

# LEARNING WITH ERROR FOR DIGITAL IMAGE ENCRYPTION

Aisyah Nooravieta Setiawan<sup>1</sup>, Indah Emilia Wijayanti<sup>2</sup>, Uha Isnaini<sup>3</sup>

<sup>1,2,3</sup>Departement of Mathematics, Universitas Gadjah Mada, Yogyakarta, Indonesia  
Email: <sup>1</sup>[aisyahnsetiawan@mail.ugm.ac.id](mailto:aisyahnsetiawan@mail.ugm.ac.id), <sup>2</sup>[indwijayanti@ugm.ac.id](mailto:indwijayanti@ugm.ac.id), <sup>3</sup>[isnainiuha@ugm.ac.id](mailto:isnainiuha@ugm.ac.id)  
\*Corresponding Author

**Abstract.** Learning With Error (LWE) is one of the development of a system linear equation that add some noise or error. These problems have good potential for cryptography, especially for the development of Key Exchange Mechanism (KEM). More-over, the question is whether LWE can be applied for digital image security or not. The digital image consists of hundreds of pixels that can be interpreted as a matrix. Each Pixel is encrypted with LWE so that the image becomes unidentified or cipher. **Keywords:** Learning With Error, Cryptography, Digital Image, Encryption, Decryp-tion.

## I. INTRODUCTION

As technology advances in modern era, of course the challenges in securing data will become more difficult. One of the challenges is countering attacks from quantum computers which have superior computing capabilities and specifications compared to ordinary computers. National Institute of Standards and Technology Interagency or Internal Report NIST (2022)[6], sets evaluation standards for cryptographic systems that are resistant to quantum computers (Quantum Secure Cryptography), which are categorized into three aspects, the first is the level of security, the second is cost and performance, and The last is the algorithm and its implemen-tation. Furthermore, it was explained that one approach to constructing a cryptographic system that is resistant to quantum computers is using lattice (lattice-based cryptography).

The study of lattice problem was first initiated by Ajtai. In 1997, Ajtai [1] again introduced his idea of Short Integer Solution (SIS), which is a development of lattice computing problems, namely finding the shortest solution to a system of homogeneous linear equations. Furthermore, in 2005, Regev [9] developed SIS from the aspects of complexity and security by adding errors to the system of linear equations known as Learning With Error (LWE). Moreover, LWE is seen as one of the fundamental theories in building Quantum Secure Cryptography. In 2023, NIST [10] gave the standard of Key Exchange Mechanism (KEM) for encrypting the key to keep it secure, which is a Module-Lattice-based Key-Encapsulation Mechanism (MLKEM). The standard is the development of Module Learning With Error.

It is undeniable that there is a wide variety of data in digital besides numerical data, such as image. These kinds of data certainly require good security as well. This paper discusses whether LWE also can be used for encrypting the image to keep it secure or not.

## II. PRELIMINARIES

This study requires minimal knowledge of cryptography and lattices beyond some basic definitions and computational problems, which are as follows.

**Definition 1 (Cryptosystem [10])** A cryptosystem is a five tuple  $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ , where the following condition are satisfied:

- i)  $\mathcal{P}$  is a finite set of possible plaintext.
- ii)  $\mathcal{C}$  is a finite set of possible ciphertext.
- iii)  $\mathcal{K}$ , the key space, is a finite set of possible key.
- iv) For each  $K \in \mathcal{K}$ , there is an encryption rule  $e_K \in \mathcal{E}$  and corresponding decryption rule  $d_K \in \mathcal{D}$ . Each  $e_K : \mathcal{P} \rightarrow \mathcal{C}$  and  $d_K : \mathcal{C} \rightarrow \mathcal{P}$  are function such that  $d_K(e_K(x)) = x$  for every plaintext element  $x \in \mathcal{P}$ .

After knowing the definition of cryptosystem, the definition of Lattice is given as follows.

**Definition 2 (Lattice [8])** An  $n$ -dimensional lattice  $\mathcal{L}$  is any subset of  $\mathbb{R}^n$  that is both:

1. an additive subgroup; and
2. discrete: every  $x \in \mathcal{L}$  has a neighborhood in  $\mathbb{R}^n$  in which  $x$  is the only lattice point.

Then, the computational problems on lattices that have been most useful in the study of LWE is given as follows.

**Definition 3 (Closest Vector Problem [5])** Given a lattice basis  $B \in \mathbb{Z}^{m \times n}$  and a target vector  $t \in \mathbb{R}^m$ , find a lattice vector  $Bx$  closest to the target  $t$ , i.e., find an integer vector  $x \in \mathbb{Z}^n$  such that  $\|Bx - t\| \leq \|By - t\|$  for any other  $y \in \mathbb{Z}^n$ .

After knowing the definition of lattice and its computational problem, given the formal definition of Learning Error (LWE). The parameterization of LWE are positive integers  $n$  and  $q$ , and an error distribution  $\chi$  over  $\mathbb{Z}$ .

**Definition 4 (LWE [8])** For a vector  $s \in \mathbb{Z}_q^n$  called the secret, the LWE distribution  $A_{s,\chi}$  over  $\mathbb{Z}_q^n \times \mathbb{Z}_q$  is sampled by choosing  $a \in \mathbb{Z}_q^n$  uniformly at random, choosing  $e \leftarrow \chi$ , and outputting  $(a, b = \langle s, a \rangle + e \pmod q)$ .

Furthermore, the following example illustrates Definition 4

**Example 1** Let secret  $\mathbf{s} = (0, 1, 2, 3, 4)$  and error  $e = 1 \rightarrow \text{Poisson}(n = 1, \lambda = 1)$ . then, choosing uniformly random vector  $\mathbf{a} = (3, 1, 3, 2, 1)$ . The samples of LWE distribution  $A_{s,\chi}$  is as follows

$$(\mathbf{a}, b) = \left( \begin{pmatrix} 3 \\ 1 \\ 3 \\ 2 \\ 1 \end{pmatrix}, \langle \mathbf{s}, \mathbf{a} \rangle + (e = 1) \pmod{5} \right) = \left( \begin{pmatrix} 3 \\ 1 \\ 3 \\ 2 \\ 1 \end{pmatrix}, 18 \pmod{5} \right) = \left( \begin{pmatrix} 3 \\ 1 \\ 3 \\ 2 \\ 1 \end{pmatrix}, 3 \right).$$

There are two computational problems of LWE i.e, search problem and decision problem, that are defined as follows

**Definition 5 (Search Problem LWE [8])** Given  $m$  independent samples  $(a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$  drawn from  $A_{s,\chi}$  for a uniformly random  $s \in \mathbb{Z}_q^n$ , find  $s$ .

**Definition 6 (Decision Problem LWE [8])** Given  $m$  independent samples  $(a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$  where every sample is distributed according to either: (1)  $A_{s,\chi}$  for a uniformly random  $s \in \mathbb{Z}_q^n$  (fixed for all samples), or (2) the uniform distribution, distinguish which is the case (with non-negligible advantage).

Based on the definitions above, adding an error is significant to change the structure, such that the vector  $s$  is hard to find. Because, without the error, finding the vector  $\mathbf{s}$  is the same as finding the solution by Gaussian elimination from the system of linear equation  $\mathbf{A}^T \mathbf{s} = \mathbf{b}$  with the column of matrix  $A$  are the sample  $a_i \in \mathbb{Z}_q^n$  from LWE distribution, and also vector  $\mathbf{b}$  is constructed from sample  $b_i \in \mathbb{Z}_q$  from LWE distribution,  $i = 1, 2, 3, \dots, m$ , for some  $m \in \mathbb{N}$ . Moreover, the search problem of LWE can be seen as the closest vector problem of Lattice. Because for LWE samples, vector  $\mathbf{b}$  is relatively close to exactly one vector in the LWE lattice

$$\mathcal{L}_{LWE}(A) = \{A^T s : s \in \mathbb{Z}_q^n\} + q\mathbb{Z}^m$$

The following examples demonstrates Definition 5 and Definition 6.

**Example 2** Consider the following problems.

- Let  $(n = 5, m = 4, q = 5)$  are the parameterization of LWE, secret  $s = (1, 2, 3, 4, 1)$  and error  $e = (1, 0, 0, 0) \rightarrow Poisson(n = 4, \lambda = 1)$ . Also,

$$A = \begin{bmatrix} 1 & 2 & 4 & 1 \\ 3 & 2 & 3 & 2 \\ 4 & 1 & 3 & 2 \\ 1 & 1 & 2 & 2 \\ 3 & 1 & 2 & 2 \end{bmatrix}.$$

Considered that,

$$A^t \cdot \mathbf{s} + \mathbf{e} \pmod{5} = \begin{bmatrix} 1 & 3 & 4 & 1 & 3 \\ 2 & 2 & 1 & 1 & 1 \\ 4 & 3 & 3 & 2 & 2 \\ 1 & 2 & 2 & 2 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \pmod{5} = \begin{bmatrix} 2 \\ 4 \\ 4 \\ 1 \end{bmatrix} \rightarrow \mathbf{b}$$

After getting sample  $b$  of the LWE distribution, then we will do the simulation of the search problem on LWE, i.e to find vector  $\mathbf{s}$  based on the sample  $(A, \mathbf{b})$ . Using Gaussian

Elimination, we obtained vector  $\mathbf{s}' = (1, 2, 3, 0, 1)$ . However,  $\mathbf{s}' \neq \mathbf{s}$ . so, it clears that the error makes the problem hard to solve.

2. Let  $(n = 5, m = 4, q = 5)$  are the parameterization of LWE, and secret  $\mathbf{s} = (1, 2, 3, 4, 1)$ . Further, let  $e = 1 \rightarrow Poisson(n = 1, \lambda = 1)$  is an error. Given some of elements in  $\mathbb{Z}_5^5 \times \mathbb{Z}_5$ , as follows ;

- (i)  $(\mathbf{a}, 1)$
- (ii)  $(\mathbf{a}, 2)$
- (iii)  $(\mathbf{a}, 3)$
- (iv)  $(\mathbf{a}, 4)$

with vector  $a = (3, 2, 3, 4, 4)$ . In the decision problem, we observe each of (i),(ii),(iii), and (iv), whether it is a sample of LWE distribution or just an element of  $\mathbb{Z}_5^5 \times \mathbb{Z}_5$ . Considered that,

$$\begin{aligned} \langle \mathbf{s}, \mathbf{a} \rangle + (e = 1) \pmod{5} &= 3 + 4 + 9 + 16 + 4 + 1 \pmod{5} \\ &= 1 + 1 \pmod{5} \\ &= 2. \end{aligned}$$

According to the estimation, the sample of LWE distribution is (ii).

After discussing LWE problems, The implementation of LWE for encryption and encryption scheme is given as follows.

### Encryption

The encryption scheme with LWE is asymmetric cryptography that uses a public key and a private key. Then, the parameterizations of LWE are two positive integers  $n$  and  $q$ . Alice and Bob will share a secret message "x" to the insecure communication channel using LWE, the steps are as follows.

- i. Bob chooses his private key,  $r \in \mathbb{Z}_q^n$ .
- ii. Both Bob and Alice acquiescent matrix  $A \in \mathbb{Z}_q^{n \times m}$  for constructing their public key.
- iii. Next, Alice share her public key to Bob, called  $b$  which is obtained from  $b = A \cdot s + e_1$  with  $s \in \mathbb{Z}_q^m$  is Alice's private key, and  $e_1$  is an error.
- iv. Last steps, using Bob's Private key and Alice's Public key, the message is encrypted as follows.

$$\mathbf{y} = (u, v) = (\mathbf{r}^T \cdot \mathbf{A} + \mathbf{e}_2, \mathbf{r}^T \cdot \mathbf{b} + e_3 + x) \quad (1)$$

with  $y$  is a pair of ciphertext from the encryption of message  $x$ . Then, the ciphertext is ready to be sent to Alice.

### Decryption

After receiving the ciphertext from Bob, Alice does a decryption scheme using her private key as follows

$$x = v - (u \cdot s). \quad (2)$$

Futhermore,

$$\begin{aligned}
 v - (u \cdot s) &= (\mathbf{r}^T \cdot \mathbf{b} + e_3 + x) - ((\mathbf{r}^T \cdot \mathbf{A} + \mathbf{e}_2) \cdot \mathbf{s}) \\
 &= \mathbf{r}^T \cdot \mathbf{b} + e_3 + x - \mathbf{r}^T \cdot \mathbf{A} \cdot \mathbf{s} + \mathbf{e}_2 \cdot \mathbf{s} \\
 &= \mathbf{r}^T \cdot (\mathbf{A} \cdot \mathbf{s} + \mathbf{e}_1) + e_3 + x - \mathbf{r}^T \cdot \mathbf{A} \cdot \mathbf{s} + \mathbf{e}_2 \cdot \mathbf{s} \\
 &= \mathbf{r}^T \cdot \mathbf{A} \cdot \mathbf{s} + \mathbf{r}^T \cdot \mathbf{e}_1 + e_3 + x - \mathbf{r}^T \cdot \mathbf{A} \cdot \mathbf{s} + \mathbf{e}_2 \cdot \mathbf{s} \\
 &\approx x + e^* \\
 &\approx x.
 \end{aligned}$$

The example below is given to demonstrate the encryption and decryption scheme of LWE as follows.

**Example 3** Bob wants to share a secret message  $m = 19$  to Alice using LWE with parameters ( $n = 20, q = 97$ ). First step, Bob and Alice choose the matrix

$$A = \begin{bmatrix} 60 & 49 & 63 & 87 & 17 & 12 & 29 & 82 & 37 & 10 & 28 & 78 & 64 & 40 & 56 & 92 & 80 & 62 & 6 & 51 \end{bmatrix}$$

for constructing their public key. Next, Alice constructst her public key using her private key  $s = 20$  dan the error

$$\mathbf{e}_1 = \begin{bmatrix} 4 & 3 & 2 & 2 & 1 & 4 & 2 & 2 & 4 & 2 & 4 & 2 & 4 & 2 & 4 & 3 & 4 & 3 & 4 & 2 \end{bmatrix}.$$

Then, Alice's public key is obtained from  $b = A \cdot s + e_1$  as follows

$$\mathbf{b} = \begin{bmatrix} 40 & 13 & 1 & 93 & 50 & 50 & 0 & 90 & 65 & 8 & 79 & 10 & 23 & 26 & 57 & 0 & 52, & 79 & 27 & 52 \end{bmatrix}.$$

Before encrypting the message, Bob convert the message  $m = 19$  to 8-bit binary number  $(0, 0, 0, 1, 0, 0, 1, 1)$ . The message is encrypted one by one of binary bits. For the simulation, we will **encrypt** the first bit call it  $x_1 = 0$ . The steps are as follows

- i) Bob choose his private key  $r = (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \in \mathbb{Z}_{97}^{20}$ .
- ii) Next, calculating the pair of ciphertext  $(u_1, v_1)$  as follows

$$\begin{aligned}
 u_1 &= A \cdot \mathbf{r} + \mathbf{e}_2 \pmod q \\
 v_1 &= \mathbf{b} \cdot \mathbf{r} + \mathbf{e}_3 + \frac{q}{2} \cdot m \pmod q.
 \end{aligned}$$

Then, we obtained the ciphertext for  $x_1$ , they are  $u_1 = 0$  dan  $v_1 = 1$ . Futhermore,  $(u_1, v_1)$  is sent to Alice and be **decrypted**. The steps as follows.

- i) The decryption scheme for  $(u_1, v_1)$  is using the methods,

$$d = v_1 - u_1 \cdot s \pmod q$$

with  $s$  is Alice's private key. If  $d < \frac{q}{2}$  then the message is 0, beside that is 1.

ii) For  $(u_1, v_1) = (9, 1)$ , considered that

$$d = 1 - (9 \cdot 20) \pmod{97} = 15.$$

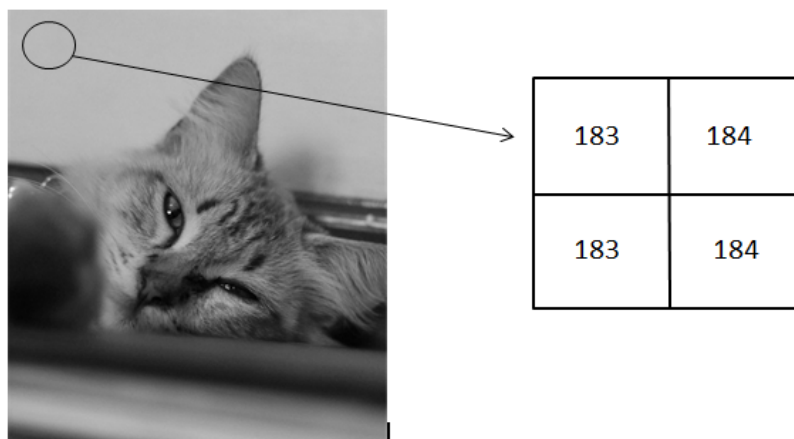
i) Because  $d < \frac{97}{2}$ , then  $x_1 = 0$ .

The encryption and decryption for subsequent bits are left as an exercise.

### III. DISCUSSION AND SIMULATION

According to Gonzalez and Woods (2018), An image may be defined as a two-dimensional function  $f(x, y)$ . where  $x$  and  $y$  are spatial (plane) coordinates and the amplitude of  $f$  at any pair of coordinates  $(x, y)$  is called the intensity of the image at the point. Then, The digital image is a two-dimensional image that is displayed on the digital screen as a set or discrete digital values called pixels or image elements. Thus, the digital image can be interpreted as a matrix whose element is a pixel value.

Marleny (2021) explained three kinds of digital images according to their colour and pixels, there are RGB images, grayscale images, and binary images. In this paper specifically discusses digital image encryption using the grayscale image. The matrix representation of grayscale image consists grey intensity values that starts from 0 (white) until 255 (black). The following picture illustrates the matrix representation of grayscale image.



**Figure 1.** Pixels Value of Grayscale Image

In the previous discussion, LWE is used for encryption and decryption of a message. Then, in this section, we will do the encryption and decryption using the digital image. Furthermore, the simulation was using a laptop with Intel(R) Core(TM) i5-6198DU CPU @2.30GHz 2.40 GHz specifications and Python 3 with the attached algorithm.

#### SIMULATION

Given  $2 \times 2$  pixels image as follows



**Figure 2.** The Image Before Encrypted.

Let matrix  $A_{2 \times 2}$  is the grayscale matrix representation of image

$$A = \begin{bmatrix} 205 & 230 \\ 193 & 219 \end{bmatrix}.$$

Let  $(n = 20, q = 251)$  as the parameters of LWE. Note that, selecting the value of  $q$  is important to restrict the grayscale intensity value. After that, we define the binary string of each element of  $A$ , call it  $a_1 = 205, a_2 = 230, a_3 = 193, a_4 = 219$ . Furthermore, we are obtained

$$\begin{aligned} a_1 &= (1, 1, 0, 0, 1, 1, 0, 1) \\ a_2 &= (1, 1, 1, 0, 0, 1, 1, 0) \\ a_3 &= (1, 1, 0, 0, 0, 0, 0, 1) \\ a_4 &= (1, 1, 0, 1, 1, 0, 1, 1). \end{aligned}$$

### ENCRYPTION

After converting the elements of  $M$  to a binary string, we encrypt each bit of the binary string using the LWE encryption scheme on Equation 1 as follows

i) For  $a_1 = (1, 1, 0, 0, 1, 1, 0, 1)$ , the pairs of ciphertext from each bit are

$$\begin{aligned} a_{11} = 1 &\rightarrow (u_1, v_1) = (51, 144) \\ a_{12} = 1 &\rightarrow (u_2, v_2) = (51, 144) \\ a_{13} = 0 &\rightarrow (u_3, v_3) = (149, 222) \\ a_{14} = 0 &\rightarrow (u_4, v_4) = (222, 175) \\ a_{15} = 1 &\rightarrow (u_5, v_5) = (222, 49) \\ a_{16} = 1 &\rightarrow (u_6, v_6) = (231, 229) \\ a_{17} = 0 &\rightarrow (u_7, v_7) = (196, 157) \\ a_{18} = 1 &\rightarrow (u_8, v_8) = (237, 97). \end{aligned}$$

From the pairs of ciphertext, constructed the new matrix call it  $M_1$

$$\begin{aligned} M_1 &= \begin{bmatrix} u_1 & v_1 & u_2 & v_2 & u_3 & v_3 & u_4 & v_4 & u_5 & v_5 & u_6 & v_6 & u_7 & v_7 & u_8 & v_8 \end{bmatrix} \\ &= \begin{bmatrix} 51 & 144 & 51 & 144 & 149 & 222 & 222 & 175 & 222 & 49 & 231 & 229 & 196 & 157 & 237 & 97 \end{bmatrix}. \end{aligned}$$



ii) For  $a_2 = (1, 1, 1, 0, 0, 1, 1, 0)$ , the pairs of ciphertext are

$$\begin{aligned} a_{21} = 1 &\rightarrow (u_1, v_1) = (184, 41) \\ a_{22} = 1 &\rightarrow (u_2, v_2) = (184, 41) \\ a_{23} = 1 &\rightarrow (u_3, v_3) = (149, 96) \\ a_{24} = 0 &\rightarrow (u_4, v_4) = (78, 58) \\ a_{25} = 0 &\rightarrow (u_5, v_5) = (244, 115) \\ a_{26} = 1 &\rightarrow (u_6, v_6) = (199, 90) \\ a_{27} = 1 &\rightarrow (u_7, v_7) = (211, 82) \\ a_{28} = 0 &\rightarrow (u_8, v_8) = (38, 0). \end{aligned}$$

From the pairs of ciphertext, constructed the new matrix call it  $M_2$

$$\begin{aligned} M_2 &= \begin{bmatrix} u_1 & v_1 & u_2 & v_2 & u_3 & v_3 & u_4 & v_4 & u_5 & v_5 & u_6 & v_6 & u_7 & v_7 & u_8 & v_8 \end{bmatrix} \\ &= \begin{bmatrix} 184 & 41 & 184 & 41 & 149 & 96 & 78 & 58 & 244 & 115 & 199 & 90 & 211 & 82 & 138 & 0 \end{bmatrix}. \end{aligned}$$

iii) For  $a_3 = (1, 1, 0, 0, 0, 0, 0, 1)$ , the pairs of ciphertext are

$$\begin{aligned} a_{31} = 1 &\rightarrow (u_1, v_1) = (121, 37) \\ a_{32} = 1 &\rightarrow (u_2, v_2) = (10, 76) \\ a_{33} = 0 &\rightarrow (u_3, v_3) = (121, 163) \\ a_{34} = 0 &\rightarrow (u_4, v_4) = (121, 163) \\ a_{35} = 0 &\rightarrow (u_5, v_5) = (93, 105) \\ a_{36} = 0 &\rightarrow (u_6, v_6) = (6, 124) \\ a_{37} = 0 &\rightarrow (u_7, v_7) = (6, 124) \\ a_{38} = 1 &\rightarrow (u_8, v_8) = (154, 195). \end{aligned}$$

From the pairs of ciphertext, constructed the new matrix call it  $M_3$

$$\begin{aligned} M_3 &= \begin{bmatrix} u_1 & v_1 & u_2 & v_2 & u_3 & v_3 & u_4 & v_4 & u_5 & v_5 & u_6 & v_6 & u_7 & v_7 & u_8 & v_8 \end{bmatrix} \\ &= \begin{bmatrix} 121 & 37 & 10 & 76 & 121 & 163 & 121 & 163 & 93 & 105 & 6 & 124 & 6 & 124 & 154 & 195 \end{bmatrix}. \end{aligned}$$



iv) For  $a_4 = (1, 1, 0, 1, 1, 0, 1, 1)$ , the pairs of ciphertext are

$$\begin{aligned} a_{41} = 1 &\rightarrow (u_1, v_1) = (0, 129) \\ a_{42} = 1 &\rightarrow (u_2, v_2) = (144, 247) \\ a_{43} = 0 &\rightarrow (u_3, v_3) = (11, 224) \\ a_{44} = 1 &\rightarrow (u_4, v_4) = (45, 24) \\ a_{45} = 1 &\rightarrow (u_5, v_5) = (144, 247) \\ a_{46} = 0 &\rightarrow (u_6, v_6) = (30, 101) \\ a_{47} = 1 &\rightarrow (u_7, v_7) = (199, 92) \\ a_{48} = 1 &\rightarrow (u_8, v_8) = (191, 183). \end{aligned}$$

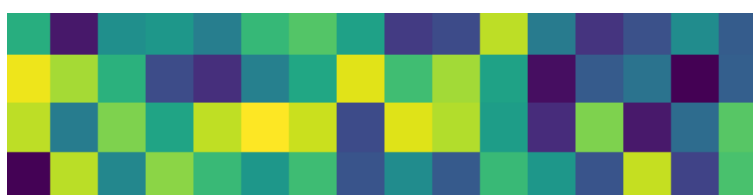
From the pairs of ciphertext, constructed the new matrix call it  $M_4$

$$\begin{aligned} M_4 &= \begin{bmatrix} u_1 & v_1 & u_2 & v_2 & u_3 & v_3 & u_4 & v_4 & u_5 & v_5 & u_6 & v_6 & u_7 & v_7 & u_8 & v_8 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 129 & 144 & 247 & 11 & 224 & 45 & 24 & 144 & 247 & 30 & 101 & 199 & 92 & 191 & 183 \end{bmatrix}. \end{aligned}$$

Then, we construct the new matrix called C, which consists of matrix block  $M_1, M_2, M_3, M_4$  as follows

$$C = \begin{bmatrix} 51 & 144 & 51 & 144 & 149 & 222 & 222 & 175 & 222 & 49 & 231 & 229 & 196 & 157 & 237 & 97 \\ 184 & 41 & 184 & 41 & 149 & 96 & 78 & 58 & 244 & 115 & 199 & 90 & 211 & 82 & 138 & 0 \\ 121 & 37 & 10 & 76 & 121 & 163 & 121 & 163 & 93 & 105 & 6 & 124 & 6 & 124 & 154 & 195 \\ 0 & 129 & 144 & 247 & 11 & 224 & 45 & 24 & 144 & 247 & 30 & 101 & 199 & 92 & 191 & 183 \end{bmatrix}$$

So, matrix C becomes the cipher of the image. Furthermore, we convert the matrix C to the grayscale image to see the visual after encryption as follows



**Figure 3.** The Encrypted Image

According to Figure 3, it is obvious that the image size is larger than Figure 2. Also, the pixels become noise so it is hard to identify.

## DECRYPTION

This section demonstrates the decryption scheme of Figure 3. In the previous discussion, the matrix representation of Figure 3 is

$$C = \begin{bmatrix} 51 & 144 & 51 & 144 & 149 & 222 & 222 & 175 & 222 & 49 & 231 & 229 & 196 & 157 & 237 & 97 \\ 184 & 41 & 184 & 41 & 149 & 96 & 78 & 58 & 244 & 115 & 199 & 90 & 211 & 82 & 138 & 0 \\ 121 & 37 & 10 & 76 & 121 & 163 & 121 & 163 & 93 & 105 & 6 & 124 & 6 & 124 & 154 & 195 \\ 0 & 129 & 144 & 247 & 11 & 224 & 45 & 24 & 144 & 247 & 30 & 101 & 199 & 92 & 191 & 183 \end{bmatrix}$$

Considering the real image size is  $2 \times 2$  pixels, each row of matrix  $C$  represents the pairs of ciphertext from each bit of binary string of real pixel value. Then, we split matrix  $C$  into four block matrix as follows

$$C_1 = \begin{bmatrix} 51 & 144 & 51 & 144 & 149 & 222 & 222 & 175 & 222 & 49 & 231 & 229 & 196 & 157 & 237 & 97 \end{bmatrix}$$

$$C_2 = \begin{bmatrix} 184 & 41 & 184 & 41 & 149 & 96 & 78 & 58 & 244 & 115 & 199 & 90 & 211 & 82 & 138 & 0 \end{bmatrix}$$

$$C_3 = \begin{bmatrix} 121 & 37 & 10 & 76 & 121 & 163 & 121 & 163 & 93 & 105 & 6 & 124 & 6 & 124 & 154 & 195 \end{bmatrix}$$

$$C_4 = \begin{bmatrix} 0 & 129 & 144 & 247 & 11 & 224 & 45 & 24 & 144 & 247 & 30 & 101 & 199 & 92 & 191 & 183 \end{bmatrix}.$$

Next, we define each element of  $C_k$  for  $k = 1, 2, 3, 4$  sequentially to be  $(u_i, v_i)$  for  $i = 1, 2, 3, 4, 5, 6, 7, 8$ . Then, we decrypt  $(u_i, v_i)$  using Equation 2. Moreover, the binary strings from the decryption are converted to the integer so that we obtain the real pixel value of Figure 2. Considered the following steps as follows.

i) For matrix  $C_1$ ,

$$c_{1,1} = 51 \rightarrow u_1$$

$$c_{1,2} = 144 \rightarrow v_1$$

$$c_{1,3} = 51 \rightarrow u_2$$

$$c_{1,4} = 144 \rightarrow v_2$$

$$c_{1,5} = 149 \rightarrow u_3$$

$$c_{1,6} = 222 \rightarrow v_3$$

$$c_{1,7} = 222 \rightarrow u_4$$

$$c_{1,8} = 175 \rightarrow v_4$$

$$c_{1,9} = 222 \rightarrow u_5$$

$$c_{1,10} = 49 \rightarrow v_5$$

$$c_{1,11} = 231 \rightarrow u_6$$

$$c_{1,12} = 229 \rightarrow v_6$$

$$c_{1,13} = 196 \rightarrow u_7$$

$$c_{1,14} = 157 \rightarrow v_7$$

$$c_{1,15} = 237 \rightarrow u_8$$

$$c_{1,16} = 97 \rightarrow v_8.$$

The plaintext  $d_1$  to represent the value of the first pixel is

$$d_1 = (1, 1, 0, 0, 1, 1, 0, 1) \rightarrow d_1 = 205.$$

ii) For matrix  $C_2$ ,

$$c_{2,1} = 184 \rightarrow u_1$$

$$c_{2,2} = 41 \rightarrow v_1$$

$$c_{2,3} = 184 \rightarrow u_2$$

$$c_{2,4} = 41 \rightarrow v_2$$

$$c_{2,5} = 149 \rightarrow u_3$$

$$c_{2,6} = 96 \rightarrow v_3$$

$$c_{2,7} = 78 \rightarrow u_4$$

$$c_{2,8} = 58 \rightarrow v_4$$

$$c_{2,9} = 244 \rightarrow u_5$$

$$c_{2,10} = 115 \rightarrow v_5$$

$$c_{2,11} = 199 \rightarrow u_6$$

$$c_{2,12} = 90 \rightarrow v_6$$

$$c_{2,13} = 211 \rightarrow u_7$$

$$c_{2,14} = 82 \rightarrow v_7$$

$$c_{2,15} = 138 \rightarrow u_8$$

$$c_{2,16} = 0 \rightarrow v_8.$$

The plaintext  $d_2$  to represent the value of the second pixel is

$$d_2 = (1, 1, 1, 0, 0, 1, 1, 0) \rightarrow d_2 = 230.$$

iii) For matrix  $C_3$ ,

$$c_{3,1} = 121 \rightarrow u_1$$

$$c_{3,2} = 37 \rightarrow v_1$$

$$c_{3,3} = 10 \rightarrow u_2$$

$$c_{3,4} = 76 \rightarrow v_2$$

$$c_{3,5} = 121 \rightarrow u_3$$

$$c_{3,6} = 163 \rightarrow v_3$$

$$c_{3,7} = 121 \rightarrow u_4$$

$$c_{3,8} = 163 \rightarrow v_4$$

$$c_{3,9} = 93 \rightarrow u_5$$

$$c_{3,10} = 105 \rightarrow v_5$$

$$c_{3,11} = 6 \rightarrow u_6$$

$$c_{3,12} = 124 \rightarrow v_6$$

$$c_{3,13} = 6 \rightarrow u_7$$

$$c_{3,14} = 124 \rightarrow v_7$$

$$c_{3,15} = 154 \rightarrow u_8$$

$$c_{3,16} = 195 \rightarrow v_8.$$

The plaintext  $d_3$  to represent the value of the first pixel is

$$d_3 = (1, 1, 0, 0, 0, 0, 0, 1) \rightarrow d_3 = 193.$$





iv) For matrix  $C_4$ ,

$$\begin{aligned} c_{4,1} &= 0 \rightarrow u_1 \\ c_{4,2} &= 129 \rightarrow v_1 \\ c_{4,3} &= 144 \rightarrow u_2 \\ c_{4,4} &= 247 \rightarrow v_2 \\ c_{4,5} &= 11 \rightarrow u_3 \\ c_{4,6} &= 224 \rightarrow v_3 \\ c_{4,7} &= 45 \rightarrow u_4 \\ c_{4,8} &= 24 \rightarrow v_4 \\ c_{4,9} &= 144 \rightarrow u_5 \\ c_{4,10} &= 247 \rightarrow v_5 \\ c_{4,11} &= 30 \rightarrow u_6 \\ c_{4,12} &= 101 \rightarrow v_6 \\ c_{4,13} &= 199 \rightarrow u_7 \\ c_{4,14} &= 92 \rightarrow v_7 \\ c_{4,15} &= 191 \rightarrow u_8 \\ c_{4,16} &= 183 \rightarrow v_8. \end{aligned}$$

The plaintext  $d_3$  to represent the value of the first pixel is

$$d_4 = (1, 1, 0, 1, 1, 0, 1, 1) \rightarrow d_4 = 219.$$

Last step, we arrange  $d_1, d_2, d_3, d_4$  as a  $(2 \times 2)$  matrix, then convert it to the grayscale images as follows

205	230		
193	219		

**Figure 4.** The Image After Decrypted

#### IV. CONCLUSIONS AND FUTURE RESEARCH DIRECTION

The paper concludes that LWE can be used for encrypting and decrypting the digital image (on grayscale). The paper suggests some possible future research directions, such as exploring the encryption and decryption for RGB images with LWE. Moreover, it is also possible to explore Ring LWE for encrypting and decrypting the digital images, whether the computation is more efficient than LWE or not.

## REFERENCES

- [1] Ajtai, M., 1996, "Generating hard instances of lattice problems", *Quaderni di Matematica*, 13:1–32.
- [2] Davidowitz, N.S., 2018, "Ring-SIS and Ideal Lattices", [www.noahsd.com](http://www.noahsd.com), Diakses pada tanggal 3 Mei 2023.
- [3] Gonzalez, R. C., and Woods, R. E., 2018, *Digital Image Processing, Fourth Edition*, Pearson, New York.
- [4] Marleny, F. D., 2021, *Pengolahan Citra Digital Menggunakan Python, Vol. 1*, CV. Pena Persada.
- [5] Macciancio, D., Goldwasser, S., 2002, *Complexity Of Lattice Problems A Cryptographic Perspective*, Springer Science Business Media, New York.
- [6] National Institute of Standards and Technology Interagency, 2022, "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process", FIPS 203.
- [7] National Institute of Standards and Technology Interagency, 2023, *Module-Lattice-based Key-Encapsulation Mechanism Standard*, FIPS 203.
- [8] Peikert, C., 2016, "A Decade of Lattice Cryptography", *Lattice Survey*, Supported by the National Science Foundation under CAREER Award CCF-1054495, by DARPA under agreement number FA8750-11- C-0096, and by the Alfred P. Sloan Foundation.
- [9] Regev, O., 2005, "On lattices, learning with errors, random linear codes, and cryptography", *J. ACM*, 56(6):1–40.
- [10] Stinson, R.D., 2006, *Cryptography Theory And Practice*, Third Edition, CRC Press.