Information Security Protection of Digitized Archives Based on State Secret Algorithms

Fen Wang
School of Business
Zhengzhou University of Economics and Business, China
wfluck2024@163.com

Abstract: *Digital archives are stored on computers or network servers, making them vulnerable to unauthorized access, theft, or tampering by hackers. In order to achieve a more efficient and secure encryption and decryption process of digital archive information, a security protection method of digital archive information based on state secret algorithm is studied. The concept of component and hierarchical design is adopted to build a digital archive data warehouse. Before the transmission of digital archive information data, the sender generates a random Symmetric Block Cipher Algorithm (SM4) key and encrypts it using the SM2 algorithm. Use the SM2 algorithm to decrypt the random key, and then use the SM4 algorithm to decrypt the ciphertext. The SM2 hybrid state secret algorithm is used to establish the authentication mechanism of the archive system and set digital certificates to ensure the consistency of information encryption. The experimental results show that the algorithm has higher encryption efficiency and advantages of digital archive information, can effectively block malicious acts, and ensure the security of digital archive information.*

Keywords: *national secret algorithm, SM2 algorithm, SM4 algorithm, digital archives information; safety protection*.

Received April 1, 2025; accepted October 23, 2025
https://doi.org/10.34028/iajit/23/3/14

1. Introduction

Digital archives information is the process of transforming traditional paper archives, documents or materials into digital forms. Scan paper archives, convert them into electronic files, and then store them on computers or other electronic devices. Digital archives typically contain various data types including text, images, audio, and video for electronic management, retrieval, and dissemination. Digital archive information has significant advantages in information storage, query, security, cost, etc. It is an important development direction of modern archive management Krishna *et al*. [10] However, digital archive information can be changed artificially. In the computer network system lacking security protection, digital archive information can be changed at will, which leads to hidden dangers in information security. The security protection of digital archive information can ensure the integrity of archive information, ensure the security of archive information, improve the management efficiency of archive information, and promote the long-term preservation of archive information Dong and Yang [4] Consequently, digital archive security has become an important research focus.

Rani *et al*. [17] proposed a digital archive image information encryption model based on the differential coding technology of magic square and chaotic mapping. The two-dimensional Arnold scrambling algorithm was used to randomize the coordinate position of the digital archive image to complete the chaotic operation. By cropping the original digital archive images, security protection of digital archive images is achieved. But both chaotic maps and magic squares require keys or initial conditions. If these information is disclosed, the encryption may be cracked. Brahim *et al*. [2] transformed the digital archive image data block into a sparse matrix through wavelet transform, and used an improved linear feedback shift register to generate a vector with the same length as the number of rows of the matrix to work. By using a value of the vector to move each line to obtain the conversion matrix, the compression matrix is obtained through the relationship between the conversion matrix and the measurement matrix, and all the compression matrices are combined to obtain the compressed image, thus realizing the encryption of digital archive image information. But compressive sensing is a method of reconstructing the original signal or image from a small amount of measurement data by utilizing the sparsity of the signal. When digital archive images do not meet the sparsity condition, compressed sensing technology may not be able to effectively compress and encrypt images. Lin *et al*. [11] through a kind of chaotic synchronization and chaos based on security communication ideas realize digital archives information security protection, through the signal of the signal structure drive signal, and information message encryption to the drive signal, form confidential communication transmission signal, through the description of chaotic signal, finally realizes the digital archives information security protection. However, this method involves more complex

encryption and decryption processes, which requires more time, and the efficiency of encryption and decryption is low, which is not conducive to information security protection. Khan *et al*. [8] put forward a secret information hidden to the digital file images lowest effective implicit method, through the convolutional neural network for digital file image hidden information extraction, encryption implicit image optimization, and the original image of implicit classification, so as to realize the digital file information security protection. However, embedding information into the least significant bit of the digital archive image may lead to the loss of image quality. If the amount of embedded information is large, the image quality may be seriously affected, making the steganography image significantly different from the original image.

In order to solve the above problems, a digital archive information security protection method based on the state secret algorithm is proposed. Build a digital archive data warehouse, and realize fast, safe and convenient key management by combining the advantages of SM2 algorithm, high encryption security, simple key management, and low bandwidth requirements, with the advantages of SM4 algorithm, fast encryption speed. The SM2 hybrid state secret algorithm is used to establish the identity verification mechanism of the archive system to ensure the security of data and the consistency of the information transmitted by both parties, and realize the encryption of digital archive information data.

2. Information Security Protection Methods for Digitized Archives

2.1. Construction of a Data Warehouse for Digitized Archives

In order to reduce the computational redundancy in the process of data transmission and encryption, a digital archive data warehouse structure including data management layer, data analysis engine and user interface is constructed based on the concept of component-based and hierarchical design. Among them, all the information and data in the digital archive system are contained in the data layer, which is introduced into the Extract Transform Load (ETL) environment through SAG100WM equipment. During this process, a centralized center for data was generated, which is the center of the warehouse [5, 18, 19]. This design prevents data loss from external attacks, and the analysis of data will no longer rely solely on the database of the archive system itself. Secondly, for the design of data analysis engine in data warehouse, this paper uses Online Analytical Processing (OLAP) technology to establish the connection between data reports. When a user sends a data transmission request to the system, the data analysis engine displays the main contents of its own relevant information on the archive system portal, and establishes a connection with the data layer through the web service data interface. Analyze the fitting relationship between data layer information and the target based on the transmission request provided by the user. In order to reduce the exceptions [3, 15, 20] caused by too many concurrent requests during data analysis, the data analysis engine is designed from bottom to top as the original data layer, data sorting layer, data storage layer, data presentation layer and data delivery layer. Figure 1 illustrates the data analysis engine's layered structure.

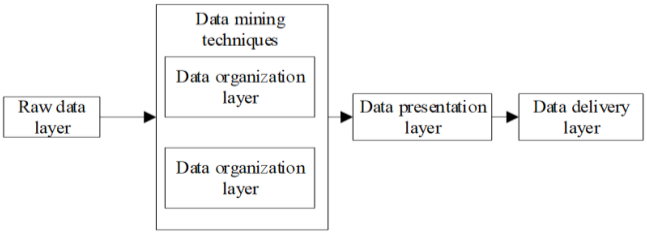


Figure 1. Structure diagram of data analysis engine.

According to Figure 1, the original data layer in the data analysis engine is directly connected to the original database in the digital archive system. The user's transmission request is decomposed into data warehouse technology Extract Transform Load (ETL) information based on database tags at the data sorting layer, and then these ETL information is stored in the data storage layer of the system, at this point, the information in the data layer is analyzed in multiple dimensions through the data representation layer. Combined with the source of file data, the data that meets the user's transmission request is transferred to the data delivery layer as the data content that is finally transferred to the user.

2.2. Designing Encryption Methods for Digitized Archival Information

SM2 algorithm is an efficient and secure public key cryptography algorithm based on elliptic curve. As the only nonlinear component in block ciphers, the design characteristics of s-boxes directly affect the algorithm's resistance to differential cryptanalysis. Taking the SMS4 algorithm as an example, its s-box is designed with a strict differential distribution matrix, so that the output differential values only contain three possibilities: 0, 2, and 4, and each non-zero input differential corresponds to an output differential 4 that only appears once. This feature significantly reduces the possibility of high probability differential paths in differential attacks, as attackers find it difficult to infer key information by statistically analyzing input-output differential pairs. In addition, the maximum algebraic number of S-box Boolean functions in SMS4 reaches 7, ensuring its high linear complexity, making it difficult for linear approximation methods to effectively approximate the output of S-boxes, further enhancing its ability to resist differential analysis. The nonlinearity of the Boolean function is 112 (close to 120 of the Bent function),

indicating a high degree of maximum deviation between the output of the S-box and the linear function, effectively preventing attackers from approximating the S-box behavior using linear equations. The elliptic curve is an algebraic curve with genus 1. All points on an elliptic curve can form an addition group, set an elliptic curve *D*, then the elliptic curve satisfies:

$$y = \left(x^3 + ix + j\right)^{\frac{1}{2}} \tag{1}$$

Among them *i*, *j* and *x* belongs to the same number field, and *i*, *j* is a known constant. The equation of Equation (1) is called weierstrass equation, which is mainly used to study the properties and behaviors of elliptic curves. In SM2 algorithm, finite field C_r denotes this number field, where *r* is an odd prime or a square power of 2.

In the affine coordinate system of the prime field, the points of an elliptic curve form an exchange group according to the following law:

1) Addition of two infinity points: the K+K=K.
2) ∀A=(x,y)∈D(C_r)\{K}, A+K=K+A=A, of which A is the public key.
3) ∀A=(x,y)∈D(C_a)\{K}, the inverse element of A, the −A=(x,−y),A+(−A)=K.
4) The rule of addition of distinct points: set $A_1=(x_1,y_1)\in D(C_a)\backslash\{K\}$, $A_2=(x_2,y_2)\in D(C_a)\backslash\{K\}$, and $x_1\neq x_2$. Set $A_3=(x_3,y_3)=A_1+A_2$, then the dot-add operation is:x_1^2

$$\begin{cases} x_3 = \alpha^2 - x_1 - x_2 \\ y_3 = \alpha\left(x_1 - x_3\right) - y_1 \end{cases} \tag{2}$$

Among them, $\alpha=(y_2-y_1)/(x_2-x_1)$, express the slope of the vector consisting of the A_1 and A_2.

5) Multiplier rule

Set $A_1=(X_1, Y_1)\in D(C_a)\backslash\{K\}$, and $y_1\neq 0$, $A_3=(x_3, y_3)=A_1+A_2$, then the multiplication point operation is expressed through Equation (3).

$$\begin{cases} x_3 = \alpha^2 - 2x_1 \\ y_3 = \alpha\left(x_1 - x_3\right) - y_1 \end{cases} \tag{3}$$

Among them, $\alpha=(3x_1^2+g)/2y_1$, g is a constant.

SM2 algorithm mainly includes three parts. They are digital signature verification algorithm, key exchange protocol and public key encryption and decryption algorithm Mahdavi *et al*. [14]. Using public key encryption and decryption algorithms for encrypting and decrypting digital archive information Babu *et al*. [1]. The sender of digital archive information encrypts the digital archive information that he wants to send with the public key of the receiver of digital archive information, while the receiver of digital archive information obtains the real digital archive information Lyu *et al*. [13] by decrypting with the corresponding private key.

The encryption process of SM2 algorithm is as follows. Assume that the digital archive information is S, l is the bit length of S F is the base point. m is the order of the base point. When the encrypted user U, who is the sender of the digitized file message, encrypts the plaintext S, the following algorithmic steps should be followed:

- *Step* 1: Generate a random number n∈[1, m−1].
- *Step* 2: Calculate $H_1=[n]F=(x_1,y_1)$.
- *Step* 3: Verify the public key A, calculate Q=[h]A. Among them. h is a fixed value that represents the horizontal coordinates of a point on an elliptic curve. If Q is the infinity point K, then report an error and exit.
- *Step* 4: Calculate $[n]A=(x_2,y_2)$.
- *Step* 5: Calculate $w=KDF(x_2//y_2,l)$. Among them, KDF(·) is a key derivation function that can derive the desired key from the original key material. If w all are 0, then return to step 1.
- *Step* 6: Calculate, $H_2=S\oplus w$,⊕ denotes a different-or operation.
- *Step* 7: Calculate $H_3=hash(x_1\|S\|y_2)$, hash(·) denotes a hash operation.
- *Step* 8: Output the ciphertext $H=H_1\|H_2\|H_3$.

The SM2 decryption algorithm operation process corresponds to the encryption operation process, Set the bit length of the ciphertext H_2 be l. Decryption user V as recipients of messages from digitized archives for received digitized archival information ciphers $H=H_1\|H_2\|H_3$ to perform the decryption operation, the specific arithmetic steps are as follows:

- *Step* 1: Validate H_1 in H whether it is on the given elliptic curve equation or not, if not, report an error and exit.
- *Step* 2: Calculate $Q=[h]H_1$. If Q is the infinity point K, then report an error and exit.
- *Step* 3: Calculate $[n]H_1=(x_2,y_2)$.
- *Step* 4: Calculate $w=KDF(x_2//y_2,l)$. If w all are 0, then report an error and exit.
- *Step* 5: Remove H_2 from H, calculate $S'=H_2\oplus W$.
- *Step* 6: Calculate $t=hash(x_2\|S'\|y_2)$. Remove H_3 from H, if $t\neq H_3$, then report an error and exit.
- *Step* 7: Output the plaintext *S*'.

SM4 algorithm is a symmetric block cipher algorithm, whose packet length and key length are 128 bits. The algorithm adopts a 32 round nonlinear iterative structure, and encrypts words (32 bits) as a unit. Both encryption algorithm and key expansion algorithm adopt 32 rounds of nonlinear iterative structure, in which each iteration is a round of nonlinear transformation. The main operations include Exclusive OR (XOR), synthetic replacement, nonlinear iteration, reverse order transformation, cyclic shift and S-box transformation Kim *et al*. [9]. This algorithm is a symmetric block cipher algorithm Ragesh and Kumar [16] for commercial purposes. The message packet length and key length of SM4 algorithm are 128 bits, as shown in Figure 2.

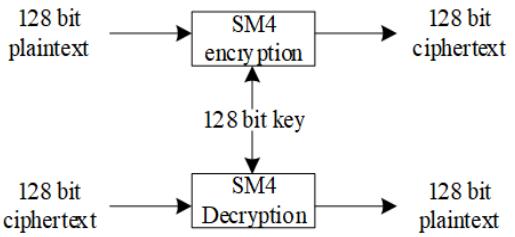


Figure 2. Encryption and decryption process of SM4 algorithm.

In the algorithm, the encryption and decryption part used to process the digital archive message and the extension part used to obtain the round key are designed using the 32 round feistel nonlinear iteration structure. Feistel nonlinear iteration is an encryption algorithm structure in cryptography, mainly used in the design of block cipher Hallaji *et al*. [7]. Each round of encryption process mainly includes XOR, non-linear transformation, and linear transformation operations. The nonlinear transformation in the algorithm calls four 8-bit output permutation s-boxes. The s-box in the SM4 algorithm is a nonlinear substitution transformation, in bytes. Its essence is 8-bit nonlinear substitution. The input and output of box S are 8-bit bytes. It maps the input bytes to the output bytes. The s-box is a fixed byte substitute, which replaces each input byte by finding a predefined S box. The SM4 decryption algorithm is similar to the encryption process, and only needs to change the order of key use. That is, the round key Geetha and Deepa [6] used for decryption of digital archive information can be obtained by simply reversing the sequence of the round key used for encryption of digital archive information.

The specific process of SM4 algorithm is described in detail below. Each round of encrypted digital file message length of the algorithm is 32 bits. Use ϕ_2^z in algorithm denote the set of vectors of bits with the length of z, so that an element in ϕ_2^{32} is a word. An element in ϕ_2^8 is a byte. The structure of SM4 algorithm is as follows:

Let the input digitized archive information plaintext be that $(\beta_0, \beta_1, \beta_2, \beta_3)\in(\phi_2^{32})^4$, the output of the digitized archival information is ciphered as $(x_0, x_1, x_2, x_3)\in(\phi_2^{32})^4$, the input for the p th round is $(\beta_p, \beta_{p+1}, \beta_{p+2}, \beta_{p+3})\in(\phi_2^{32})^4$, the digitized archive information round key used for the p th round is $\varepsilon_p\in\phi_2^{32}$, of which p=0,1,2, ,31. The process of SM4 algorithm performing a round of encryption operation is as follows:

$$\beta_{p+4} = \beta_p \oplus \gamma\left(\beta_{p+1} \oplus \beta_{p+2} \oplus \beta_{p+3} \oplus \varepsilon_p\right) \quad (4)$$

Among them$\gamma(\cdot)$is a combined function of nonlinear and linear functions.

Four parallel s-boxes are used in the nonlinear function, and the input is $(A_0, A_1, A_2, A_3)\in(\phi_2^8)^4$, the output is $(B_0, B_1, B_2, B_3)\in(\phi_2^8)^4$. Then:

$$B=(B_0,B_1,B_2,B_3)=\left(SBOX(A_0),SBOX(A_1),SBOX(A_2),SBOX(A_3)\right) \quad (5)$$

The output of a nonlinear function is the input of a linear function. Let the input be $B\in\phi_2^{32}$, the output is $C\in\phi_2^{32}$. Then:$C = B \oplus (B \lll 2) \oplus (B \lll 10) \oplus (B \lll 18) \oplus (B \lll 24)$.

Among them,$\oplus$ is a different-or operation, and B<<<2, B<<<10, B<<<18, B<<<24 respectively indicate that B shift left by 2 bits, shift left by 10 bits, shift left by 18 bits, shift left by 24 bits. The encryption process of SM4 algorithm is shown in Figure 3.

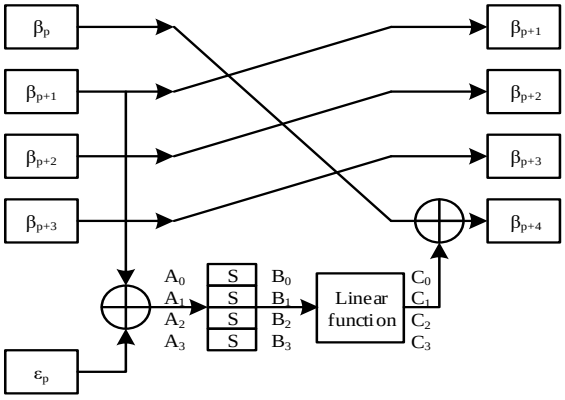


Figure 3. SM4 encryption process.

After 32 rounds of iterative operations, the ciphertext $(x_0, x_1, x_2, x_3)=(\beta_{35}, \beta_{34}, \beta_{33}, \beta_{32})$.

The SM4 algorithm's digital archive information decryption process is basically similar. When encrypting digital archive information, the sequence of round key is $(\varepsilon_0, \varepsilon_1, \ ,\varepsilon_{31})$. And when performing decryption of digitized archival information, the order of the round keys is $(\varepsilon_{31}, \varepsilon_{30}, \ ,\varepsilon_0)$.

2.3. Encryption of Digitized Archival Information

By taking advantage of the advantages of SM4 algorithm's fast encryption speed and SM2 algorithm's high encryption security, simple key management and low bandwidth requirements, a more efficient and secure encryption technology can be obtained by combining the two. The basic principle is that the sender randomly generates a random key of SM4 algorithm before the data is communicated in the network *Key* , use SM4 algorithm to encrypt the plaintext data of digital archive information to be transmitted, and then use SM2 algorithm to encrypt the Key. In this way, the receiver will decrypt the random Key with SM2 algorithm after receiving the encrypted data of the digital archive information and the encrypted key data Key, and then with this randomized key to decrypt the ciphertext SM4. Random key for each plaintext data encryption Key, they are all different. There is no SM4 Key management problem. This encryption and decryption scheme not only ensures data security but also improves the speed of encryption and decryption Linh and Yem. [20]. Thus, the network data can be transmitted safely, efficiently and quickly.

The process of hybrid encryption algorithm is: Let the sender of the digitized archive information be X, the recipients of digitized archival information be Y, the session key used for SM4 encryption is Key. The public key and the key of the recipient of the digitized archival message are denoted as PubKeyY, SecKeyY respectively. By mixing SM2 and SM4, the flow of plaintext data transmission in the encryption method is shown in Figure 4.

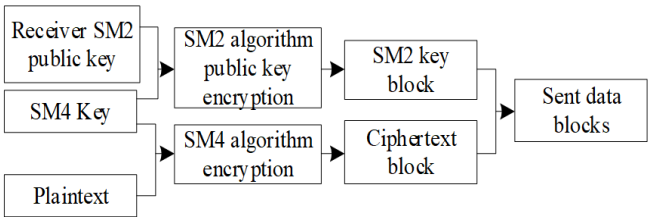


Figure 4. SM2 and SM4 hybrid algorithm encryption process.

The specific process of hybrid algorithm encryption is:

- *Step* 1: The sender X of the digitized archival information randomly generate keys for encryption and decryption of SM4 algorithm Key.
- *Step* 2: The sender X of the digitized archive information obtain the public key of SM2 algorithm published by the receiver from the key server *PubKeyY* .
- *Step* 3: The sender X of the digitized archive information use SM4 algorithm key SM4 encryption to perform on the clear text of the digital file to obtain the ciphertext block.
- *Step* 4: The sender X of the digitized archive information use the receiver public key PubKeyY for SM2 algorithm encryption key to get the Key block.
- *Step* 5: The sender X of the digitized archive information use ciphertext block and the key block are added together to form the send data.

Hybrid algorithms to achieve the process of decryption of digitized archive information for the reverse process of encryption of digitized archive information, digitized archive information received by the receiver of the ciphertext decryption to go through the following steps, as shown in Figure 5.

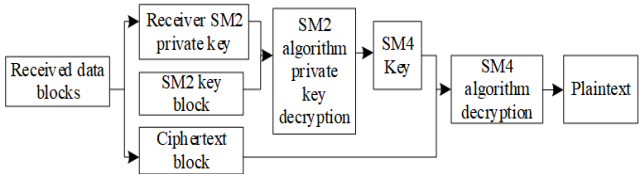


Figure 5. SM2 and SM4 hybrid algorithm decryption process.

The specific process of decryption of digitized archival information by hybrid algorithms is:

- *Step* 1: The recipient of the digitized archival information Y divides the data into ciphertext blocks and key blocks.
- *Step* 2: The receiver of the digital archive information Y uses the SM2 private key SecKeyY to decrypt the key block by SM2 to obtain the SM4 Key.
- *Step* 3: The recipient of the digitized archival information Y uses SM4 Key SM4 decrypts the ciphertext block to get the plaintext.

Through the above process, the encryption and decryption process of digital archives information can be realized, so as to realize the security protection of digital archives information.

2.4. Establish an Authentication Mechanism

In order to ensure the security of data and the consistency of information between the two parties, SM2 hybrid state secret algorithm is used to establish the authentication mechanism of the archive system. Use the SM2 national security encryption algorithm to set up digital certificates for users to achieve verification and signature functions. When the receiving end receives the data information sent by the archive system, the unique verification key is used to decrypt the data. The data transmission process based on this is as follows. Suppose that user A wants to send a specific data to user B, this A only needs to use its own private key to encrypt the data. The encryption key tested is to sign the data. After user B receives the encrypted file, it uses user A's public key to decrypt the encrypted data to obtain the corresponding correct information.

The basis for realizing this process is that user A's signature on the transmission data can be confirmed and cannot be forged. In addition, in order to improve the security of data, this paper sets the reuse attribute and tamper proof attribute for signatures. In accordance with the above principles, when using the hybrid national security encryption algorithm in section 2.3 to calculate digital signatures, this paper sets the signature length L as a multiple of 64, while constraining its maximum value not to be greater than 1024, and the minimum value not to be less than 512. Correspondingly, the prime factor length of the digital signature is L-1. Under the effect of the random number k, combine H (x): one-way hash function calculation signature.

Firstly, randomly generate k, make sure k<L, at the same time, calculate:

$$r = \left[g^k \bmod (L-1) \right] \bmod L \tag{6}$$

Among them, the digital signature uses r to express, transmission data size is g, where it is operated on by the number of characters.

Secondly, the signed data information can be described as:

$$s = \left[k^{-1} H(m) + xr \right] \bmod L \tag{7}$$

Where: s represents signed data the information; m represents data information to be transmitted; x represents the key. Finally, the encryption of the

transmitted data is completed by Equations (6) and (7), and the calculation method of the receiver's identity authentication can be expressed as:

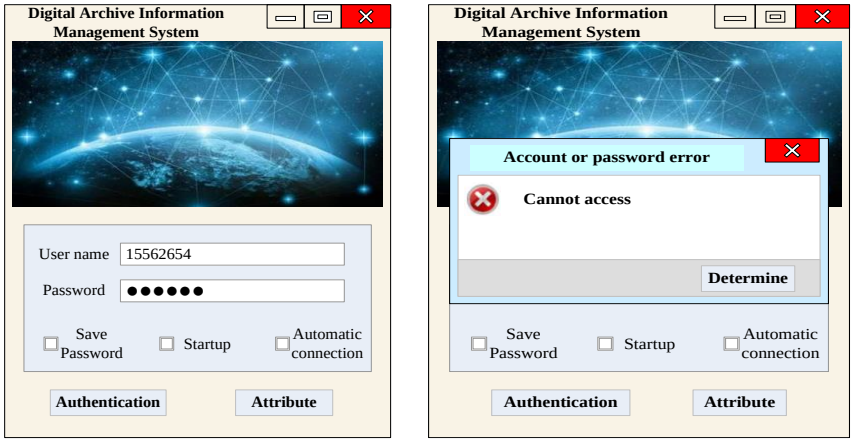
$$\begin{cases} w = s^{-1} \bmod L \\ u_1 = [H(m) \times w] \bmod L \\ u_2 = [r \times w] \bmod L \\ v = \left[(g^{u} l \times y^{u_2}) \bmod (L-1) \right] \bmod L \end{cases} \quad (8)$$

Where: w represents the key distribution parameter; u_1 and u_2 denote the conversion parameters for validation, respectively; the v indicates the signature information output by the receiver. y indicates the public key information. When v=r is established, then the authentication is passed and the data transmission is carried out; when v=r is not the case, the data encryption is rejected without verification. By the above way, the data can be encrypted safely and accurately.

3. Experimental Analysis

In order to verify the effectiveness of the algorithm in this paper to achieve digital archive information security protection, a financial enterprise is taken as the research object for algorithm analysis. The enterprise's digital archive information includes contract management, intellectual property protection, human resource management and other aspects of archive management. Digital archive information includes various types, such as text, pictures, audio, video, etc. The enterprise stores digital archive information into a computer, which is equipped with Intel Core i5-10400 processor, has 8GB DDR4 2666MHz memory and 256GB M.2 NVMe SSD hard disk.

The reality of the login page of the digitized file information management system of this financial enterprise is shown in Figure 6.



a) Management system login page. b) Management system login failure page.

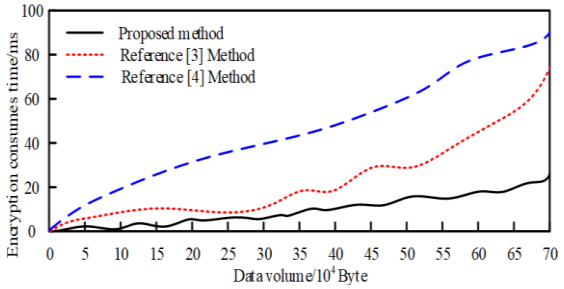
Figure 6. Digital file information management system page.

As can be seen in Figure 6, when a user tries to access the system, he or she first needs to pass through the authentication barrier. Only when the input account and password match the data recorded in the system, the user can successfully enter the system. If the authentication is not passed, the system will not only reject the user's access request, but also display a pop-up window on the screen, clearly informing the user of account or password errors, and to prevent further operations, which greatly enhances the security of digitized archival information. Even in the face of unknown intruders, it can effectively prevent their malicious behavior to ensure the security of archived information. Therefore, through the algorithm in this paper to achieve a better protection of digital archive information, can effectively prevent the unknown invasion.

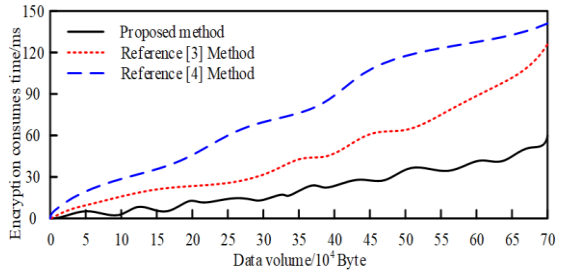
In order to further verify the effectiveness of the method of this paper, for the method of this paper to achieve the effect of the encryption and decryption process of digitized archival information research, the method of this paper and the method of Couvreur and Lequesne [3]. and the method of Dong and Yang [4]. of different forms of encryption process of digitized archival information to consume the time of the case of comparison, the results are shown in Figure 7.

As can be seen from Figure 7, for different types of digitized archive information, the time consumption required for the encryption process varies greatly. The algorithm introduced in this paper shows high efficiency and advantages in encryption of digitized archive information in text form when dealing with different types of digitized archive information. This efficient performance makes the algorithm has a wide range of application prospects in practical applications, and provides a strong support for guaranteeing the security of digitized archive information. For text encryption, the proposed method consistently exhibits lower Central Processing Unit (CPU) and memory utilization compared to the reference method, thereby enhancing its efficiency advantage. In image encryption, although CPU usage increases moderately with the increase of data volume, memory consumption remains stable, indicating effective resource management. For video encryption with significantly large data volumes, the proposed method shows a gradual increase in CPU and memory usage, but is slower than the reference method.

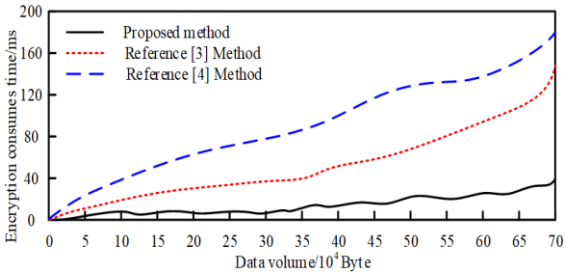
These findings indicate that the proposed method not only performs well in terms of encryption speed, but also maintains better scalability, making it suitable for large-scale digital archive protection.



a) Digital file information encryption time in the form of text.



b) Digital file information encryption time in the form of pictures.



c) Digital file information encryption time in the form of video.

Figure 7. Different forms of digital file information encryption process time consumption.

In order to further the effect of information security protection of digitized archives realized by the algorithm of this paper, the access records of the digitized archive information management system of the experimental financial enterprises within 10 days are counted, and the results obtained are shown in Table 1.

Table 1. Access records of the digital archival information management system of financial enterprises in the experiment.

Serial number	Accessed	Verified	Accessing IP addresses	Malicious behavior exists	Whether to intercept
1	2021/3/24, 5:17:20	No	231.143.26.0	Malicious login	Blocked
2	2021/3/24, 14:35:00	No	224.454.23.0	Malicious login	Blocked
3	2021/3/25, 9:17:00	Yes	121.114.56.0	/	/
4	2021/3/25, 19:33:00	No	152.123.30.0	Malicious login	Blocked
5	2021/3/26, 14:09:00	Yes	121.114.56.0	/	/
6	2021/3/27, 8:11:00	No	114.79.125.0	Virus implantation	Blocked
7	2021/3/28, 10:57:00	Yes	121.114.56.0	/	/
8	2021/3/28, 12:05:00	No	132.521.69.0	Malicious login	Blocked
9	2021/3/29, 9:14:00	No	125.38.146.0	Malicious login	Blocked
10	2021/3/30, 9:23:00	Yes	121.114.56.0	/	/
11	2021/3/30, 14:32:00	No	224.61.43.0	Malicious login	Blocked
12	2021/3/31, 10:42:00	No	129.118.12.0	Malicious login	Blocked
13	2021/4/1, 8:25:00	Yes	121.114.56.0	/	/
14	2021/4/1, 15:34:00	No	256.38.29.0	Virus implantation	Blocked
15	2021/4/2, 13:48:00	No	121.114.56.0	Malicious login	Blocked

It can be seen from Table 1 that the digital archive information security protection system realized by the algorithm described in this paper has a significant effect in protecting digital archive information security. The system can not only effectively prevent malicious login behavior, but also intercept such behavior immediately when it is detected, thus ensuring the security of file information. The system can also accurately record the intrusion time and corresponding IP address while intercepting malicious logins. This function not only provides key information for subsequent investigation, but also provides further proof for the security of the system.

In order to further verify the effectiveness of the digital archive information security protection realized by the algorithm in this paper, the network vulnerability

detection is carried out through the network vulnerability checking and killing software on the experimental digital archive information management system of financial enterprises, and the detection results obtained are shown in Figure 8.

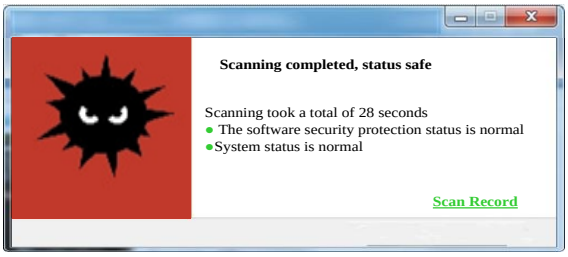


Figure 8. Network vulnerability detection software test result.

It can be seen from Figure 8 that comprehensive detection is carried out with the help of network vulnerability detection software. The results show that the system is in a stable and normal operation state, and no malicious acts or potential security threats have been found. This result strongly proves that the algorithm proposed in this paper has significant advantages in the security protection of digital archive information. It is a method with high protection performance, which not only improves the security protection capability of digital archive information management system, but also ensures the security and integrity of enterprise digital archive information.

In order to further verify the performance of the algorithm proposed in this article in digital archive information security protection, the CPU usage rate was used as the test indicator, and a hybrid encryption method of Advanced Encryption Standard-Galois Counter Mode (AES-GCM) and Rivest Shamir Adleman (RSA) was introduced as the comparative test indicator. The specific experimental values are shown in Table 2.

Table 2. CPU usage testing using different methods.

Number of tests	Proposed method	AES-GCM method	RSA hybrid method
1	25	33	44
2	22	38	49
3	18	35	46
4	15	31	39
5	21	39	47

From Table 2, it can be seen that in the 5 comparative tests, the encryption method proposed in this paper has shown good performance in terms of CPU usage. Compared with the hybrid encryption method of AES-GCM and RSA, the CPU usage of this method is relatively low. This indicates that the method proposed in this article has higher efficiency and better resource management capabilities in digital archive information security protection, further demonstrating its feasibility and superiority in practical applications.

4. Conclusions

In order to ensure the security and integrity of digital archive information, the research method of digital archive information security protection based on state secret algorithm is proposed. Through the combination of SM2 algorithm and SM4 algorithm based on the national secret algorithm, taking full advantage of the advantages of fast encryption speed of SM4 algorithm and high security of SM2 algorithm encryption, simple key management and low bandwidth requirements, the digital file information data encryption is realized through hybrid algorithm. The experimental results show that the proposed method has a good protective effect on digital archive information and can effectively block unknown intrusions. When dealing with different types of digital archive information, it shows high efficiency and advantages, providing a solid backing for maintaining the security of digital archive information. However, the encryption efficiency of this method still needs to be improved in the encryption of digital archive information of pictures and videos. Therefore, further research is needed on this algorithm to make it more perfect, so as to achieve better security protection of digital archive information.

The digital archive information security protection scheme based on national secret algorithms (including SM2, SM4, etc.,) proposed in this article has undergone rigorous experimental verification and performance evaluation, demonstrating high security and attack resilience. In response to the potential side channel attacks that the SM2 algorithm may face, this solution effectively reduces the risk of information leakage by optimizing the algorithm implementation and hardware deployment.

Funding

Zhengzhou City level Project, Research on the Ideas and Key Measures for Promoting the Development of Big Data Industry in Zhengzhou City; Project number: ZSLX20220981.

References

[1] Babu R., Jayashree K., Viswanathan K., and Vijay K., “An Efficient Spam Detector Model for Accurate Categorization of Spam Tweets Using Quantum Chaotic Optimization-Based Stacked Recurrent Network,” *Nonlinear Dynamics*, vol. 111, no. 19, pp. 18523-18540, 2023. https://doi.org/10.1007/s11071-023-08697-z

[2] Brahim A., Pacha A., and Said N., “A New Fast Image Compression-Encryption Scheme Based on Compressive Sensing and Parallel Blocks,” *Journal of Supercomputing*, vol. 79, no. 8, pp. 8843-8889, 2023. https://doi.org/10.1007/s11227-022-04999-y

[3] Couvreur A. and Lequesne M., “On the Security of Subspace Subcodes of Reed-Solomon Codes for Public Key Encryption,” *IEEE Transactions on Information Theory*, vol. 68, no. 1, pp. 632-648, 2022. https://doi.org/10.1109/TIT.2021.3120440

[4] Dong Y. and Yang Y., "Simulation of Digital Reconstruction of Building Model Based on Improved Minimum Spanning Tree," *Computer Simulation*, vol. 40, no. 3, pp. 197-201, 2023.
[5] Farah K., Chabir K., and Abdelkrim M., "High Level Petri Nets-Based Proposal of an Integrated Intrusion Detection and Prevention Mechanism in Network Controlled Systems," *IET Communications*, vol. 17, no. 4, pp. 469-477, 2023. https://doi.org/10.1049/cmu2.12557
[6] Geetha T. and Deepa A., "A FKPCA-GWO WDBiLSTM Classifier for Intrusion Detection System in Cloud Environments," *Knowledge-Based Systems*, vol. 253, pp. 1-14, 2022. https://doi.org/10.1016/j.knosys.2022.109557
[7] Hallaji E., Far R., Saif M., and Viedma E., "Label Noise Analysis Meets Adversarial Training: A Defense Against Label Poisoning in Federated Learning," *Knowledge-Based Systems*, vol. 266, pp. 1-10, 2023. https://doi.org/10.1016/j.knosys.2023.110384
[8] Khan A., Shaikh A., Cheikhrouhou O., Laghari A., and et al., "IMG-Forensics: Multimedia-Enabled Information Hiding Investigation Using Convolutional Neural Network," *IET Image Processing*, vol. 16, no. 11, pp. 2854-2862, 2023. https://doi.org/10.1049/ipr2.12272
[9] Kim J., Jeon D., Seong J., Badloe T., and et al., "Photonic Encryption Platform via Dual-Band Vectorial Metaholograms in the Ultraviolet and Visible," *ACS Nano*, vol. 16, no. 3, pp. 3546-3553, 2023. https://doi.org/10.1021/acsnano.1c10100
[10] Krishna R., Kumar G., Terlapu P., Jayaram D., and Samreen S., "Trust Enabled Secure Routing in Vehicular Adhoc Networks," *The International Arab Journal of Information Technology*, vol. 22, no. 3, pp. 592-613, 2025. DOI: 10.34028/iajit/22/3/13
[11] Lin C., Pham D., and Huynh T., "Encryption and Decryption of Audio Signal and Image Secure Communications Using Chaotic System Synchronization Control by TSK Fuzzy Brain Emotional Learning Controllers," *IEEE transactions on Cybernetics*, vol. 52, no. 12, pp. 13684-13698, 2022. https://doi.org/10.1109/TCYB.2021.3134245
[12] Linh D. and Yem V., "A Turbo-Based Encryption and Coding Scheme for Multiple-Input Multiple-Output Orthogonal Frequency Division Multiplexing Wireless Communication Systems Affected by Doppler Frequency Offset," *IET Communications*, vol. 17, no. 5, pp. 632-640, 2023. https://doi.org/10.1049/cmu2.12568
[13] Lyu M., Gharakheili H., and Sivaraman V., "A Survey on DNS Encryption: Current Development, Malware Misuse, and Inference Techniques," *ACM Computing Surveys*, vol. 55, no. 8, pp. 1-28, 2023. https://doi.org/10.1145/3547331
[14] Mahdavi E., Fanian A., Mirzaei A., and Taghiyarrenani Z., "ITL-IDS: Incremental Transfer Learning for Intrusion Detection Systems," *Knowledge-Based Systems*, vol. 253, pp. 1-17, 2022. https://doi.org/10.1016/j.knosys.2022.109542
[15] Moizuddin M. and Jose M., "A Bio-Inspired Hybrid Deep Learning Model for Network Intrusion Detection," *Knowledge-Based Systems*, vol. 238, pp. 1-20, 2022. https://doi.org/10.1016/j.knosys.2021.107894
[16] Ragesh G. and Kumar A., "Trust-Based Secure Routing and Message Delivery Protocol for Signal Processing Attacks in IoT Applications," *Journal of Supercomputing*, vol. 79, no. 3, pp. 2882-2909, 2023. https://doi.org/10.1007/s11227-022-04766-z
[17] Rani N., Mishra V., and Sharma S., "Image Encryption Model Based on Novel Magic Square with Differential Encoding and Chaotic Map," *Nonlinear Dynamics*, vol. 111, no. 3, pp. 2869-2893, 2023. https://doi.org/10.1007/s11071-022-07958-7
[18] Shaw S. and Dutta R., "Forward Secure Offline Assisted Group Key Exchange from Isogeny-Based Blinded Key Encapsulation Mechanism," *IEEE Transactions on Information Theory*, vol. 69, no. 7, pp. 4708-4722, 2023. https://doi.org/10.1109/TIT.2023.3260005
[19] Shikder A., Kumar P., and Nishchal N., "Image Encryption by Structured Phase Encoding and Its Effectiveness in Turbulent Medium," *IEEE Photonics Technology Letters*, vol. 35, no. 3, pp. 128-131, 2023. https://doi.org/10.1109/LPT.2022.3226200
[20] Vu L., Nguyen Q., Nguyen D., Hoang D., and Dutkiewicz E., "Deep Generative Learning Models for Cloud Intrusion Detection Systems," *IEEE Transactions on Cybernetics*, vol. 53, no. 1, pp. 565-577, 2022. https://doi.org/10.1109/TCYB.2022.3163811

Fen Wang obtained her Bachelor's degree in Information Management and Information System from Zhongyuan University of Technology in 2006; Master's degree in Business Management from Zhongyuan University of Technology in 2009; Doctor's degree in Business Administration, Namseoul University in 2024; research direction: Information Management. Work experience: 2009-present, Zhengzhou University of Economics and Business, teacher. Academic status: Published 15 academic papers, published 4 academic books and textbooks, and participated in 8 research projects.