[[1]](#footnote-1)

Encryption and Decryption Message Using Determinant and Inverse of Key Matrix

2017113356 Kim min sung, 2017116965 Jun Geon Min, KNU CSE

*Abstract* – We studied how to use the matrix for key values when encrypting and re-encrypting messages. First of all, we set two key matrices A and B and obtained a determinant of matrix A and an inverse of matrix B. Then, using the property of the matrix we conduct by encrypting the massages entered and showing the results of encryption and decryption. Also, by this method, we searched for ways for machine learning.

*Index Terms*—Decryption, Determinant, Encryption, Inverse of matrix, Machine running, Matrix, Send and Receive Messages

# INTRODUCTION

F

rom ancient times, people have whispered, sent and received words that are hard to say or should not be leaked out to others through secret letters or personal texts. Through this way, people have not only engaged in secret conversations, but also in national affairs, such as espionage and intelligence warfare. As machine learning has recently attracted attention, we want to apply a secret communication method to computer for sending and receiving messages. Most computers use encryption to send and receive data. So, we implemented sending and receiving messages using symmetric key algorithms and the properties of matrices learned in linear algebra class.

# Related Works

We searched for related works to get idea of algorithms of encryption and decryption and way to use matrix properties to machine learning.

## Enhancement outsourcing security

There were Matrix Determinant Computation (MDC), Matrix Multiplication Computation (MMC), Matrix Inverse Computation (MIC) method for enhancement outsourcing security. In this study, the authors conducted outsourcing algorithms based on matrix operations of MDC, MMC, MIC. Each method had the potential to be a negligible function in high accuracy and security. This preceding study will demonstrate that the accuracy and security of message encryption algorithms using matrix operations can be ensured in a similar way.

## Convolution Neural Network

We also referred to examples of research on algorithms that encrypt images based on Dynamic Chaos Theory and Matrix Convolution which are using Convolution Neural Network in recent machine learning field. In fact, the mathematical approach to introducing matrices into encryption algorithm was taken rather than using of matrix convolution. Through this approach, we will enable the algorithm to be made mathematical based on matrix operation and implemented in programming language. (in C)

# MATH

The properties of matrix and matrix operations used in the study are very simple but basic and important in the linear algebra.

## Inverse of matrix

An n-by-n square matrix A is called invertible (also nonsingular or nondegenerate), if there exist an n-by-n square matrix such that

where denotes the n-by-n identity matrix and the multiplication used is ordinary matrix multiplication. Here the following expression can be obtained for any matrix P

If we call matrix P a message and matrix A is a key matrix, we can easily implement the encryption-decryption process by simply multiplying the original and inverse matrix.

## Treating the determinant as constant

A determinant of matrix is a function of matching scalar to a square matrix. So, the determinant of matrix can be treated like a scalar, i.e. constants.

Let 3x3 matrix be a massage. And the determinant of key matrix B become . We applied the encryption/decryption process by subtracting and adding to each component of matrix P. The following equation is that.

## Coordinate transformation and parallel movement of matrix

From the perspective of the coordinate system, the process of multiplying a matrix by a particular matrix and multiplying its inverse and subtracting and adding a certain constant value can be geometrically interpreted as coordinate transformation and parallel movement, respectively. If these are performed in combination, it is also possible to move the matrix freely and then return it to its original position. We used these points to encrypt and decrypt the message.

# Algorithm & Result

## Algorithm

We organized the algorithm by dividing the series of processes from matrixing input messages to encoding and decoding them in reverse and matrix ways into a total of six stages.

Phase 1. Matrixing initial input message

First, we input a message until ending of point ‘.’. The message may be at most 100 characters.

We make the massage to form of 10-by-10 matrix. One character’s ASCII value become one component of the matrix. The point ‘.’ set as 0.0. Non-character component set as -2.0. We call this message matrix P for next phase.

Phase 2. Subtracting determinant of key matrix B from each message matrix components

As subtracting determinant, the matrix P from phase 1 becomes another matrix, but has the information of previous one. This process may be considered as parallel movement.

Phase 3. Multiplying key matrix A to message matrix

The key matrix A must be 10-by-10 square matrix for multiplying to matrix P. This process may be considered as coordinate transformation or linear transformation.

Phase 4. Multiplying matrix to message matrix

Compute the inverse of matrix A and simply multiply the inverse to matrix from phase 3. We can get the matrix of phase 2 back.

Phase 5. Adding determinant of key matrix B to message matrix component

As adding determinant, the matrix become back to matrix of phase 1 which is the initial message matrix.

Phase 6. Decoding initial input message

By converting each component of matrix from phase 5 to character, the decoded message will be the output of our program.

## Implementation

We used fixed key matrix A and B as following

Also, we show the process by animation using ‘sleep’ for each stage. (The detail process will be the demonstration video.)

## Result Analysis

Encryption message and decoding it performed well.

There will be small challenge – The phase 3, 4. The message matrix must be n-by-n matrix which can contain at most n-by-n texts, and as the message become long, the key matrix must be large, too. So, the computer should compute the multiplying matrix process no matter how long the message and the key matrix. – This may require additional studies to overcome the difficulty by machine learning.

# Conclusion

In our study, we used fixed key matrices. But, if we apply a key generation algorithm when apply actual environment, security is enhanced as the number of cases increases.

Also, there will be following potential security risks - When multiplying the inverse and then multiplying the original matrix again, the key matrix used in the inverse process is exposed. And when different matrices have the same determinant used during add and subtract process. So, the follow-up studies are required to prevent these problems.

References

[1] Shengxia Zhang, Chengliang Tian, Hanlin Zhang, Jia Yu, and Fengjun Li, “Practical and Secure Outsourcing Algorithms of Matrix Operations Based on a Novel Matrix Encryption Method” IEEE Trans, Mar. 2019.

[2] Xiancheng Hu, Liansuo Wei, Wei Chen, Qiqi Chen, and Yuan Guo, “Color Image Encryption Algorithm Based on Dynamic Chaos and Matrix Convolution” IEEE Trans, Dec. 2019.

[3] Huaibo Sun, Hong Luo, and Yan sun, “Data Hiding for Ensuring the Quality of the Host Image and the Security of the Message”, IEEE Trans, Feb. 2019.

[4] D.N. Wu, Q. Q. Gan, and X.M. Wang, “Verifiable Public Key Encryption with Keyword Search Based on Homographic Encryption in Multi-User Setting” IEEE Access, 2018.

[5] Wenju Xu, Yu Zhan, Zheng Wang, Baocang Wang, and Yuan Ping, “Attack and Improvement on a Symmetric Fully Homographic Encryption Scheme” IEEE Access, 2019.

1. [↑](#footnote-ref-1)