

Typical Applications of Matrices in Cryptography and Their Theoretical Support for Efficient and Green Intelligent Computing

Siyu Yang, Meimei Zhang * and Yiting Li

School of Mathematical Sciences, Changsha Normal University, Changsha, Hunan, China

* Corresponding author: Meimei Zhang (Email: ynuhzhangmeimei@163.com)

Abstract: As the core content of linear algebra, matrices provide basic mathematical support for many algorithms in artificial intelligence (AI). The characteristic of efficient computation in matrix theory facilitates the dual improvement of the performance and energy efficiency of AI algorithms. This paper focuses on the typical applications of matrices in cryptography, aiming to provide theoretical support for constructing an efficient and green intelligent computing path. Research shows that as a bridge connecting mathematical theory and technological applications, matrices not only occupy a fundamental position in the development of AI but also possess extensive research value and profound social significance.

Keywords: Matrix; Artificial Intelligence (AI); Cryptography.

1. Introduction

Matrix, as one of the core tools in mathematics, is not only an important object of theoretical research, but also demonstrates strong application value in cutting-edge technological fields such as artificial intelligence. Matrix theory supports the entire process of artificial intelligence technology development, from optimizing underlying algorithms to implementing upper level applications [1][2]. In recent years, artificial intelligence technology has experienced explosive growth. At the application level, AI technology itself is showing a trend of "matrix" development, from intelligent agent collaboration to multimodal large models, matrix architecture is becoming a key paradigm for integrating complex AI applications[3]. However, there is still a lack of systematic and cross level application of matrices in the field of AI, especially in the comprehensive analysis of combining national strategic needs with technological breakthroughs. Therefore, this article aims to deepen the understanding of matrices as the "arithmetic foundation" for AI development through cross perspective integration analysis, provide theoretical references for related research, and strengthen the importance of interdisciplinary integration in responding to major national strategic needs[4][5].

2. The Application of Matrix in Cryptography

In recent years, the proposal of the "dual carbon" target not only signifies the urgency of energy conservation and emission reduction, but also emphasizes the importance of optimizing industrial structure. Cryptography has built a trusted data foundation for the implementation of the "dual carbon" strategy by ensuring the authenticity, transmission security, and privacy of carbon data[6]. Matrix, as the "arithmetic foundation" for the development of AI, not only provides mathematical support for its development, but also has profound significance for social and economic transformation and interdisciplinary innovation. Its application value and potential are worth exploring continuously.

2.1. The Basic Principles of Matrix in Cryptography

In cryptography, matrix encryption relies on linear algebra theory to construct a clear and efficient security mechanism. The core process can be summarized as follows: first, digitize the plaintext, for example

Table 1. Password book

Characters	A	B	C		X	Y	Z	0	1		9	Spaces
Numbers	1	2	3		24	25	26	27	28		36	0

Using a codebook (such as an alphanumeric correspondence table) to convert textual information into numerical sequences; Then arrange these values into a clear matrix according to the dimension requirements of the encryption matrix. During the encryption phase, a reversible matrix should be selected as the encryption key to ensure the feasibility of decryption operations. By left-multiplying the plaintext matrix with key matrix A_1 and right-multiplying it with key matrix A_2 , a ciphertext matrix is generated to achieve dual encryption and improve the security of the

password. When decrypting, the receiver needs to multiply the inverse of the left multiplication key matrix A_1 and the inverse of the right multiplication key matrix A_2 to restore the original plaintext matrix, and finally recover the plaintext information through the reverse transformation of the codebook. This process demonstrates the rigor and effectiveness of matrices as linear transformation tools in information encoding and decoding[7][8].

2.2. Application Examples

Here, we use matrix operations to encrypt and decrypt the information 'CarbonNeutrality by 2060', demonstrating the crucial role of matrix tools in national security and strategic implementation.

Assumption 1: The corresponding relationship between symbols and numbers is shown in Table 1.

Assumption 2: Assuming that the characters in "CARBONNEUTRALITYBY2060" are grouped from left to right, with 4 characters per group. Two spaces are added after 2060, and the corresponding numbers are used as columns of the matrix, resulting in a matrix with 4 rows. After encryption, it remains a matrix with 4 rows and its elements are integers.

Step 1: Information matrixization

Convert the information "CARBONNEUTRALITYBY2060" into a matrix by comparing it with the table

$$A_1 M = \begin{pmatrix} 3 & 13 & 11 & 9 \\ 15 & 1 & 5 & 12 \\ 4 & 20 & 25 & 12 \\ 5 & 8 & 8 & 0 \end{pmatrix} \begin{pmatrix} 3 & 15 & 21 & 12 & 2 & 33 \\ 1 & 14 & 20 & 9 & 25 & 27 \\ 18 & 14 & 18 & 20 & 29 & 0 \\ 2 & 5 & 1 & 25 & 27 & 0 \end{pmatrix} = \begin{pmatrix} 238 & 426 & 530 & 598 & 893 & 450 \\ 160 & 369 & 437 & 589 & 524 & 522 \\ 506 & 750 & 946 & 1028 & 1557 & 672 \\ 167 & 299 & 409 & 292 & 442 & 381 \end{pmatrix} = B.$$

To increase the security of password transmission, we multiply a reversible key matrix by right on this basis

$$A_2 = \begin{pmatrix} 1 & 2 & 1 & 1 & 2 & 3 \\ 3 & 4 & 2 & 1 & 1 & 1 \\ 4 & 2 & 3 & 2 & 2 & 1 \\ 2 & 2 & 1 & 4 & 1 & 3 \\ 3 & 3 & 2 & 1 & 1 & 2 \\ 2 & 1 & 1 & 2 & 2 & 2 \end{pmatrix}.$$

Encrypt again to obtain

$$B A_2 = \begin{pmatrix} 238 & 426 & 530 & 598 & 893 & 450 \\ 160 & 369 & 437 & 589 & 524 & 522 \\ 506 & 750 & 946 & 1028 & 1557 & 672 \\ 167 & 299 & 409 & 292 & 442 & 381 \end{pmatrix} \begin{pmatrix} 1 & 2 & 1 & 1 & 2 & 3 \\ 3 & 4 & 2 & 1 & 1 & 1 \\ 4 & 2 & 3 & 2 & 2 & 1 \\ 2 & 2 & 1 & 4 & 1 & 3 \\ 3 & 3 & 2 & 1 & 1 & 2 \\ 2 & 1 & 1 & 2 & 2 & 2 \end{pmatrix} = \begin{pmatrix} 8411 & 7565 & 5514 & 5909 & 4353 & 6150 \\ 6809 & 5942 & 4368 & 5327 & 3720 & 5145 \\ 14611 & 13303 & 9658 & 10161 & 7583 & 10756 \\ 5372 & 4639 & 3549 & 3656 & 2947 & 3731 \end{pmatrix} = C.$$

Step 3: Information Decryption

After obtaining the ciphertext matrix C , we need to find

$$A_1^{-1} C A_2^{-1} = \begin{pmatrix} -32 & 184 & -160 & 39 \\ 4169 & 4169 & 4169 & 379 \\ 752 & -155 & -409 & 31 \\ 4169 & 4169 & 4169 & 379 \\ -732 & 40 & 509 & -8 \\ 4169 & 4169 & 4169 & 379 \\ 77 & 31 & 2 & -48 \\ 1137 & 1137 & 379 & 379 \end{pmatrix} \begin{pmatrix} 8411 & 7565 & 5514 & 5909 & 4353 & 6150 \\ 6809 & 5942 & 4368 & 5327 & 3720 & 5145 \\ 14611 & 13303 & 9658 & 10161 & 7583 & 10756 \\ 5372 & 4639 & 3549 & 3656 & 2947 & 3731 \end{pmatrix} \begin{pmatrix} -7 & -7 & -25 & -7 & 5 & 55 \\ 9 & 54 & 54 & 27 & 6 & 54 \\ 1 & 14 & -4 & 1 & -1 & -2 \\ 9 & 27 & 27 & 27 & 3 & 27 \\ 7 & -10 & 26 & 7 & -1 & -41 \\ 9 & 27 & 27 & 27 & 3 & 27 \\ 0 & 1 & 1 & 1 & -1 & -1 \\ 2 & 6 & 6 & 3 & 2 & 6 \\ 9 & 27 & 27 & 27 & 3 & 27 \\ 1 & -13 & -4 & 1 & 2 & -2 \\ 9 & 27 & 27 & 27 & 3 & 27 \end{pmatrix}$$

$$= \begin{pmatrix} 3 & 15 & 21 & 12 & 2 & 33 \\ 1 & 14 & 20 & 9 & 25 & 27 \\ 18 & 14 & 18 & 20 & 29 & 0 \\ 2 & 5 & 1 & 25 & 27 & 0 \end{pmatrix} = M.$$

$$M = \begin{pmatrix} 3 & 15 & 21 & 12 & 2 & 33 \\ 1 & 14 & 20 & 9 & 25 & 27 \\ 18 & 14 & 18 & 20 & 29 & 0 \\ 2 & 5 & 1 & 25 & 27 & 0 \end{pmatrix}.$$

Step 2: Information Encryption

Translate 'CODEMATHKEYHILL' and add a space as the encryption key matrix

$$A_1 = \begin{pmatrix} 3 & 13 & 11 & 9 \\ 15 & 1 & 5 & 12 \\ 4 & 20 & 25 & 12 \\ 5 & 8 & 8 & 0 \end{pmatrix}.$$

It is easy to know that the determinant of the matrix is not 0, and the matrix is invertible. Perform one round of encryption by left-multiplying the plaintext matrix with the key matrix A_1

the inverse matrix of A_1 and the inverse matrix of A_2 .

$$A_1^{-1} = \begin{pmatrix} -32 & 184 & -160 & 39 \\ 4169 & 4169 & 4169 & 379 \\ 752 & -155 & -409 & 31 \\ 4169 & 4169 & 4169 & 379 \\ -732 & 40 & 509 & -8 \\ 4169 & 4169 & 4169 & 379 \\ 77 & 31 & 2 & -48 \\ 1137 & 1137 & 379 & 379 \end{pmatrix},$$

$$A_2^{-1} = \begin{pmatrix} -7 & -7 & -25 & -7 & 5 & 55 \\ 9 & 54 & 54 & 27 & 6 & 54 \\ 1 & 14 & -4 & 1 & -1 & -2 \\ 9 & 27 & 27 & 27 & 3 & 27 \\ 7 & -10 & 26 & 7 & -1 & -41 \\ 9 & 27 & 27 & 27 & 3 & 27 \\ 0 & 1 & 1 & 1 & -1 & -1 \\ 2 & 6 & 6 & 3 & 2 & 6 \\ 9 & 27 & 27 & 27 & 3 & 27 \\ 1 & -13 & -4 & 1 & 2 & -2 \\ 9 & 27 & 27 & 27 & 3 & 27 \end{pmatrix},$$

Then, decrypt $M = A_1^{-1} C A_2^{-1}$ to recover the plaintext.

Finally, by comparing the plaintext matrix with the ciphertext, the information obtained is "CARBONNEUTRALITYBY2060".

In the field of cryptography, matrices have become the core tool for information encryption and decryption due to their unique mathematical structure and computational properties. At the same time, matrix tools have irreplaceable value in national security and strategic implementation. From basic character replacement to advanced public key cryptography, from data integrity verification to forward-looking research on quantum encryption, matrix theory has always provided solid support for the underlying logic of information security.

3. Summary

As the core tool of linear algebra, matrices play a fundamental supporting role in the field of artificial intelligence, and their application value is particularly prominent in cryptography. Matrix based encryption algorithms, such as dynamic encryption schemes based on bidirectional mapping matrices or multivariate public key cryptography systems, significantly enhance the unpredictability of keys and the system's resistance to attacks by constructing randomized, highly complex matrix operation structures. Facing the future, in order to address the security challenges brought by emerging technologies such as quantum computing, matrix encryption technology needs to further evolve into higher-order and more complex forms, such as combining quantum random walks to generate random sequences or fusing anti quantum properties such as MRD codes (maximum rank codes) to enhance the security of algorithms in the post quantum era. Continuously optimizing the matrix encryption mechanism has profound significance for ensuring the confidentiality of data circulation in the intelligent era and promoting AI technology to achieve secure and efficient green computing under the "dual carbon" goal.

Acknowledgments

The authors acknowledge the support from the Fund of the

Teaching Reform Research Project of General Undergraduate Universities in Hunan Province (Exploration of Case-based Teaching in Mathematics Major Courses for the Purpose of Strengthening Application, No. 202502001824).

The authors gratefully acknowledge the support from the College Students' Innovation and Entrepreneurship Training Program (Dual Drive of Learning and Research: Innovative Projects in Mathematics Transition and Application S202413806009).

References

- [1] Zhang Mengran. AI creates efficient and accurate mathematical algorithms for the first time. Computer and Network, 2022.
- [2] Ilya Solovychik, Ilya Liubomirsky. Matrix multiplication calculation device and AI accelerator device for AI accelerator integrated circuits: CN202322826485.7 [P]. CN221960554U [2025-12-04]. 2025.
- [3] Diao Wenqi. Research and Implementation of Matrix Computing Architecture Based on Delay Constrained Asynchronous Circuit. Lanzhou University, 2021.
- [4] Shen Jian. Developing specialized directional sports skills through matrix games. Chinese School Physical Education, 2024, 43(05): 35-36.
- [5] Kang jian. GTX860M Extreme Matrix Gaming Machine Review. Computer and Network, 2014, 000 (017): 24-26.
- [6] Li Chen. Dong Shijie. 5G empowers password to promote the safe and high-quality development of traditional manufacturing industry. China Cement, 2023.
- [7] Song Chen. Master's thesis on privacy protection in deep learning model inference based on cryptography. Guangxi University, 2024.
- [8] Wang Weijin, Yuan Jixue A database password encoding algorithm based on Hill cipher idea. Computer and Modernization, 2005.