Int. j. adv. multidisc. res. stud. 2024; 4(2):1040-1043

Received: 22-02-2024
Accepted: 02-04-2024

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Application of Matrix in Information Encryption

Nguyen Thi Xuan Mai
Thai Nguyen University of Technology - Thai Nguyen University, Vietnam

Corresponding Author: **Nguyen Thi Xuan Mai**

Abstract
Entering the age of digital technology, traditional industries such as telecommunications and cultural education are undergoing dramatic changes. Other industries such as information technology (IT) and related services are growing at a rapid pace. In particular, the Internet has revolutionized communication because it eliminates the limitations of distance, time, and volume. Information encryption is constantly mentioned by many people. However, when there was no technology, our ancestors also knew how to use many different methods to encode information. One of those methods is to use matrices. This article will present the application of matrices in encrypting communication information.

Keywords: Matrix, Uncoded Row Matrix, Encoding Matrix, Encryption, Cryptography, Decryption, Security...

1. Introduction

In cryptography - a branch of mathematics applied to information technology, encryption is a method to transform information (in the form of movies, text, images...) from a normal format to another format that cannot be understood without a means of decoding, the purpose is to ensure that only the two communicating parties can understand that information, helping to protect the information from being exposed to the outside, avoiding being known by many people. The encryption process needs to ensure the confidentiality, integrity and authenticity of information.

Decryption is the process of returning encrypted information to its original form, which is the reverse process of encryption. The encryption process turns the original data A into data B, then the encrypted data B is sent to the recipient, and the recipient have to decode the data B back into the data A to get the information.

An encryption system includes the following components:

1. Information before encryption, denoted P *(Plaintext).*
2. Information after encryption, denoted C *(Ciphertext).*
3. Key, denoted K *(Key).*
4. Encryption/decryption method, denoted E/D *(Encryption/Decryption).*

In this paper, the encryption of text information using the matrix method is introduced. The information before encryption is a letter, the information after encryption is a sequence of numbers. The key for performing encryption or decryption is an invertible square matrix.

2. Application of matrix in information encryption

First, we recall some basic knowledge about matrices.

Matrix with size (order) of $m \times n$, is a table of numbers arranged in m rows and n columns. A matrix can be denoted by an uppercase letter such as $A, B, C...$ A matrix can be denoted by a representative element enclosed in brackets, such as $\left[a_{ij}\right], \left[b_{ij}\right], \left[c_{ij}\right]...$ A matrix can be denoted by a rectangular array of numbers

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

Each number a_{ij} is called an element in the i row, the j column of the matrix A.
If $A=\left[a_{ij}\right]$ is an $m\times n$ matrix and $B=\left[b_{ij}\right]$ is an $n\times p$ matrix, then the product matrix AB is an $m\times p$ matrix, $AB=\left(c_{ij}\right)$, Where

$$c_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj}=a_{i1}b_{1j}+a_{i2}b_{2j}+...+a_{in}b_{nj}$$

This definition means the entry in the i row and the j column of the product matrix AB is obtained by multiplying the entries in the i row of A by the corresponding entries in the j column of B and then adding the result.
To perform the encryption, we first assign a number to each letter in the alphabet. As follows

0 = _	10 = J	20 = T
1 = A	11 = K	21 = U
2 = B	12 = L	22 = V
3 = C	13 = M	23 = W
4 = D	14 = N	24 = X
5 = E	15 = O	25 = Y
6 = F	16 = P	26 = Z
7 = G	17 = Q	
8 = H	18 = R	
9 = I	19 = S	

Accordingly, the content of the letter will be converted from text to number and divided into uncoded row matrices, each having n entries (The value of n depends on the sender's intention).

Example 1:
Write the uncoded row matrices of size 1×3 for the message: MEET ME TONIGHT.
Because it is necessary to be converted row matrices with size of 1×3, so the message is divided into groups, each group has three characters (including blank spaces, but ignoring punctuation). According to the convention of converting from letters to numbers mentioned above, we get the following corresponding row matrices

$$\begin{array}{cccccccccccccc}
[13 & 5 & 5] & [20 & 0 & 13] & [5 & 0 & 20] & [15 & 14 & 9] & [7 & 8 & 20] \\
M & E & E & T & _ & M & E & _ & T & O & N & I & G & H & T
\end{array}$$

Thus, in the encryption system mentioned above, the message: MEET ME TONIGHT is the information before encryption P (plaintext), and the corresponding row matrices

$$[13\ \ 5\ \ 5]\ [20\ \ 0\ \ 13]\ [5\ \ 0\ \ 20]\ [15\ \ 14\ \ 9]\ [7\ \ 8\ \ 20]$$

are information matrices that need to be encoded.
To encrypt the message content, an invertible matrix with size of $n\times n$ is chosen. The matrix is multiplied by a row matrix corresponding to the message content to obtain the encryption matrix. This process will be clearly shown in example 2.

Example 2:
Use the matrix $A=\begin{bmatrix}1 & 3 & -2\\ -1 & -2 & 5\\ 1 & 4 & 2\end{bmatrix}$ to encode the message: MEET ME TONIGHT.
From example 1, we have the row matrices with size of 1×3 for the message is

$$[13\ \ 5\ \ 5]\ [20\ \ 0\ \ 13]\ [5\ \ 0\ \ 20]\ [15\ \ 14\ \ 9]\ [7\ \ 8\ \ 20]$$

The coded row matrices is obtained by multiplying each the uncoded row matrices by the matrix A. As follows:

Uncoded row matrix	Encoding matrix A	Coded row matrix
$[13\ \ 5\ \ 5]$	$\begin{bmatrix}1 & 3 & -2\\ -1 & -2 & 5\\ 1 & 4 & 2\end{bmatrix}_{=}$	$[13\ \ 49\ \ 9]$

$[20 \quad 0 \quad 13]$	$\begin{bmatrix} 1 & 3 & -2 \\ -1 & -2 & 5 \\ 1 & 4 & 2 \end{bmatrix}_{=}$	$[33 \quad 112 \quad -14]$
$[5 \quad 0 \quad 20]$	$\begin{bmatrix} 1 & 3 & -2 \\ -1 & -2 & 5 \\ 1 & 4 & 2 \end{bmatrix}_{=}$	$[25 \quad 95 \quad 30]$
$[15 \quad 14 \quad 9]$	$\begin{bmatrix} 1 & 3 & -2 \\ -1 & -2 & 5 \\ 1 & 4 & 2 \end{bmatrix}_{=}$	$[10 \quad 53 \quad 58]$
$[7 \quad 8 \quad 20]$	$\begin{bmatrix} 1 & 3 & -2 \\ -1 & -2 & 5 \\ 1 & 4 & 2 \end{bmatrix}_{=}$	$[19 \quad 85 \quad 66]$

The sequence of coded row matrices is

$[13 \quad 49 \quad 9] \; [33 \quad 112 \quad -14] \; [25 \quad 95 \quad 30] \; [10 \quad 53 \quad 58] \; [19 \quad 85 \quad 66]$

Finally, removing the brackets produces the cryptogram below

$13 \quad 49 \quad 9 \quad 33 \quad 112 \quad -14 \quad 25 \quad 95 \quad 30 \quad 10 \quad 53 \quad 58 \quad 19 \quad 85 \quad 66$

So, if someone does not know the matrix A, it is very difficult to understand the content of this cryptogram. Therefore, to perform decoding, the recipient of the information must know the encoding matrix A.

To perform decryption, the receiver multiplies the coded row matrices with the matrix A^{-1} to obtain the uncoded row matrices. The mathematical theoretical basis is as follows: If the matrix $X = [x_1 \quad x_2 \quad \dots \quad x_n]$ is an uncoded row matrix, then $Y = X.A$ is the corresponding encoded matrix and $Y.A^{-1} = XA.A^{-1} = X.I = X$, where I is the n-level unit matrix.
Accordingly, decoding will be done by finding the inverse matrix and performing the multiplication of the two matrices. To illustrate, let's consider the following example.

Example 3:

Use the inverse of the matrix $A = \begin{bmatrix} 1 & 3 & -2 \\ -1 & -2 & 5 \\ 1 & 4 & 2 \end{bmatrix}$ to decode the cryptogram:

$13 \quad 49 \quad 9 \quad 33 \quad 112 \quad -14 \quad 25 \quad 95 \quad 30 \quad 10 \quad 53 \quad 58 \quad 19 \quad 85 \quad 66$

Because matrix A is square and $\det(A) = 1 \neq 0$ so A is an invertible matrix. Then, use the Gauss - Jordan elimination method to find the inverse matrix A^{-1}.

$$[A|I] = \left[\begin{array}{ccc|ccc} 1 & 3 & -2 & 1 & 0 & 0 \\ -1 & -2 & 5 & 0 & 1 & 0 \\ 1 & 4 & 2 & 0 & 0 & 1 \end{array}\right] \xrightarrow[H_3 = H_3 - H_1]{H_2 = H_2 + H_1} \left[\begin{array}{ccc|ccc} 1 & 3 & -2 & 1 & 0 & 0 \\ 0 & 1 & 3 & 1 & 1 & 0 \\ 0 & 1 & 4 & -1 & 0 & 1 \end{array}\right] \xrightarrow{H_3 = H_3 - H_2} \left[\begin{array}{ccc|ccc} 1 & 3 & -2 & 1 & 0 & 0 \\ 0 & 1 & 3 & 1 & 1 & 0 \\ 0 & 0 & 1 & -2 & -1 & 1 \end{array}\right]$$

$$\xrightarrow[H_2 = H_2 - 3H_3]{H_1 = H_1 + 2H_3} \left[\begin{array}{ccc|ccc} 1 & 3 & 0 & -3 & -2 & 2 \\ 0 & 1 & 0 & 7 & 4 & -3 \\ 0 & 0 & 1 & -2 & -1 & 1 \end{array}\right] \xrightarrow{H_1 = H_1 - 3H_2} \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -24 & -14 & 11 \\ 0 & 1 & 0 & 7 & 4 & -3 \\ 0 & 0 & 1 & -2 & -1 & 1 \end{array}\right].$$

So $A^{-1} = \begin{bmatrix} -24 & -14 & 11 \\ 7 & 4 & -3 \\ -2 & -1 & 1 \end{bmatrix}$.

Now, to decode the above cryptogram, because the matrix A is 3×3 in size, we divide that cryptogram into groups, each group consists of three numbers and write it as the coded row matrices.

$$[13 \quad 49 \quad 9] \; [33 \quad 112 \quad -14] \; [25 \quad 95 \quad 30] \; [10 \quad 53 \quad 58] \; [19 \quad 85 \quad 66]$$

To obtain the decoded row matrices, multiply each coded row matrix by A^{-1}

Coded row matrix	Decoding matrix A^{-1}	Decoded row matrix
$[13 \quad 49 \quad 9]$	$\begin{bmatrix} -24 & -14 & 11 \\ 7 & 4 & -3 \\ -2 & -1 & 1 \end{bmatrix}=$	$[13 \quad 5 \quad 5]$
$[33 \quad 112 \quad -14]$	$\begin{bmatrix} -24 & -14 & 11 \\ 7 & 4 & -3 \\ -2 & -1 & 1 \end{bmatrix}=$	$[20 \quad 0 \quad 13]$
$[25 \quad 95 \quad 30]$	$\begin{bmatrix} -24 & -14 & 11 \\ 7 & 4 & -3 \\ -2 & -1 & 1 \end{bmatrix}=$	$[5 \quad 0 \quad 20]$
$[10 \quad 53 \quad 58]$	$\begin{bmatrix} -24 & -14 & 11 \\ 7 & 4 & -3 \\ -2 & -1 & 1 \end{bmatrix}=$	$[15 \quad 14 \quad 9]$
$[19 \quad 85 \quad 66]$	$\begin{bmatrix} -24 & -14 & 11 \\ 7 & 4 & -3 \\ -2 & -1 & 1 \end{bmatrix}=$	$[7 \quad 8 \quad 20]$

So, the sequence of decoded row matrices is

$$[13 \quad 5 \quad 5] \; [20 \quad 0 \quad 13] \; [5 \quad 0 \quad 20] \; [15 \quad 14 \quad 9] \; [7 \quad 8 \quad 20]$$

And the message is

13	5	5	20	0	13	5	0	20	15	14	9	7	8	20
M	E	E	T	_	M	E	_	T	O	N	I	G	H	T

3. Conclusion

Through an invertible matrix and using matrix multiplication, information can be encoded and decoded during transferring between two parties to avoid the information being disclosed to third parties. The advantages of the encryption are simple and easy to understand, but it is still rudimentary and not very secure.

Today, with the development of science and technology, especially the rapid development of the information technology, humanity has invented many more modern, sophisticated and higher security ways of encoding and decoding.

Therefore, the method of using matrices to encode information has become classic. Up to now, it is only for orientation, introducing learners to the applications of matrices and how the ancients kept information secure. It also let learners see that mathematics is really interesting and meaningful in life.

4. Acknowledgement

The authors thank the Thai Nguyen University of Technology for supporting this work.

5. References

1. Nguyễn Đình Trí, Tạ Văn Đĩnh, Nguyễn Hồ Quỳnh - Toán học cao cấp (tập một) - NXB Giáo dục, 2006.
2. Nguyễn Đình Trí, Tạ Văn Đĩnh, Nguyễn Hồ Quỳnh - Bài tập Toán học cao cấp (tập một) - NXB Giáo dục, 2006.
3. Ron Larson, David C. Falvo. Elementary Linear Algebra, 2009.