

Through facial feature recognition, combined with biometric technology and graphics processing technology, the payment system compares the existing facial information, confirms the identity of the consumer, and finally realizes the transaction payment business [15]. At present, the face payment system is mostly used in unmanned retail, catering, supermarkets, and other places. In recent years, it has also been researched and applied in the rail transit payment ticketing system [7,16]. With the development of face payment, more fields will gradually become popular in the future. To take face payments, as an incentive, merchants can accumulate customer resources through face payment. With big data as the basis, they can expand in more fields such as consumer finance, financial management, and other diversified business models.

The main goal of the system is to realize the security of data transmission in the payment process, to ensure the fast and efficient operation environment, to solve the problems of long checkout time and low efficiency in the payment process, to simplify the payment process and maintain an instant completion state, and the payment time is about 1 s. The second is to implement face detection performance indicators and a cryptographic algorithm to achieve big data security [17]. In the payment process, we need to consider the impact of climate environment adaptability, voltage deviation range, signal interference, electromagnetic radiation, and other factors on the system stability as well as the hardware, operating system, image quality requirements, etc. These are the factors that affect the system stability, and are also the secondary goal in research. In addition, in face recognition, the camera's suitable distance, stereo and plane judgment, light intensity, data tolerance for error, and other factors on the recognition accuracy will be regarded as problems that need to be solved in the implementation of the system. During the process of building the system, it is necessary to consider the influence of each factor and then build the software and hardware platform of the system and write application programs according to the priority level.

2.1. System Architecture and Hardware Design

Combined with the current innovation of face payment technology, the system is equipped with a 3D structured light camera with live detection function, which enables dynamic collection and fast recognition. It adopts a1.8 GHz octa-core 64-bit ARM processor core module, and the operating environment is an Android8.1 safe operating system, and the development environment is more secure and convenient. It supports 4G full Netcom, Wi-Fi, and Bluetooth communication methods; built-in contactless card reader module, supports NFC, and can realize omni-channel payment. Other hardware modules of the system are connected to the corresponding interfaces of the core module in the form of peripherals to achieve the functional requirements. The external interface is reserved for the later application software joint Debug port and program upgrade port, and the hardware configuration options (such as contactless module, code scanning module) can be detachable. Under the premise of meeting the standard configuration and considering the upgradeability and scalability of the performance indicators, the face module focuses on heat dissipation and power consumption design. The system security chip has a built-in hardware security encryption module with strong architectural features, supports a variety of encryption security algorithms, and the hardware supports a variety of attack

detection functions. The system has a built-in 512 KB security Flash, 64 KB SRAM, and 4 KB OTP storage area, and integrates a wealth of peripheral resources. All peripheral driver software is compatible with the current mainstream security chip software interface, which can be rapidly developed and transplanted, and provides higher frequency and lower power consumption. The system topology and hardware block diagram are shown in Figures 1 and 2. The facial recognition terminal in Figure 1 is a terminal where users use face recognition to realize offline payment transactions. An acquirer is a business system that provides terminal management, capital settlement, and other services for merchants. The face routing gateway receives the face data ciphertext, routing index code, and other information synchronized by the business system of the account management agency, and is used for the addressing routing of offline payment transactions for face recognition. The transfer clearing system provides the transaction transfer clearing function in the financial payment service. The card issuer provides users with account and fund management services. In Figure 2, the hardware system takes the 64-bit ARM processor and the security control module as the core, and other hardware modules are equipped with external core board corresponding interfaces to meet the functional requirements. Modules can be disassembled and are expandable.

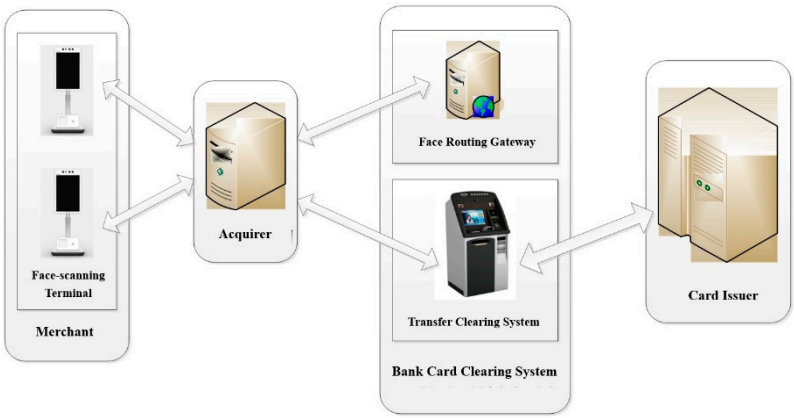


Figure 1. The diagram of the payment system network architecture.

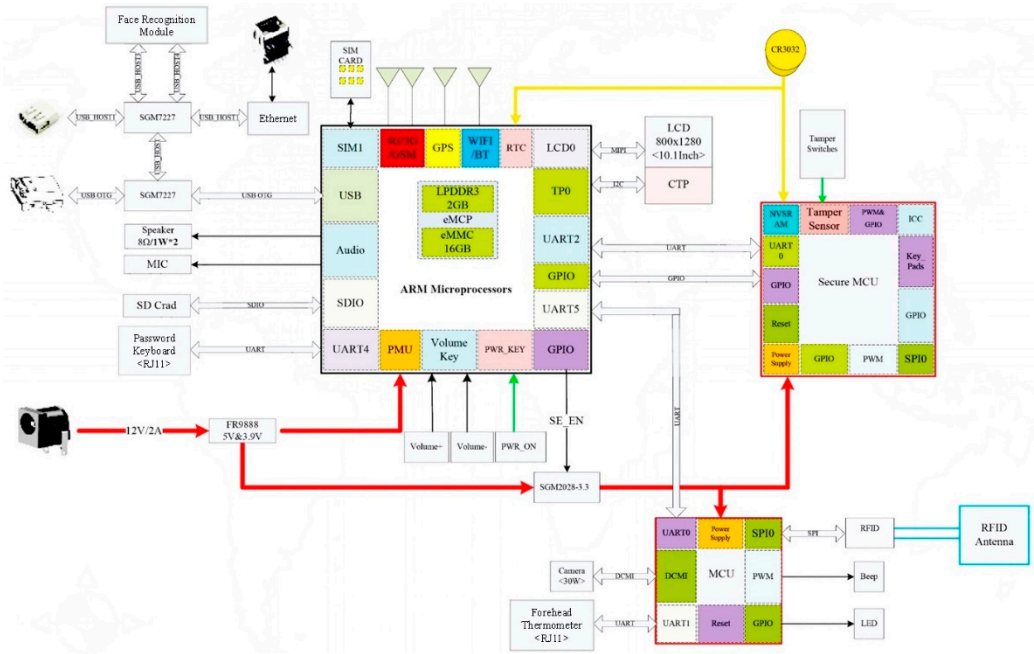


Figure 2. The hardware block diagram.

2.2. System Software Design

The software system consists of three parts: the boot program, operating system, and application program. The boot program is responsible for the initialization at the beginning of the system startup, the download, and startup of the operating system program. The operating system is responsible for downloading, managing, and deleting applications as well as launching applications. The operating system includes hardware drivers, key authority management, and other parts that mainly complete the authority management such as secure channel management and application security status clearing. The key management service provides symmetric algorithm operation, asymmetric algorithm operation, password hash operation, key management, message authentication code calculation, and other functions. At the same time, the module provides strict file level protection. It provides a set of secure and reliable access control mechanisms for key related files. The application consists of two parts: the API and the APP. The APP calls the interface provided by the API. The APP application layer is the code layer of the specific implementation of the business including the application business program and the EMV kernel and other codes. API is an abstraction layer of common functions and driver codes, providing a unified interface for the application layer, which is convenient for the development and transplantation of application layer programs, specifically as shown in Figure 3.

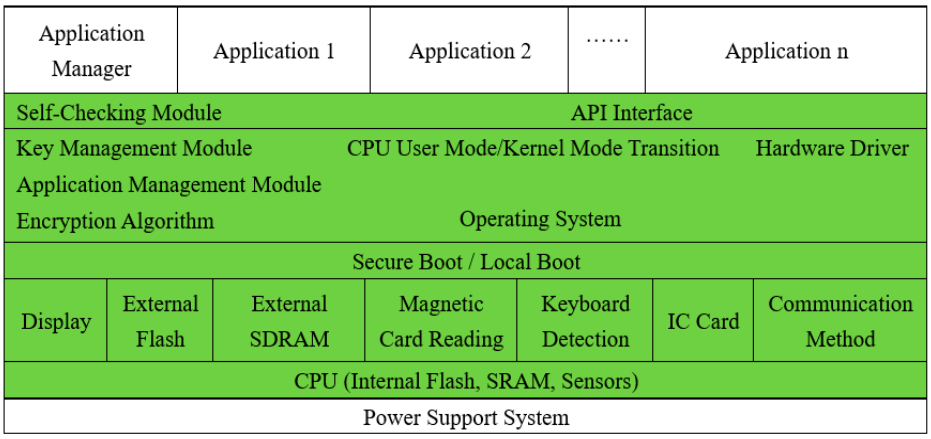


Figure 3. A diagram of the system software design.

The driver layer software directly controls and manages the hardware platform including the reading and writing of RAM, FLASH, registers, etc. as well as various device modules, etc., which are called by the security layer through the API interface. In the system, all operations on the hardware platform are encapsulated into simple, clear, and convenient functions. For each module such as SM4 encryption module, USB, GPIO module, it provides a function interface that can be easily operated.

The FLASH storage mechanism can be divided into three layers. One is the user application layer, which is mainly the mapping of various FLASH storage applications on the upper layer to the logical layer. The logical abstraction layer mainly completes the mapping from logical address to FLASH physical address. The logical address is continuous in the application process, but the physical address can be discontinuous. The FLASH layer is mainly used to read, write, and erase the underlying FLASH. The FLASH storage system fully considers its physical characteristics and implements a load balancing mechanism. Load balancing means that the same FLASH block will not be frequently erased and written:

```
UINT32  gSF_Start_Block;        // Start block of secure storage area
UINT32  gSF_Block_Nums;         // Number of blocks in secure storage area
UINT32  gNormal_Start_Block;    // Start block of normal storage area
UINT32  gNormal_Block_Nums;     // Number of blocks in normal storage area
```

The first four bytes of each FLASH are used to store, and one gSF Map[ ] and one gSF Status[ ] are used to identify the logical address of this FLASH block and whether it has been used. The process of realizing the storage mechanism is shown in Figure 4.

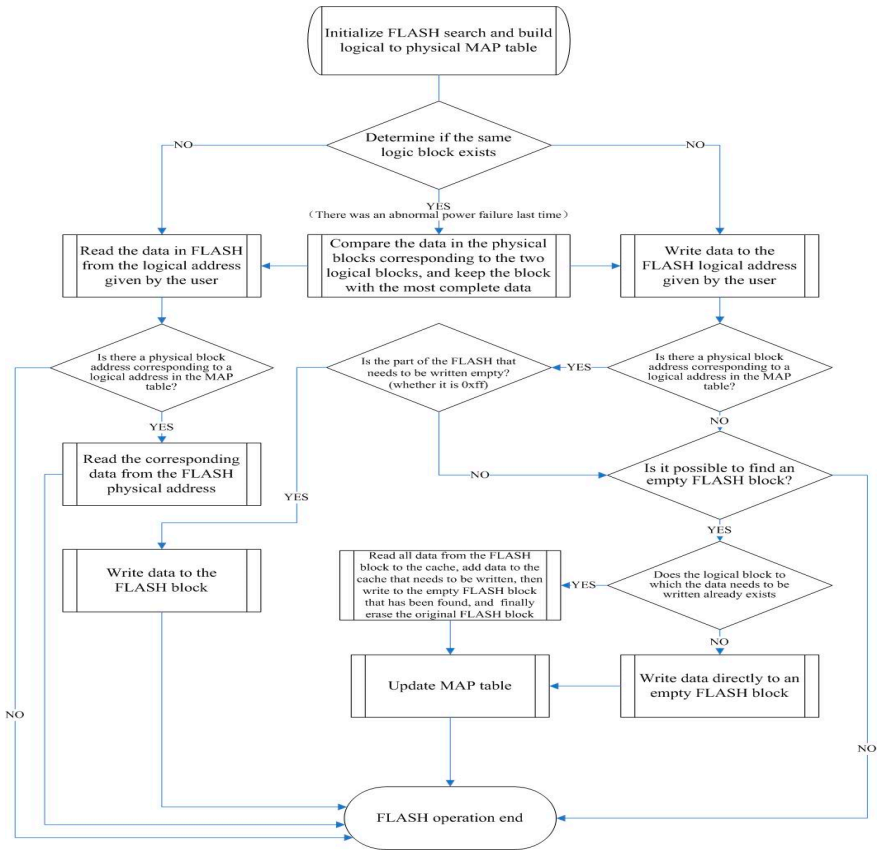


Figure 4. A flow chart of the FLASH storage mechanism implementation.

The security module has an encrypted storage function for the internal EEPROM data of the chip, and supports the encrypted operation function. The encryption operation is for the EEPROM as a whole, and all of the stored data in the EEPROM will be stored in ciphertext. The data output by the EEPROM will reach the processor through the decryption channel. Similarly, the data written by the processor into the EEPROM will also reach the EEPROM through the encrypted channel, and will be stored in unreadable plaintext, which increases the security of the memory, making it impossible for the external data to obtain sensitive data information by directly reading the EEPROM data. The overall framework and startup process of the operating system are shown in Figures 5 and 6. The Android architecture is divided into four layers: the application layer, application framework layer, library layer, and kernel layer. The application layer includes all apps on the mobile phone, whether they are built-in or developed by users, and are all developed based on the second layer application framework layer. The application framework layer is the most commonly used layer. It provides a variety of system APIs. Developers use these APIs to build a variety of apps on the upper layer. The third layer consists of two parts: the first part is the native C\C++ system library layer, which mainly provides a series of third-party class libraries, and the second part is the running environment including the Dalvik virtual machine and Java core library. The kernel layer is the bottom layer of the Android system. This is based on the Linux system and mainly provides various hardware drivers.

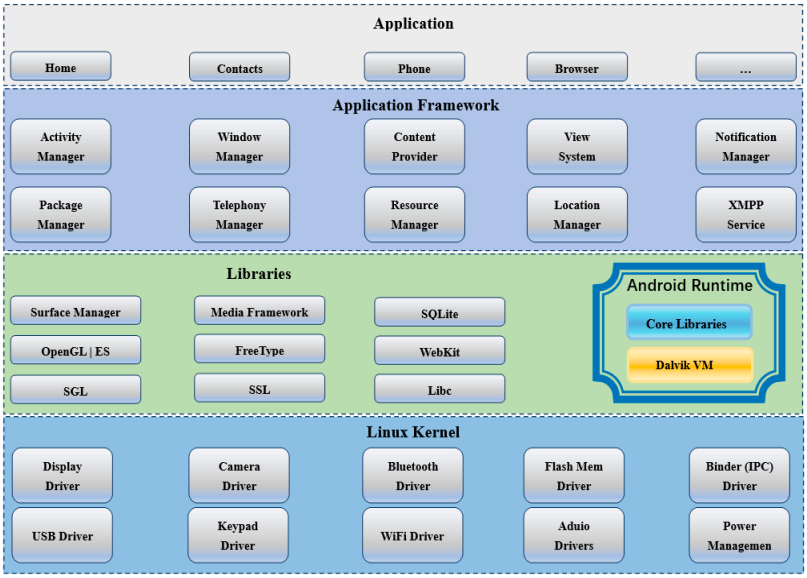


Figure 5. The Android system architecture diagram.

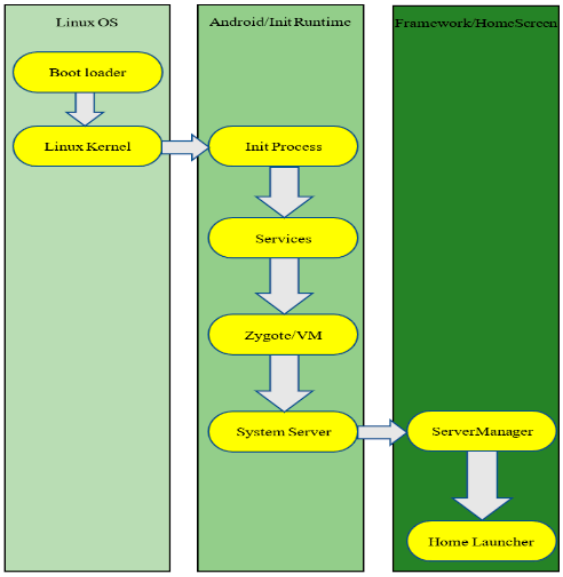


Figure 6. The start process.

3. Algorithms and Performance

The system hardware architecture adopts a dual-chip structure scheme. The main chip is a 64-bit processor with an ARM 11 CPU core, and the auxiliary chip is a state secret security chip. All security-related algorithms are implemented by the security control module, and all sensitive information (keys, security-related parameters, etc.) are stored inside the security module. The SM4 algorithm was officially released by the International Organization for Standardization (ISO) in 2021 and became an ISO/IEC international standard, effectively promoting the improvement in the symmetric cryptographic algorithm system and which has safe and efficient functional characteristics. It has certain advantages in design and implementation such as resource reuse in design; the code can be run in SM4, and easy to develop, not only suitable for software programming, but also for more hardware chip implementation.

3.1. Key Management System Design

The key management system is the basis of software operation, and also determines the security of the algorithm. The system key management adopts a hierarchical key management mechanism. The key is basically divided into three layers, as shown in Figure 7.

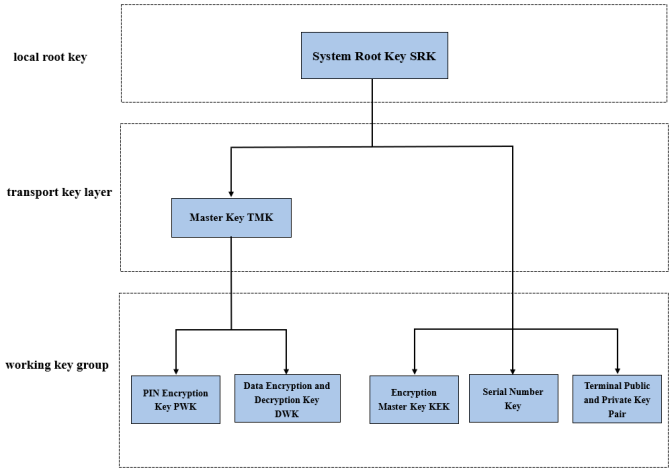


Figure 7. The three layer key architecture.

The first layer, the local root key layer, also known as the system root key SRK, is at the top layer of the key system and is a 128-bit symmetric key, which is generated by the true random number generator of the state secret chip and used to encrypt all locally stored keys (including passwords and public keys that require encryption protection). The keys stored locally are all encrypted by SRK. Therefore, SRK is the most important keys, which is stored in the BPK area of the state secret chip. The BPK area is a battery-backed on-chip SRAM data area, providing 128 bytes of user data storage space without power failure, and SRK occupies 16 bytes of it. The data in the BPK area are automatically reset to zero by the hardware after being attacked. When initialized or after being attacked to clear the information, a set of 16-byte random numbers are automatically generated by the true random number generator of the state secret chip as the system root key. SRK is generated in a fully automatic manner and requires no external intervention for import or installation.

The second layer, the transmission key layer, is also known as the master key TMK. For the protection of data key distribution, or encrypting the working key that needs to be transmitted on the communication route. Input into the terminal using the dual control technique or import into the terminal using KDT (encrypted with the corresponding encryption master key KEK). Export is not supported. After the master key is installed, use the system root key SRK to encrypt it, and then save the encrypted ciphertext in the secure data area of the national secret module according to the specified index number. Decrypt the ciphertext of the work key WKi requested to be downloaded by the terminal.

The third layer, the work key group includes the work key WKi (PIN encryption key, MAC key, track encryption key), asymmetric key pair and public key certificate, etc., which are mainly used for sensitive data encryption and decryption, PIN encryption and MAC calculation and verification, data signature verification, etc. The work key set (WKi) is generated by the customer. Sending updates from the background when a transaction requests to download a work key every time, the application is also designed to re-initiate the sign-in request every other day to ensure that the life cycle of the work key does not exceed 24 h.

The encryption master key (KEK) is generated by the terminal management system of the customer security department to encrypt and protect the master key when it is transmitted on the communication line. Keys are imported into the terminal using dual control technology in a customer secure environment. The dual control technology refers to

splitting the key into two key components, which are kept by different people, respectively. The two key components are entered on the terminal in turn, and then synthesized by XOR in the internal security RAM. The KEK component synthesis formula: KEK = KEK1⊕KEK2. The private key of the terminal public–private key pair is encrypted with the system root key SRK, and then the encrypted ciphertext is stored in the secure data area of the state secret module. Private keys cannot be modified and can only be redistributed.

After all keys are used, the relevant sensitive data will be cleared from RAM at the bottom layer, and there will be no residual data in the memory, causing security risks. The session key is actively destroyed after the session ends, and each session will be regenerated.

3.2. SM4 Algorithm and Performance

SM4 is a block cipher algorithm. It is a dedicated block cipher algorithm for the WLAN (Wireless Local Area Network) and Trusted Computing System. It is a part of the WAPI standard and can also be used for data encryption protection in other environments. Its block length and cipher key length are both 128-bits. SM4 adopts an unbalanced Feistel structure and iterates its round functions for 32 times in both the encryption and key expansion algorithm. Each iterative operation is a round of transformation function F. The structure of decryption is the same as the encryption. However, the decryption round keys are in the reverse order of the encryption round keys. The SM4 algorithm uses module 2 plus and cyclic shift as basic operations. The modules used by the round transform include XOR, S-box with an 8-bit input and 8-bit output, and a linear permutation with a 32-bit input, which is very suitable for processor implementation [18]. The nonlinear change τ is adopted in the key expansion algorithm, which greatly enhances the security of key expansion.

At present, the commonly used symmetric encryption algorithms include SM4, AES, 3DES, RC4, and other algorithms. The AES algorithm uses a complex key scheduling algorithm, and the decryption algorithm also requires additional code, which is more complicated to implement [19]. The SM4 algorithm is relatively simple to implement, the key scheduling and encryption algorithms are basically the same, and the same procedure can be used for decryption, as long as the order of the keys is reversed. The 3DES algorithm avoids similar attacks by increasing the key length of DES, rather than designing a brand-new block cipher algorithm, which is slower to implement in software [20]. The SM4 algorithm adds nonlinear transformation in the calculation process, the security and running rate are higher than 3DES, the software and hardware implementation are faster, and it is more advanced than the 3DES algorithm. RC4 is immune to differential attack and linear attack, and is highly nonlinear. However, when the beginning of the output key stream is not discarded, or a non-random or highly correlated key is used, it is very insecure and easy to be cracked [21]. The algorithm is simpler than SM4 and easy to program. In practical applications, the SM4 algorithm can resist various attack methods against the block cipher algorithm including exhaustive search attack, differential attack, linear attack, etc. It is easy to implement in hardware and has a fast operation speed.

3.2.1. Algorithm Description

The SM4 encryption and decryption process can be described in terms of the encryption process, 32 rounds of iteration, key expansion, round function, and decryption process. The data packet length of SM4 algorithm is 128-bits, and the key length is also 128-bits. Both the encryption algorithm and key expansion algorithm adopt 32 rounds of a nonlinear iteration structure. Each round uses a round key, and each iteration is a round of transformation function F.

(1) The encryption process:

The encryption operation is performed in words (32-bit). The input is 4-word plaintext (X_0, X_1, X_2, X_3), and the output is 4-word ciphertext (Y_0, Y_1, Y_2, Y_3). The input round key is

rk_i, $i = 0, 1, \ldots, 31$. The encryption process is divided into two steps, 32 rounds of iteration, and 1 reverse order transformation. As follows:

$$X_{i+4} = F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) = X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i)\ i = 0, 1, \ldots, 31. \quad (1)$$

$$(Y_0, Y_1, Y_2, Y_3) = R(X_{32}, X_{33}, X_{34}, X_{35}) = (X_{35}, X_{34}, X_{33}, X_{32}) \quad (2)$$

(2) 32 rounds of iteration:

The input plaintext is X_0, X_1, X_2, X_3. When $i = 0$, it is the first round of transformation, which continues until $i = 31$; Put $X_{i+1}, X_{i+2}, X_{i+3}$ and the round key rk_i XOR operation obtains a 32-bit data as the input of the box transform:

$$Sbox\_input = X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i \quad (3)$$

Divide the *Sbox_input* into four 8-bit data, perform box transformation, respectively, then combine the four 8-bit *Sbox_output* into a 32-bit output, and move the *Sbox_output* just obtained by 2-, 10-, 18-, 24-bit to the left, respectively, to obtain four 32-bit results, record the shift result as $Y_2, Y_{10}, Y_{18}, Y_{24}$, XOR the shift results $Y_2, Y_{10}, Y_{18}, Y_{24}$ with the box transform *Sbox_output* and X_i to obtain X_{i+4}, which is

$$X_{i+4} = Sbox\_output \oplus Y_2 \oplus Y_{10} \oplus Y_{18} \oplus Y_{24} \oplus X_i \quad (4)$$

Thus far, one round of encryption and decryption operation has been completed. In the actual encryption and decryption process, the above operation needs to perform 32 rounds, using 32 different rk_i, which are generated by the key extension. Finally, the generated four 32-bit data $X_{35}, X_{34}, X_{33}, X_{32}$ are combined into a 128-bit data output as the final output result. The whole process of encryption processing is like a sliding window with a width of four words. After one round of encryption processing, the window slides one word. After the window slides 32 times in total, the encryption iteration ends.

(3) Key expansion:

rk_i is generated by key expansion, and each round of encryption in the 32-round iteration structure uses a 32-bit round key. The SM4 algorithm uses a key expansion algorithm to generate 32 round keys. There are two values of constant FK and fixed parameter CK in the key expansion algorithm.

FK_0 = (A3B1BAC6), FK_1 = (56AA3350), FK_2 = (677D9197), FK_3 = (B27022DC).

There are 32 fixed parameters $CK = (CK_0, CK_1, \ldots, CK_{31})$, CK_i is a word. The input encryption key is $MK = (MK_0, MK_1, MK_2, MK_3)$, the output round key is rk_i. Then, the key expansion algorithm can be described as follows:

$$(K_0, K_1, K_2, K_3) = (MK_0 \oplus FK_0, MK_1 \oplus FK_1, MK_2 \oplus FK_2, MK_3 \oplus FK_3) \quad (5)$$

For $i = 0, 1, \ldots, 31$.

$$rk_i = K_{i+4} = K_i \oplus T'(K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus CK_i) \quad (6)$$

The T' transformation is basically the same as T in the encryption algorithm round function, only the linear transformation L is modified to L':

$$L'(B) = B \oplus (B \lll 13) \oplus (B \lll 23) \quad (7)$$

The key expansion algorithm is similar to the encryption algorithm in terms of the algorithm structure, which also adopts 32 rounds of similar iterative processing. However, the key expansion algorithm adopts nonlinear transformation T', which greatly enhances the security of key expansion. SM4 and AES passwords are similar in this regard.

(4) Round function:

The round function of the SM4 algorithm is a cryptographic function that uses words as the processing unit. Let the input of the round function $F = (X_0, X_1, X_2, X_3)$, four 32-bit words, and the round key is rk. The output is also a 32-bit word.

$$F(X_0, X_1, X_2, X_3) = X_0 \oplus T(X_1 \oplus X_2 \oplus X_3 \oplus rk) \tag{8}$$

The synthetic transformation T is T(X) = L(τ(X)), which is composed of the nonlinear transformation τ and the linear transformation L. The nonlinear transformation τ is in word units and consists of 4 S-boxes juxtaposed. Linear transformation L input and output are 32-bit words. The role of its cryptography is to play a diffusion role. Let the input of L be word B and the output be word C, then:

$$C = L(B) = B \oplus (B \lll 2) \oplus (B \lll 10) \oplus (B \lll 18) \oplus (B \lll 24) \tag{9}$$

The synthetic transformation T plays the role of confusion and diffusion, and improves the security of the password.

(5) The decryption process:

The SM4 algorithm has the same structure of encryption and decryption, except that the round key is reversed, and the decryption round key is the reverse order of the encryption round key. That is, the input round key is rk_i, i = 31, 30, . . . , 1, 0, the input ciphertext is (X_0, X_1, X_2, X_3), and the output plaintext is (Y_0, Y_1, Y_2, Y_3).

$$X_{i+4} = F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) = X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i)\ i = 31,\ 30,\ ...,\ 1,\ 0. \tag{10}$$

$$(Y_0, Y_1, Y_2, Y_3) = (X_{35}, X_{34}, X_{33}, X_{32}) \tag{11}$$

3.2.2. Algorithm Performance and Test Result

The software and hardware of the face recognition payment system realize data encryption, the SM4 main encryption algorithm encrypts and protects data in static storage and transmission channels, and the round function and nonlinear transformation play the role of confusion and diffusion, improving the password security. In the system, we also used the RSA algorithm and SHA2 (Secure Hash Algorithm 2) cryptographic hash function to perform the digital signature, verify the digital signature, and generate the data message digest, and assist the SM4 algorithm for data encryption protection. The face data between the terminal split and external components and the host is encrypted and protected by the key to prevent theft, replay, and tampering, and has the feature of preventing the use of the exhaustive detection of payment passwords. The terminal software encrypts and protects information, the operating environment is safe and reliable, and it has prevention and control capabilities such as Trojan horse virus prevention.

The SM4 algorithm performs three encryption and decryption tests on the transaction data, respectively, and takes the average value of the three operations to calculate the average rate. The test results of the encryption operation are shown in Table 1, and the decryption are shown in Table 2. The average rate of encryption operation is 3971.89 Kbps, decryption is 3971.81 Kbps, and the average execution time of system encryption and decryption data is 0.264 s. In the research on mobile terminal payment security, there have been few studies on the application of the state secret algorithm in face recognition payment systems. The AES + RC4 algorithm was used to encrypt the payment system in [22], and the efficiency of the encryption scheme was tested and analyzed. The algorithm takes 1.921 s to encrypt 1 Kb data, while the SM4 algorithm in this paper only required 0.264 s to encrypt 128 K data, which was much faster than the AES + RC4 algorithm in [22]. In the mobile network payment, the SM4 hybrid encryption algorithm took 2.64 ms to encrypt 128-bit data in [23], while the payment system in this paper needed 264 ms to encrypt 128 KB data, the data length was equivalent to 8000 times that in [24], and the encryption time was only

100 times. The encryption rate was much higher than the former. Messages containing different numbers of characters were used to test the performance of the security encryption module in [24], and the number of characters per message ranged from 100 to 65,000. When the number of characters is 10,000, the encryption and decryption time of the 3DES-RC4 algorithm is about 0.3 s, and when the number of characters is 65,000, the encryption and decryption time is about 1.7 s. In this paper, the SM4 algorithm encrypted and decrypted 128 KB of data, which was much more than the previous number of characters, but the encryption and decryption time was far less than the 3DES-RC4 algorithm. Five sets of parameters were selected according to the actual test environment in [25], and the time consumed to realize a complete payment transaction was about 318.41 ms, which was also slower than the payment system in this paper. Through the above comparison, the effectiveness and superiority of the payment system in this paper can be illustrated.

Table 1. The SM4 algorithm encryption test results.

Encryption Data (KB)	Operation Time (Seconds)			Average Execution Time (Seconds)	Average Operation Rate (Kbps)
	First Time	Second Time	Third Time		
128	0.265	0.263	0.264	0.264	3971.89

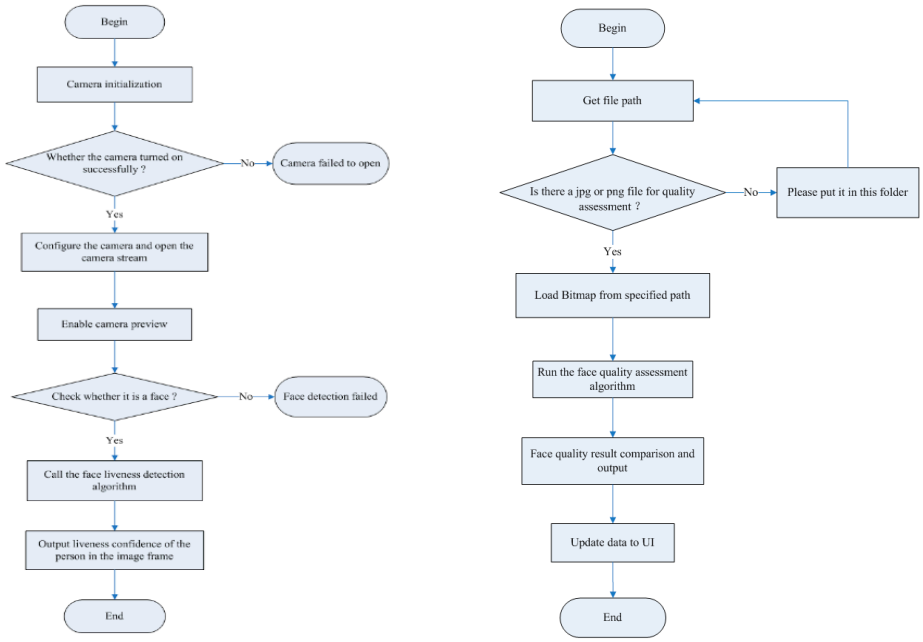
Table 2. The SM4 algorithm decryption test results.

Decryption Data (KB)	Operation Time (Seconds)			Average Execution Time (Seconds)	Average Operation Rate (Kbps)
	First Time	Second Time	Third Time		
128	0.264	0.264	0.265	0.264	3971.81

3.3. Face Recognition Algorithm Program

The payment system processes the input dynamic recognition image or video stream based on the facial features of people, and further extracts the identity features contained in each face according to the position and size of each face and the position information of each main facial organ. Compare it with the known face, and cooperate with the relevant technologies of the recognition system such as face image acquisition, face positioning, face recognition preprocessing, identity confirmation, and identity search, etc. to confirm the identity of the specific person.

The face recognition system includes a liveness detection algorithm and a quality assessment algorithm. The liveness detection algorithm needs to use a camera module that supports infrared image streaming, and the quality assessment algorithm does not need to connect the camera module. The algorithm flow chart is shown in Figure 8. The 3D structured light living module has high performance and low power consumption, and can effectively resist prosthetic attacks; compared with the binocular stereo imaging and TOF (time-of-flight) schemes, the structured light scheme has great advantages. Because the RGB binocular camera relies heavily on pure image feature matching, the effect is very poor in the case of dark lighting or overexposure. In addition, if the tested scene itself lacks texture, it is difficult to extract and match features [26]. The TOF scheme and structured light scheme are the most promising due to their advantages of convenient use and low cost. However, the structured light scheme surpasses the previous two schemes in terms of accuracy and is very suitable for intelligent terminals [27]. 3D structured light face recognition technology is far superior to TOF and binocular face recognition in terms of security, recognition accuracy, recognition speed, etc., and can more effectively defend against attacks by various props such as paper and masks; the analysis time changed from the previous 1–2 seconds compressed to the millisecond level; and it was not affected by the intensity of ambient light, which is very suitable for face recognition payment scenarios. The algorithm program is shown in Figure 9.



(**a**) (**b**)

Figure 8. The flow chart of the face algorithm: (**a**) is the flow chart of the liveness detection algorithm, (**b**) is the flow chart of the quality assessment algorithm.

```
//Quality assessment algorithm, time-consuming
long tt = System.currentTimeMillis();
FaceQuality faceQuality = Frame.detectFaceQuality(path);
long qualityTime = System.currentTimeMillis() - tt;

//Compare the result
String faceDetail = compareFaceQuality(faceQuality);

//Update data to UI
mFaceImage.post(new Runnable() {
    @Override
    public void run() {
        mFaceImage.setImageBitmap(mBitmap);
        mFaceText.setText(faceDetail + "\n"
        + "file path: " + path + "\n\n"
        + "face evaluation time-consuming: "
        + qualityTime + "ms");
    }
});
```

(**a**) (**b**)

Figure 9. Face algorithm program: (**a**) is the main program of the liveness detection algorithm, (**b**) is the main program of the quality assessment algorithm.

3.4. Face Detection Result

Liveness detection can prevent 2D and 3D prosthesis attacks, and we carried out multi-dimensional attack tests under the influence of external factors such as different light, distance, angle, posture, prosthesis material and process such as 2D image attack; 3D mask attack; 3D head model attack; 3D simulated face attack, etc. [28]. The liveness detection module supports the enhanced liveness detection function, when the ratio on guard against 2D and 3D prosthesis attack times is 9:1; when the LDAFAR (Liveness Detection Attack False Acceptance Rate) is 0.1%, the LPFRR (Liveness Presentation False Rejection Rate) <1%. This demonstrates the high stability and strong anti-attack capability of the system, which ensures the data security in the face payment process.

The system tested the pass rate when the number of face databases was 5000. The pass rate refers to the percentage of the total number of correct rejections and correct identifications in the number of tests in the face identification process. The 5000 face database data were provided by the Bank Card Test Center, which is a specific dataset for system detection. The test results are shown in Table 3, which meet the requirements

of face identification performance indicators in the "Technical specification for offline payment security application of face recognition". The pass rate was ≥98.3% when the false recognition rate was 0.01%, and the pass rate was ≥98% when the false recognition rate was 0.001%. At present, some face recognition payment technologies can only reach 94% and 91%, and their performances were lower than that of this system in terms of dataset dependency and fault tolerance. In [29], the training samples are divided into 9 regions, and the weights of these 9 regions are assigned respectively based on the feature weighting scheme. In Scheme 4, the eye region is assigned as 4, the nose and mouth regions are assigned as 2, and the remaining regions are assigned as 1. When the number of training samples is 280, the correct recognition accuracy is the highest, 97.52%. However, the number of face databases of this sys-tem far exceeds the number of samples in [29], with a pass rate of over 98%. In [30], when the number of face samples was 240, the highest accuracy of correct recognition was 96.13%, which was also lower than the accuracy of the system algorithm. For the 3000 face database dataset in [31], the pass rate was 97.2% when the false recognition rate was 1%, and the pass rate was 91.2% when the false recognition rate was 0.1%. The pass rate of our system was much higher than the test results in [31]. In [32], based on the influence of the length of the verification key on the accuracy of the identification and authentication, the accuracy of biometric encryption authentication was evaluated from the false acceptance rate (FAR), false rejection rate (FRR), and other indicators, and the authentication accuracy of three keys with different lengths was evaluated, respectively, with a maximum of 94%, which was also far lower than the pass rate of this system.

Table 3. The performance test results.

Number of Face Databases	False Recognition Rate	Pass Rate	Performance Requirement
5000	0.01%	98.85%	≥98.3%
5000	0.001%	98.51%	≥98%

4. Discussion

During the research process, we consulted a large number of studies. At present, there are very few studies on the application of the state secret algorithm to the face payment system. Therefore, the ideas and research schemes proposed in this paper also fill the gaps in this field. During the design and implementation of the system, it was found that the performance was the most stable in a climate environment with a temperature of 0–40 °C and a relative humidity of 15–90% without condensation. The system can work normally when the rated voltage deviation range is ±5%. In the radiation continuous disturbance test, the quasi-peak limit was 40 dBμV/m when the frequency was 30–230 MHz, and the quasi-peak limit was 47 dBμV/m when the frequency was 230–1000 MHz; the test results meet the communication frequency band requirements. The system should avoid running the function in sunlight. The sunlight will interfere with the module, resulting in unusable functions or poor accuracy. Therefore, it is recommended to use it indoors or in places with weak sunlight to avoid direct sunlight on the module camera. Thermal radiation and high temperature will cause accelerated aging of the grating of the laser transmitter and affect the accuracy. The camera module designed based on the speckle structured light principle, equipped with an ASIC (Application Specific Integrated Circuit) chip, is suitable for face recognition at a distance of 0.28–1 m. It can quickly and accurately obtain the depth information of the target, and can perform three-dimensional and two-dimensional judgments. The face recognition model can defend against adversarial attacks, which improves the robustness of the model [28]. It is more suitable for close-range face recognition scenarios such as face payment in the new retail industry and personal ID verification in railway stations.

In light of the current security risks in the transaction process, the system focuses on security performance requirements in the design and implementation process such as

hardware "disassembly and self-destruction" and software "firmware encryption, self-check" and other functions, effectively ensuring the security of the transaction. The system uses a secure key management mechanism and key distribution mechanism to ensure the integrity, authenticity, and tamper-proof modification of transaction data during the transmission process, and prevent keys from being illegally injected, replaced, and used. The M-sequence scrambling mechanism ensures that the random number quality is not affected by physical noise source. The security module itself is designed with high and low voltage and high and low frequency detection. When the input signal exceeds the range, the module will stop working, avoiding the impact on the physical noise source. The encryption operation of sensitive data is completed in the RAM inside the security module. After encryption is completed, all sensitive data in plaintext are deleted immediately. Even if the power is lost during the encryption operation, the data in the RAM will be automatically lost, and no sensitive data in plaintext will be retained. The face image test dataset in the liveness detection algorithm was provided by the Bank Card Test Center, and the system ran the algorithm to encrypt and identify it. In processing massive face database data, the system demonstrates the security performance of the underlying algorithm to encrypt big data. It effectively resists prosthetic attacks, and ensures that the face data are not leaked and tampered during the whole process from the acquisition of face data by the acquisition module to the completion of the encryption operation in the encryption module, and is transmitted in a secure manner.

5. Conclusions

In the information age, two indicators have been pursued: speed and safety (not passion). The security algorithm will always evolve with the progress over time, and it is a never-ending battle of offense and defense. Face 3D recognition technology enables machines to accurately identify facial systems. Compared with flat QR codes, face recognition technology is more secure, and accounts are almost never stolen. Face recognition technology has the function of verification. In addition to identifying accounts and making payments, it can also confirm identity and verify valid information. For example, after face recognition technology is extended to crowded places such as stations, airports, and banks, the situation of manual ticket checking will be greatly reduced, and machine recognition can maximize the efficiency and reduce manual errors. Moreover, the equipment has the advantages of low cost, convenient access, and labor saving. In the current research, there are relatively more studies on face recognition payment in the field of smart rail transit security payment, and certain results have been achieved. There are few studies and applications in other payment fields. The payment system studied in this paper can be applied in multiple scenarios. The state secret algorithm SM4 is the main encryption algorithm, and combined with face liveness detection algorithm and encryption algorithms such as RSA and SHA2, they are used to make the entire transaction process more secure. In the next step, we plan to apply the SM2 and SM3 algorithms to the system to replace the RSA and SHA2 algorithms for digital signature and verification as well as the generation and verification of random numbers and message authentication codes to improve the overall security performance and operating speed of the system. The payment system has been tried out in enterprises and has achieved satisfactory application results, improving the user's transaction experience. The payment system has a good application prospect because it is suitable for payment transactions in multiple scenarios. The research scheme of this paper will also provide some valuable references in the field of face recognition payment security.

6. Patents

The patent generated by the research work of this paper is: A face recognition payment device with an adjustment device, patent number: ZL202121238908.8, authorized announcement number: CN214752141U.

Author Contributions: Conceptualization, Y.Z. (Yukun Zhou) and N.W.; Methodology, B.H.; Software, N.W. and J.Q.; Validation, Y.Z. (Yukun Zhou) and B.H.; Investigation, Y.Z. (Yitao Zhang) and N.W.; Resources, B.H.; Data curation, Y.Z. (Yukun Zhou), B.H. and W.C.; Writing—original draft preparation, Y.Z. (Yukun Zhou); Writing—review and editing, Y.Z. (Yukun Zhou), N.W., W.C. and Y.Z. (Yitao Zhang); Project administration, Y.Z. (Yukun Zhou) and B.H.; Funding acquisition, Y.Z. (Yukun Zhou) and W.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Scientific Research Project of Zhejiang Provincial Department of Education under Grant No. Y202045049; Zhejiang Basic Public Welfare Research Program Project of China under Grant No. LGF20F010002; the Visiting Engineer of Zhejiang Province "School-Enterprise Cooperation Project" under Grant No. FG2020113; Technical Commissioner Team of Ningbo City under Grant No. 2018-65; and the Major Special Projects of Ningbo City under Grant No. 2019B10079.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Liu, X.M.; Xia, T.W. Research on application status and problems of face-scanning payment technology in payment institutions. *Financ. Technol. Time* **2020**, *12*, 59–61.
2. *ISO/IEC 18033-3:2010/AMD 1:2021*; Information Technology-Security Techniques—Encryption Algorithms—Part 3: Block ciphers—Amendment 1: SM4. International Organization for Standardization: Geneva, Switzerland, 2021.
3. Gao, G.Q. Security of SM4 against correlated key linear cryptanalysis. *J. Beijing Inst. Graph. Commun.* **2020**, *28*, 154–160.
4. Xiao, Y. Design of Face Anti-Spoofing Based on Deep Learning. Master's Thesis, Zhejiang University, Hangzhou, China, July 2021; pp. 15–21.
5. Luan, X.; Li, X.S. Face anti-spoofing algorithm based on multi-feature fusion. *Comput. Sci.* **2021**, *48*, 410–413.
6. Zhang, Y.; Ma, C.Z.; Yang, P.; Wang, X.M. Face feature extraction algorithm based on wavelet transform and improved principal component analysis. *J. Jilin Univ. (Sci. Ed.)* **2021**, *59*, 1500–1503.
7. Yang, B.; Chen, Y.C. Smart rail transit secure payment system based on face recognition. *Commun. Technol.* **2020**, *53*, 506–511.
8. Huang, J.Y. Face liveness detection technology based on security encryption. *Pract. Electron.* **2019**, 77–78. [CrossRef]
9. Chen, Y.; Chen, C.S.; Hu, H.G. Research on power analysis of SM4 hardware implementation. *Netinfo Secur.* **2018**, *5*, 52–54.
10. Chen, L.; Zhong, W.D.; Yang, X.Y.; Liu, W.C. Mixed intelligent side channel analysis attack method for SM4. *Comput. Eng. Appl.* **2019**, *55*, 86–91.
11. Jin, Y.X.; Yang, H.Z.; Wang, X.B.; Yuan, Q.J. Improved differential fault attack for SM4 cipher. *J. Cryptologic Res.* **2020**, *7*, 453–463.
12. Li, Y.H.; Nie, M.X.; Su, X.P.; Zhou, X.J.; He, C. Face recognition algorithm based on regional feature extraction. *J. Northwest Univ. (Nat. Sci. Ed.)* **2020**, *50*, 812–818.
13. Zuo, C.; Zhang, X.L.; Hu, Y.; Yin, W.; Shen, D.T.; Zhong, J.X.; Zheng, J.; Chen, Q. Has 3D finally come of age?—An introduction to 3D structured-light sensor. *Infrared Laser Eng.* **2020**, *49*, 0303001.
14. Shi, Q.Y.; Li, H.; Shi, F.R.; Yang, K.F. 3D face recognition algorithm based on near-infrared structured light and visible light. *Wirel. Internet Technol.* **2019**, *4*, 124–125.
15. Xing, W.Q.; Liu, C.J. Application research of improved face recognition algorithm in APP. *Electron. Des. Eng.* **2019**, *27*, 185–188.
16. Jing, L.; Zhou, C.; Liu, P. Application and discussion of face recognition technology in the automatic fare collection system of urban rail transit. *Shanghai Constr. Sci. Technol.* **2021**, *2*, 24–26.
17. Yang, G.Q.; Ding, H.C.; Zou, J.; Jiang, H.; Chen, Y.Q. A big data security scheme based on high-performance cryptography implementation. *J. Comput. Res. Dev.* **2019**, *56*, 2207–2215.
18. Luo, Q.B.; Li, X.Y.; Yang, G.W. Quantum circuit implementation of S-box for SM4 cryptographic algorithm. *J. Univ. Electron. Sci. Technol. China* **2021**, *50*, 821–822.
19. Wang, X.X.; Hu, W.; Tan, J.; Zhu, J.C.; Tang, S.B. Correlation fault attack on AES. *J. Xidian Univ.* **2021**, *48*, 192–199.
20. Wu, J.F.; Zheng, B.W.; Nie, Y.; Chai, Z.L. FPGA accelerator for 3DES algorithm based on OpenCL. *Comput. Eng.* **2021**, *47*, 147–155.
21. Chen, H.; Liu, Y.M.; Xiao, C.L.; Guo, P.F.; Xiao, Z.J. Improved RC4 algorithm based on elliptic curve. *J. Comput. Appl.* **2019**, *39*, 2339–2345.
22. Gao, X.M. Research on Security of Mobile Payment. Master's Thesis, Chang'an University, Xi'an, China, May 2017; pp. 59–60.
23. Mao, Y. Research on Chinese Domestic Cipher Algorithms in Mobile Network Payment. Master's Thesis, Harbin University of Science and Technology, Harbin, China, March 2018; pp. 46–47.
24. Wang, D.D. Design and Implementation of Secure Encrypted Instant Messaging System. Master's Thesis, Shenyang Institute of Computing Technology Chinese Academy of Sciences, Shenyang, China, June 2020; pp. 62–64.
25. Dou, M.J. Identity Authentication Mechanism Based on Blockchain in Mobile Payment. Master's Thesis, Xidian University, Xi'an, China, July 2020; pp. 55–57.

26. Zhuang, S.F.; Ji, Y.; Tu, D.W.; Zhang, X. Underwater RGB-D camera based on binocular stereo vision. *Acta Photonica Sin.* **2022**, *51*, 0404003.
27. Sun, D.Q.; Duan, H.X.; Pei, H.D.; Hu, L. Pose measurement method of Space non-cooperative targets based on TOF camera. *Acta Opt. Sin.* **2021**, *41*. [CrossRef]
28. Manzo, M.; Giordano, M.; Maddalena, L.; Guarracino, M.R. Performance Evaluation of Adversarial Attacks on Whole-Graph Embedding Models. In Proceedings of the 15th Learning and Intelligent Optimization Conference, Athens, Greece, 20–25 June 2021; pp. 219–236.
29. Huang, C.M. Third Party Payment System Based on Face Recognition. Master's Thesis, Yangzhou University, Yangzhou, China, November 2018; pp. 32–36.
30. Liu, Q. Embedded Mobile Payment System Based on Face Recognition. Master's Thesis, Yangzhou University, Yangzhou, China, October 2019; pp. 35–36.
31. Yi, S. Railway Passengers Unconscious Outbound Key Technology and Application Scheme Research. Master's Thesis, China Academy of Railway Sciences, Beijing, China, June 2020; pp. 48–50.
32. Wang, B. Research and Implementation of Security Mechanism of Virtual Campus Card Based on Blockchain. Master's Thesis, Beijing Jiaotong University, Beijing, China, September 2020; pp. 52–54.