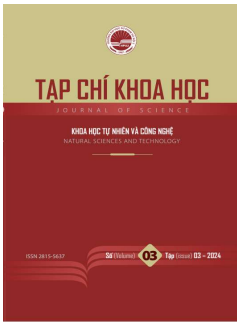
HPU2 Journal of Sciences:
Natural Sciences and Technology

Journal homepage: https://sj.hpu2.edu.vn



Article type: Research article

Hybrid affine cipher and eigenvector methods for cryptography

Anh-Thang Le[a], Thanh-Huyen Pham Thi[a], Van-Dong Vu[a*], Mai-Thanh Hoang Thi[b], Bich-Ngoc Nguyen Thi[c]

[a]*Hanoi University of Industry, Hanoi, Vietnam*
[b]*Tuyet Nghia Secondary School, Hanoi, Vietnam*
[c]*Ngoc My Secondary School, Hanoi, Vietnam*

Abstract

This paper systematically presents a specific application of linear algebra in information security and cryptography, highlighting the crucial role of matrix operations and linear techniques in the design and analysis of encryption algorithms. Specifically, we focus on a method that utilizes linear algebra to enhance the security and efficiency of modern cryptographic systems. A detailed illustrative example is provided to help readers better understand how these mathematical tools are applied in practice. Furthermore, we review existing encryption techniques and propose a new matrix-based scheme that leverages linear algebra to improve data security, optimize the encryption-decryption process, and ensure the integrity and confidentiality of information throughout transmission and storage.

Keywords: Information security, encryption, encryption methods, linear algebra applications, affine-eigenvalue encryption

1. Introduction

Linear algebra plays a crucial role in many areas of life, particularly in economics and engineering. In economics, optimization models, data analysis, and forecasting rely on linear algebra methods to efficiently process and analyze large volumes of data (see e.g. [1]–[3]). In the field of engineering, linear algebra serves as the foundation for applications such as signal processing, solving differential equations, and automatic control systems (see e.g. [4]–[6]). Additionally, in computer science, linear algebra supports the development of algorithms and data encryption, thereby ensuring information security within network systems (see e.g. [7]). With its diverse and extensive applications,

* Corresponding author, E-mail: dongvv@haui.edu.vn

https://doi.org/10.56764/hpu2.jos.2024.3.3.80-87

Received date: 30-9-2024 ; Revised date: 06-11-2024 ; Accepted date: 14-11-2024

This is licensed under the CC BY-NC 4.0

linear algebra is not only a powerful tool for scientists but also a bridge between mathematics and practice.

In the field of information encryption, linear algebra plays a key role in designing security algorithms, such as Rivest-Shamir-Adleman (RSA) public key encryption, matrix-based cryptosystems, and the Advanced Encryption Standard (AES) (see e.g. [8]). Linear transformations and matrix algebra facilitate the construction of robust encryption systems; thereby protecting information from unauthorized access and ensuring data integrity during transmission (see e.g. [9]). Specifically, techniques such as eigenvalue decomposition and singular value decomposition are employed to tackle complex encryption problems, optimizing the process of encrypting and decrypting information (see e.g. [10]). These applications highlight the significance of linear algebra in creating secure and efficient encryption systems that meet the growing demands for information security in the digital age. This paper aims to present some applications of linear algebra in the field of information security and cryptography, thereby clarifying the important role of matrix operations and linear techniques in the construction and analysis of encryption algorithms. Specifically, the paper will focus on methods that utilize linear algebra to enhance the safety and efficiency of modern encryption systems, while also providing illustrative examples and real-world case studies to help readers gain a better understanding of how these mathematical tools are applied in practice.

The remainder of the paper is organized as follows: The next section presents some linear algebra knowledge used to develop efficient encryption algorithms, aiding in the optimization of information security processes. The third section will provide a brief overview of several well-known encryption techniques in practice. In the fourth section, we propose a matrix-based encryption program that applies linear algebra techniques to improve the security and efficiency of the system. Finally, the last section will provide some conclusions and future research prospects.

2. Some fundamentals of linear algebra

This section presents some fundamental concepts of linear algebra, derived from sources such as [11], [12], and [13], that are useful in the development and analysis of encryption algorithms.

Definition 2.1 (Matrix). An $m \times n$ matrix is a rectangular array of real numbers, arranged in m rows and n columns. The elements of a matrix are called the entries. The expression $m \times n$ denotes the size of the matrix.

A general $m \times n$ matrix A has the form

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix},$$

where each *matrix element* $a_{ij} \in \mathbb{R}$. If $m = n$ the matrix is said to be square.

Definition 2.2 (Matrix addition and scalar multiplication). If A and B are two $m \times n$ matrices, then the sum of the matrices $A + B$ is the $m \times n$ matrix with the ij term given by $a_{ij} + b_{ij}$. The scalar product of the matrix A with the real number c, denoted by cA, is the $m \times n$ matrix with the ij term given by ca_{ij}.

Definition 2.3 (Matrix multiplication). Let A be an $m\times n$ matrix and B be an $n\times p$ matrix; then the product AB is an $m\times p$ matrix. The ij term of AB is the dot product of the i th row vector of A with the j th column vector of B, so that

$$(AB)_{ij}=\sum_{k=1}^{p}a_{ik}b_{kj}=a_{i1}b_{1j}+a_{i2}b_{2j}+\cdots+a_{ip}b_{pj}. \tag{1}$$

Definition 2.4 (Minors and cofactors of a matrix). If A is a square matrix, then the minor M_{ij}, associated with the entry a_{ij}, is the determinant of the $(n-1)\times(n-1)$ matrix obtained by deleting row i and column j from the matrix A. The cofactor of a_{ij} is $C_{ij}=(-1)^{i+j}M_{ij}$.

Definition 2.5 (Determinant of a square matrix). Let A be an $n\times n$ matrix, The determinant of the matrix A, denoted as $\det(A)$, is defined by

$$\det(A)=a_{11}C_{11}+a_{12}C_{12}+\cdots+a_{1n}C_{1n}=\sum_{k=1}^{n}a_{1k}C_{1k} \tag{2}$$

Definition 2.6 (Inverse of a square matrix). Let A be an $n\times n$ matrix. If there exists an $n\times n$ matrix B such that $AB=I=BA$ then the matrix B is a (multiplicative) inverse of the matrix A, and it is denoted by A^{-1}.

Theorem 2.1. Let A be an invertible $n\times n$ matrix. Then

$$A^{-1}=\frac{1}{\det(A)}\operatorname{adj}A=\frac{1}{\det(A)}\begin{bmatrix}c_{11}&c_{21}&\cdots&c_{n1}\\c_{12}&c_{22}&\cdots&c_{n2}\\\cdots&\cdots&\cdots&\cdots\\c_{1n}&c_{2n}&\cdots&c_{nn}\end{bmatrix}. \tag{3}$$

where $c_{ij}=(-1)^{i+j}\det(M_{ij})$.

Definition 2.7 (Eigenvalue and eigenvector). Let A be an $n\times n$ matrix. A number λ is called an eigenvalue of A provided that there exists a nonzero vector v in $\mathbb{R}^n$ such that

$$Av=\lambda v.$$

Every nonzero vector satisfying this equation is called an eigenvector of A corresponding to the eigenvalue λ.

Definition 2.8 (Null space of mattrix). The null space of a matrix A, denoted as $\operatorname{Null}(A)$, is the set of all vectors x such that:

$$Ax=0.$$

Let's summarize the procedure to find the eigenvalues and eigenvectors (eigenspaces) of a matrix A, where A is an $n\times n$ matrix.

- Compute the characteristic polynomial $\det(A-\lambda I)$ of A.
- Find the eigenvalues of A by solving the characteristic equation $\det(A-\lambda I)=0$ for λ.
- For each eigenvalue λ, find the null space of the matrix $A-\lambda I$. This is the eigenspace E_λ, the nonzero vectors of which are the eigenvectors of A corresponding to λ.
- Find a basis for each eigenspace.

3. Some encryption techniques

To encrypt or decrypt a message, we need to assign a number to each letter in the alphabet. The easiest way to do this is to associate 0 with a blank or space, 1 with A, 2 with B, and so on.

0 = , 1 = A, 2 = B, 3 = C, 4 = D, 5 = E, 6 = F, 7 = G, 8 = H, 9 = I,

10 = J, 11 = K, 12 = L, 13 = M, 14 = N, 15 = O, 16 = P, 17 = Q, 18 = R,

19 = S, 20 = T, 21 = U, 22 = V, 23 = W, 24 = X, 25 = Y, 26 = Z.

Another way is to associate 0 to a blank or space, 1 to A, -1 to B, 2 to C, -2 to D, and so on.

3.1. Hill cipher

Hill cipher is a matrix encryption method invented by Lester S. Hill in 1929 (see [14]). It is one of the first block cipher systems to use linear algebra. Since then, many authors have utilized this technique, for example, in [15] and [16].

Idea: The original information (in vector form) can be encrypted by multiplying it with a key matrix. Specifically, a message can be represented as a vector, and encryption is achieved by multiplying this vector with an invertible key matrix.

Encryption process:

- Use a square matrix K of size $n \times n$ as the encryption key.
- The original text string is divided into character blocks of length n. Each block is represented as a column vector.
- Encrypt each block by multiplying the key matrix with the character vector: $C = MK$, where M is the original text vector and C is the encrypted vector.

Decryption process:

- Calculate the inverse matrix K^{-1} of the key matrix.
- Decrypt each block by multiplying the inverse matrix with the encrypted vector: $M = CK^{-1}$.

Note: The matrix K must have a non-zero determinant and an inverse matrix K^{-1} must exist.

3.2. Affine cipher

Idea: Use an affine encryption method based on linear algebra, where a message is transformed by a linear function and a constant (matrix) is added (see, for example [17]–[19]).

Encryption process:

- Use two matrices A and B, with A being a non-degenerate square matrix (having a non-zero determinant).
- Encrypt each character using the linear transformation: $C = MA + B$.

Decryption process:

- Calculate the inverse matrix A^{-1}.
- Decrypt by applying the inverse transformation: $M = (C - B)A^{-1}$.

Note: A must have an inverse.

3.3. Based quadratic form encryption

This technique uses the encoding matrix as the diagonalized matrix of a given quadratic form (see [20]. For example, if the quadratic form is given by $Q(x_1, x_2, x_3) = 6x_1^2 + 5x_2^2 + 7x_3^2 - 4x_1x_2 + 4x_1x_3$

then the matrix of this quadratic form

$$\begin{bmatrix} 6 & -2 & 2 \\ -2 & 5 & 0 \\ 2 & 0 & 7 \end{bmatrix}.$$

Also the canonical form is $3y_1^2 + 6y_2^2 + 9y_3^2$ whose matrix is given by

$$E = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 9 \end{bmatrix}.$$

We have the encoder as E. Then the message matrix is converted into a new matrix X (encoded matrix) using matrix multiplication as $X = ME$, where M is a message matrix. Then this is sent to the receiver. Then the receiver decode this matrix with the help of a matrix D (decoder matrix) which is nothing but the inverse of the encoder (i.e., $D = E^{-1}$), to get the message matrix back as $M = XE^{-1}$.

The encryption methods presented in this section offer several notable advantages. The Hill cipher processes data in blocks, providing better security compared to single-character encryption methods, while also being easy to implement with basic matrix operations. The affine cipher can be extended to various applications due to its linear nature. The method based on quadratic forms enhances security and offers flexibility in specific applications.

4. Affine cipher and eigenvectors-based encryption

The methods presented in the previous section also have drawbacks: Hill cipher and affine cipher are vulnerable to attacks if the original and encrypted pairs are exposed, and they are not strong enough for modern applications. The method based on quadratic forms is more complex, requiring extensive computation and careful key selection to avoid exploitation. Building on the eigenvectors of the matrix and the affine cipher technique, we propose the following encryption and decryption method:

Encryption process:

- Let A and B be two matrices.
- Find the eigenvalues and the corresponding eigenvectors of the matrix A. Construct the matrix P whose columns are the eigenvectors of A.
- Encrypt the message M using the formula $C = P^{-1}MP + B$.

Decryption process

Decrypt by applying the inverse transformation: $M = P(C - B)P^{-1}$.

Note that the matrix A is chosen such that the matrix P is invertible, and B is any matrix that satisfies the additive condition with matrix A.

Example

Consider the message to be sent: GOOD LUCK.

We take the standard codes as follows: 0 → Space, 1 → A, 2 → B, ... 26 → Z;

- We convert the above message into a stream of numerical values as follows

G	O	O	D		L	U	C	K
7	15	15	4	0	12	21	3	11

- We construct the message matrix M with this stream of numerals as

$$M = \begin{bmatrix} 7 & 15 & 15 \\ 4 & 0 & 12 \\ 21 & 3 & 11 \end{bmatrix}$$

- We take the

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 6 & -2 & 0 \\ 7 & -4 & 2 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & 2 & 5 \\ 3 & 2 & -1 \\ 3 & 5 & 3 \end{bmatrix}$$

To find the eigenvalues of A, we solve the characteristic equation

$$\det(A - \lambda I) = (1-\lambda)(-2-\lambda)(2-\lambda) = 0.$$

Thus, the eigenvalues of A are $\lambda_1 = 1$, $\lambda_2 = -2$, $\lambda_3 = 2$.

The corresponding eigenvectors, which are linearly independent, are given, respectively, by

$$v_1 = \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}, \qquad v_2 = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \qquad v_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

- Then we have the Encoder as:

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}, \quad P^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 1 & -1 & 1 \end{bmatrix}$$

- Then the encoded matrix is given by

$$C = P^{-1}MP + B = \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 1 & -1 & 1 \end{bmatrix}\begin{bmatrix} 7 & 15 & 15 \\ 4 & 0 & 12 \\ 21 & 3 & 11 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 2 & 5 \\ 3 & 2 & -1 \\ 3 & 5 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 53 & 32 & 20 \\ -85 & -46 & -19 \\ 77 & 37 & 17 \end{bmatrix}$$

Hence the encoded numeric message is given by

53 32 20 -85 -46 -19 77 17

- The encoded numeric message is to be decoded by

$$M = P(C-B)P^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}\left(\begin{bmatrix} 53 & 32 & 20 \\ -85 & -46 & -19 \\ 77 & 37 & 17 \end{bmatrix} - \begin{bmatrix} 1 & 2 & 5 \\ 3 & 2 & -1 \\ 3 & 5 & 3 \end{bmatrix}\right)\begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 1 & -1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 7 & 15 & 15 \\ 4 & 0 & 12 \\ 21 & 3 & 11 \end{bmatrix}$$

This stream of numerals is converted in to the text message as

7	15	15	4	0	12	21	3	11
G	O	O	D		L	U	C	K

Remark. Since for each eigenvalue there are infinitely many corresponding eigenvectors, there are multiple matrices P that can be chosen for each matrix A. Therefore, we believe that this technique is more secure than the techniques mentioned in Section 3.

The proposed method combines affine cipher and eigenvector-based encryption, demonstrating how matrix operations significantly enhance data security and optimize the encryption-decryption process. This method stands out for its flexibility, as the infinite choice of eigenvectors for a given eigenvalue allows for the use of multiple encryption matrices, making this technique more secure than traditional methods. The proposed method has a computational complexity related to calculating the eigenvalues and eigenvectors of the matrix. However, if the matrix has a special structure (e.g., symmetric), the complexity can be significantly reduced. Compared to traditional encryption methods like the Hill cipher, this method is more computationally efficient in certain practical cases.

5. Conclusion

In conclusion, this paper highlights the vital role of linear algebra in information security and cryptography. We have demonstrated how matrix operations and linear techniques enhance the design of encryption algorithms. Our proposed matrix-based scheme improves data security and optimizes the encryption-decryption process, ensuring the integrity and confidentiality of information during transmission and storage. The illustrative example provided aids in understanding the practical application of these concepts. We believe that further exploration of linear algebra in cryptography will yield more robust security solutions in the evolving information technology landscape.

References

[1] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge, UK: Cambridge Univ. Press, 2004, doi: 10.1017/cbO9780511804441.

[2] F. Aleskerov, H. Ersel, and D. Piontkovski, *Linear algebra for economists* (Springer texts in business and economics), Heidelberg, Germany: Springer, 2011, doi: 10.1007/978-3-642-20570-5.

[3] D. C. Lay, S. R. Lay, and J. J. McDonald, *Linear algebra and its applications*, 5th ed. Boston, MA, USA: Pearson, 2016.

[4] G. Strang, *Linear algebra and its applications*, 4th ed. Boston, MA, USA: Cengage Learning, 2006.

[5] F. Neri, *Linear algebra for computational sciences and engineering*. Cham, Switzerland: Springer, 2019, doi: 10.1007/978-3-030-21321-3.

[6] H. Anton, C. Rorres, and A. Kaul, *Elementary linear algebra: Applications version*, 12th ed. New York, USA: Wiley, 2019.

[7] J. S. Chahal, *Fundamentals of linear algebra,* 1st ed. Boca Raton, FL, USA: CRC Press, 2018, doi:10.1201/9780429425479.

[8] N. Koblitz, *A course in number theory and cryptography* (Graduate texts in mathematics), New York, USA: Springer, 1994, doi: 10.1007/978-1-4419-8592-7.

[9] D. R. Stinson, *Cryptography: Theory and practice*, 3rd ed. Chapman, MA, USA: CRC Press, 2006, doi: 10.1201/9781420057133.

[10] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*, 1st ed. Boca Raton, FL, USA: CRC Press, 1997, doi: 10.1201/9780429466335.

[11] S. Andrilli and D. Hecker, *Elementary linear algebra*, 4th ed. Amsterdam, Netherlands: Academic Press, 2010.

[12] J. DeFranza and D. Gagliardi, *Introduction to linear algebra with applications*, 1st ed, Illinois, USA: Aveland Press, Inc, 2015.

[13] D. Poole, *Linear algebra: A modern introduction*, 3rd ed. Boston, MA, USA: Brooks Cole, 2010.

[14] L. S. Hill, "Cryptography in an algebraic alphabet," *Am. Math. Mon.,* vol. 36, no. 6, pp. 306–312, Jun. 1929, doi: 10.1080/00029890.1929.11986963.

[15] B. Schneier, *Applied cryptography: Protocols, algorithms, and source code in C*, 2nd ed. New York, USA: John Wiley & Sons Inc, 1996.

[16] N. T. Thanh-Giang, "Applications of linear algebra in encryption," *HPU2. Nat. Sci. Tech*., vol. 2, no. 1, pp. 46–52, Apr. 2023, doi: 10.56764/hpu2.jos.2023.1.2.46-52.

[17] S. Singh, *The code book: The science of secrecy from ancient Egypt to quantum cryptography*, 1st ed. London, UK: Fourth Estate, 1999.

[18] D. R. Stinson, *Cryptography: Theory and practice* (Discrete mathematics and its applications), 3rd ed. New York, USA: Chapman and Hall/CRC, 2005, doi: 10.1201/9781420057133.

[19] M. Kazemi, H. Naraghi, and H. M. Golshan "On the affine ciphers in Cryptography," In *Informatics engineering and information science*. *ICIEIS 2011. Communications in computer and information science*, 2011, pp. 185-199, doi: 10.1007/978-3-642-25327-0_17.

[20] B. Vellaikannan, Dr. V. Mohan, and V. Gnanaraj, "A note on the application of quadratic forms in coding theory with a note on security," *Int. J. Comp. Tech*. *Appl*., vol 1, no 1, pp. 78–87, Jun. 2010.