Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th October 2023. Vol. 2. No. 3; e-ISSN : 2808-4519

Digital Image Security Implementation With Uses Super Encryption Algorithm Myszkowski And The Algorithm Paillier Cryptosystem

Eva Piona[1], Achmad Fauzi [2], Milli Alfhi Syari[3]

1,2,3 Teknik Informatika, STMIK KAPUTAMA

Jl. Veteran No. 4A-9A, Binjai, Sumatera Utara, Indonesia

evapiona1@gmail.com[1], fauzyrivai88@gmail.com[2], milli.fhisya@gmail.com[3]*

Abstract

This study aims to implement digital image security by applying two encryption algorithms, namely the Myszkowski algorithm and the Paillier Cryptosystem algorithm. Digital images are a very important form of data and are used frequently in a variety of applications, so protecting their security is a major concern. The encryption method proposed in this study uses a combination of the Myszkowski algorithm to randomize image pixels and the Paillier Cryptosystem algorithm to perform symmetric key encryption.
At the experimental stage, qualitative and quantitative analysis was carried out on the performance of the encryption implemented on digital images. Testing is carried out by comparing the level of security and encryption speed of the two algorithms used. In addition, size analysis of encrypted images was also performed to evaluate the efficiency of the proposed system.
The results of the study show that the use of a combination of the Myszkowski algorithm and the Paillier Cryptosystem algorithm provides a high level of security for digital images. In addition, the efficiency of this system has also been proven in producing efficient encryption image sizes, so that it can be implemented in image-based applications that require a higher level of security.

Keywords: *Cryptography, image, myszkowski algorithm, paillier cryptosystem algorithm.*

1. Introduction

In today's digital era, it is very important to consider information security. Information generated by users or companies must often be kept confidential to prevent misuse by unauthorized individuals. The problem of computer information security is an important issue in today's digital era. There are many cyber crimes that we often hear from the mass media. Criminals take advantage of security holes in computer-based systems to enter and manipulate information. One form of confidential information is a digital image. A digital image is an image consisting of pixels which can be represented as a binary number.

Using Myszkowski and Paillier Cryptosystem is one way to secure images. The combination of these two algorithms can create security in digital images, by encrypting images by changing objects that are blurry or not very clear, so that it is not easily understood by unauthorized people. The Myszkowski algorithm is a cryptographic technique used to increase the security of digital images by randomizing the arrangement of pixels in the image. The Paillier Cryptosystem algorithm is a cryptographic algorithm used for data encryption and decryption. The algorithm developed by Pascal Paillier in 1999 is a probabilistic asymmetric algorithm for public key cryptography.

2. Research methodology

2.1. Cryptography

Cryptography comes from the Greek words crypto and graphia. Crypto means secret and graphia means writing. In general, cryptography can be interpreted as a science and art that aims to maintain the secrecy of a message. Cryptography has been known since ancient times, according to history cryptography has been used thousands of years ago, which was introduced by the Egyptians during the war to send secret messages to a general sent by courier [1].

2.2. Classic Algorithms and Modern Algorithms

Classical cryptography is a type of cryptography that has been around for centuries, and was used to secure messages in the past. Classical cryptography alters the original message using certain techniques so that only people with special knowledge can read or understand it. This technique can be done in several ways, such as replacing characters or words, changing letters, or combining separate words. Classical algorithms can be grouped into two types of ciphers, namely substitution ciphers and transposition ciphers [2].

Modern cryptography is cryptography that is widely used in the digital era. Digital computers represent data in binary form (0 and 1), so information in any form can be encrypted as long as it is represented in binary form. The emergence of modern cryptography was caused by the use of computers, so that classical cryptography was developed into modern cryptography by utilizing information technology equipment to be able to solve it [3].

2.3. Myszkowski Algorithm

Myszkowski algorithm is one of the cryptographic algorithms used for encryption. In the encryption process, the plaintext is written horizontally from left to right, then the ciphertext is read vertically according to the key sequence that has been made [4].
The encryption and decryption techniques in the Myszkowski algorithm are as follows:
Myszkowski encryption technique: Before carrying out the encryption process, a key is formed first. Several letters that are formed manually or randomly can add variety to the formation of keys and strengthen the security of the encryption process. For example plaintext and key as follows :
Plaintext : HARI INI CUACA SANGAT CERAH
Key : EVA PIONA
The encryption process using the key above produces the ciphertext as follows:
Ciphertext : RCCG CXHU AISR INHN AAIA EAAT
Myszkowski decryption technique: The decryption process can be done by writing the ciphertext vertically from top to bottom sequentially according to the key number. For the same key numbering, the ciphertext must be written horizontally.
Ciphertext : RCCG CXHU AISR INHN AAIA EAAT
Key : EVA PIONA
So that from the above decryption process, the plaintext initial results can be obtained as follows:
Plaintext : HARI INI CUACA SANGAT CERAH

2.4. Paillier Cryptosystem Algorithm

The algorithm developed by Pascal Paillier in 1999 is a probabilistic asymmetric algorithm for public key cryptography. The security of this algorithm is based on the difficulty of solving the nth residual problem. The paillier cryptosystem algorithm consists of procedures for generating public and private keys, encryption and decryption procedures [5].
Private key formation process:

1. Choose two prime numbers at random p and q
2. Calculate the value $n = p * q$ and $\lambda = LCM(p - 1, q - 1)$.
   LCM = Least Common Multiple or
3. Choose a random integer g, where $g < n^2$.
4. Calculate $\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$, where the function $L(x) = (x-1) / n$.

The results of the key formation process above:

1. The public key is (g, n).
2. The private key is (λ, μ).

Encryption process:

1. Suppose m is the message to be encrypted, provided that $0 \leq m < n$.
3. Choose a random integer r with conditions $0 \leq r < n$ and PBB (r,n) = 1.
4. Calculate ciphertext from m with the following formula: $c = gm * rn \bmod n^2$

Decryption process:

1. Suppose c ciphertext to be decrypted.
2. Calculate the plaintext of c with the following formula:
   $m = L(c\lambda \bmod n^2) * \mu \bmod n$
   To get the public and private keys, the process is as follows:
   The key formation process using the paillier cryptosystem algorithm is as follows:
   a. Choose two prime numbers p and q at random
      p = 11
      q = 13
   b. Calculate the value of n and λ
      n = p *q
      n = 11 * 13
      n = 143
      $\lambda = LCM(p - 1, q - 1) = LCM(11 - 1, 13 - 1)$
      $= LCM(10, 12)$
      $= 60$
      LCM (10, 12)
      $10 = 2 * 5$ and $12 = 2^2 * 3$, so that the KPK = $2^2 * 5 * 3 = 60$
   c. Choose a random integer g, where $g < n^2$
      g = 3260

d. Calculate the value of $\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$, where the function $L(x) = (x-1) / n$.
$(L(g^{\lambda} \bmod n^2))^{-1} \bmod n$
$L(g^{\lambda} \bmod n^2) = L(3260^{60} \bmod 143^2)$
$= L(3260^{60} \bmod 20449)$
$= L(10297)$
$L(x) = (x-1) / n$
$L(x) = (10297 – 1) /143$
$L(x) = 72$
$\mu = 72^{-1} \bmod 143 = 2$
e. Public key (g, n) = (3260, 143)
f. Private key (λ, μ) = (60, 2)

2.5. Image definition

Image is a still image (photo) or moving image such as a video recording, while digital is image or image processing that is done digitally using a computer [6]. Digital image refers to 2-dimensional image processing using a computer. A digital image is an array (array) containing real and complex values presented with a certain row of bits. The process of making a digital image begins with taking pictures with a digital camera or scanner. The image is then converted into a digital format that can be processed by a computer. At this stage, the image is split into small pixels that have different color values and light intensities [7].

3. Results

3.1. Myszkowski algorithm encryption calculation

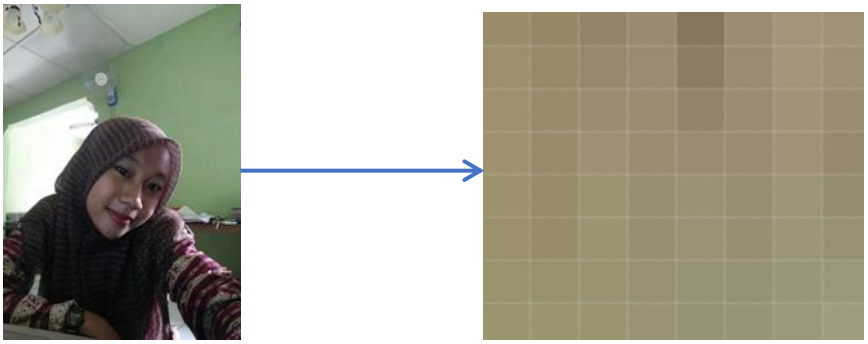

Figure 1: Example Image and 8X8 Pixel Image Pixels

Figure 1 is an image to be encrypted. To find the value of each pixel by using additional software, namely Photoshop. The image size used is 1201 x 1698 pixels. In the process of securing this digital image, an image sample with a size of 8 x 8 pixels will be taken, then the pixels will be converted into RGB (Red, Green, Blue) values using Photoshop which will start from pixels (0,0) to (7, 7). Following are the plaintext steps that will be performed by the Myszkowski encryption process, namely Plaintext:

Table 1: 8x8 Pixel Sample

R : 153 G : 140 B : 106	R : 149 G: 136 B: 102	R : 146 G : 132 B : 102	R : 153 G : 139 B : 113	R : 133 G : 119 B : 93	R : 154 G : 140 B : 114	R : 162 G : 148 B : 121	R : 160 G : 147 B : 115
R : 156 G : 143 B : 109	R : 151 G : 138 B : 104	R : 150 G : 136 B : 107	R : 154 G : 140 B : 114	R : 139 G : 125 B : 99	R : 154 G : 140 B : 114	R : 162 G : 148 B : 121	R : 158 G : 145 B : 113
R : 158 G : 145 B : 111	R : 153 G : 140 B : 106	R : 153 G : 142 B : 110	R : 153 G : 142 B : 114	R : 145 G : 133 B : 107	R : 152 G : 140 B : 114	R : 159 G : 148 B : 118	R : 152 G : 141 B : 111
R : 159 G : 146 B : 112	R : 153 G : 140 B : 106	R : 157 G : 146 B : 114	R : 153 G : 142 B : 114	R : 152 G : 140 B : 114	R : 152 G : 140 B : 114	R : 158 G : 147 B : 117	R : 149 G : 138 B : 108
R : 155 G : 145 B : 109	R : 150 G : 140 B : 104	R : 156 G : 148 B : 112	R : 152 G : 143 B : 112	R : 154 G : 145 B : 116	R : 151 G : 142 B : 113	R : 155 G : 149 B : 117	R : 147 G : 141 B : 109
R : 155 G : 145 B : 109	R : 151 G : 141 B : 105	R : 156 G : 148 B : 112	R : 152 G : 143 B : 112	R : 155 G : 146 B : 117	R : 152 G : 143 B : 114	R : 155 G : 149 B : 117	R : 151 G : 145 B : 113

R : 153	R : 151	R : 154	R : 151	R : 152	R : 151	R : 154	R : 155
G : 148	G : 146	G : 148	G : 145	G : 147	G : 146	G : 150	G : 151
B : 110	B : 108	B : 112	B : 113	B : 115	B : 117	B : 121	B : 122
R : 154	R : 154	R : 154	R : 153	R : 151	R : 152	R : 156	R : 160
G : 149	G : 149	G : 148	G : 147	G : 146	G : 147	G : 152	G : 156
B : 111	B : 111	B : 112	B : 115	B : 114	B : 118	B : 123	B : 127

The plaintext encryption process is calculated with the following key:
Key: TEHMANIS
To start the encryption process, the first step is to determine the number of rows and columns that will be used to load the plaintext. There are 64 tables or boxes in plaintext as a reference for forming rows, and there are 8 keys as a reference for forming columns. So the number of columns and rows needed is:
Key = 8 letters => 8 columns
Plaintext = 64 tables => 64/8 = 8 lines
So that the numbering can be given according to the initial letters of the alphabet, namely as follows:

Table 2: Key numbering process according to the first letter of the alphabet

T	E	H	M	A	N	I	S
8	2	3	5	1	6	4	7

After forming rows and columns, plaintext can be filled in sequentially and horizontally.

Table 3: Encryption Process

T	**E**	**H**	**M**	**A**	**N**	**I**	**S**
8	**2**	**3**	**5**	**1**	**6**	**4**	**7**
R : 153	R : 149	R : 146	R : 153	R : 133	R : 154	R : 162	R : 160
G : 140	G: 136	G : 132	G : 139	G : 119	G : 140	G : 148	G : 147
B : 106	B: 102	B : 102	B : 113	B : 93	B : 114	B : 121	B : 115
R : 156	R : 151	R : 150	R : 154	R : 139	R : 154	R : 162	R : 158
G : 143	G : 138	G : 136	G : 140	G : 125	G : 140	G : 148	G : 145
B : 109	B : 104	B : 107	B : 114	B : 99	B : 114	B : 121	B : 113
R : 158	R : 153	R : 153	R : 153	R : 145	R : 152	R : 159	R : 152
G : 145	G : 140	G : 142	G : 142	G : 133	G : 140	G : 148	G : 141
B : 111	B : 106	B : 110	B : 114	B : 107	B : 114	B : 118	B : 111
R : 159	R : 153	R : 157	R : 153	R : 152	R : 152	R : 158	R : 149
G : 146	G : 140	G : 146	G : 142	G : 140	G : 140	G : 147	G : 138
B : 112	B : 106	B : 114	B : 114	B : 114	B : 114	B : 117	B : 108
R : 155	R : 150	R : 156	R : 152	R : 154	R : 151	R : 155	R : 147
G : 145	G : 140	G : 148	G : 143	G : 145	G : 142	G : 149	G : 141
B : 109	B : 104	B : 112	B : 112	B : 116	B : 113	B : 117	B : 109
R : 155	R : 151	R : 156	R : 152	R : 155	R : 152	R : 155	R : 151
G : 145	G : 141	G : 148	G : 143	G : 146	G : 143	G : 149	G : 145
B : 109	B : 105	B : 112	B : 112	B : 117	B : 114	B : 117	B : 113
R : 153	R : 151	R : 154	R : 151	R : 152	R : 151	R : 154	R : 155
G : 148	G : 146	G : 148	G : 145	G : 147	G : 146	G : 150	G : 151
B : 110	B : 108	B : 112	B : 113	B : 115	B : 117	B : 121	B : 122
R : 154	R : 154	R : 154	R : 153	R : 151	R : 152	R : 156	R : 160
G : 149	G : 149	G : 148	G : 147	G : 146	G : 147	G : 152	G : 156
B : 111	B : 111	B : 112	B : 115	B : 114	B : 118	B : 123	B : 127

In the table above for the two rows above are the key and the number on the key used in the encryption process. So that in the encryption process the myszkowski algorithm produces ciphertext as shown in the table below.

Table 4: Myszkowski Ciphertext Algorithm

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
R : 133	R : 149	R : 146	R : 162	R : 153	R : 154	R : 160	R : 153
G : 119	G: 136	G : 132	G : 148	G : 139	G : 140	G : 147	G : 140
B : 93	B: 102	B : 102	B : 121	B : 113	B : 114	B : 115	B : 106
R : 139	R : 151	R : 150	R : 162	R : 154	R : 154	R : 158	R : 156
G : 125	G : 138	G : 136	G : 148	G : 140	G : 140	G : 145	G : 143
B : 99	B : 104	B : 107	B : 121	B : 114	B : 114	B : 113	B : 109
R : 145	R : 153	R : 153	R : 159	R : 153	R : 152	R : 152	R : 158
G : 133	G : 140	G : 142	G : 148	G : 142	G : 140	G : 141	G : 145
B : 107	B : 106	B : 110	B : 118	B : 114	B : 114	B : 111	B : 111
R : 152	R : 153	R : 157	R : 158	R : 153	R : 152	R : 149	R : 159
G : 140	G : 140	G : 146	G : 147	G : 142	G : 140	G : 138	G : 146
B : 114	B : 106	B : 114	B : 117	B : 114	B : 114	B : 108	B : 112
R : 154	R : 150	R : 156	R : 155	R : 152	R : 151	R : 147	R : 155
G : 145	G : 140	G : 148	G : 149	G : 143	G : 142	G : 141	G : 145
B : 116	B : 104	B : 112	B : 117	B : 112	B : 113	B : 109	B : 109
R : 155	R : 151	R : 156	R : 155	R : 152	R : 152	R : 151	R : 155
G : 146	G : 141	G : 148	G : 149	G : 143	G : 143	G : 145	G : 145

B : 117	B : 105	B : 112	B : 117	B : 112	B : 114	B : 113	B : 109
R : 152	R : 151	R : 154	R : 154	R : 151	R : 151	R : 155	R : 153
G : 147	G : 146	G : 148	G : 150	G : 145	G : 146	G : 151	G : 148
B : 115	B : 108	B : 112	B : 121	B : 113	B : 117	B : 122	B : 110
R : 151	R : 154	R : 154	R : 156	R : 153	R : 152	R : 160	R : 154
G : 146	G : 149	G : 148	G : 152	G : 147	G : 147	G : 156	G : 149
B : 114	B : 111	B : 112	B : 123	B : 115	B : 118	B : 127	B : 111

3.2. Calculation of the paillier crptosystem encryption algorithm

The key formation process formula using the paillier cryptosystem algorithm is as follows:

a. Choose two prime numbers p and q at random
   p = 11
   q = 17
b. Calculate the value of n and λ
   n = p *q
   n = 11 * 17
   n = 187
   λ = LCM(p – 1, q – 1)
   = LCM(11 – 1, 17 – 1)
   = LCM(10, 16)
   = 80
   LCM (10, 16)
   $10 = 2 * 5$ and $16 = 2^4$, so LCM = $2^4 * 5 = 80$
c. Choose a random integer g, where $g < n^2$
   g = 257
d. Calculate the value of $\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$, where the function L(x) = (x-1) / n.
   $(L(g^{\lambda} \bmod n^2))^{-1} \bmod n$
   $L(g^{\lambda} \bmod n^2) = L(257^{80} \bmod 187^2)$
   $= L(257^{60} \bmod 34969)$
   = L(14774)
   L(x) = (x-1) / n
   L(x) = (14774 – 1) /187
   L(x) = 79
   $\mu = 79^{-1} \bmod 187 = 116$
e. Public key (g, n) = (257, 187)
   Private key (λ, μ) = (80, 116)

Furthermore, the encryption process uses the paillier cryptosystem algorithm with plaintext as follows:
Plaintext :

Table 5: Plaintext

Pos Pixel	0	1	2	3	4	5	6	7
	R : 133	R : 149	R : 146	R : 162	R : 153	R : 154	R : 160	R : 153
0	G : 119	G: 136	G : 132	G : 148	G : 139	G : 140	G : 147	G : 140
	B : 93	B: 102	B : 102	B : 121	B : 113	B : 114	B : 115	B : 106
	R : 139	R : 151	R : 150	R : 162	R : 154	R : 154	R : 158	R : 156
1	G : 125	G : 138	G : 136	G : 148	G : 140	G : 140	G : 145	G : 143
	B : 99	B : 104	B : 107	B : 121	B : 114	B : 114	B : 113	B : 109
	R : 145	R : 153	R : 153	R : 159	R : 153	R : 152	R : 152	R : 158
2	G : 133	G : 140	G : 142	G : 148	G : 142	G : 140	G : 141	G : 145
	B : 107	B : 106	B : 110	B : 118	B : 114	B : 114	B : 111	B : 111
	R : 152	R : 153	R : 157	R : 158	R : 153	R : 152	R : 149	R : 159
3	G : 140	G : 140	G : 146	G : 147	G : 142	G : 140	G : 138	G : 146
	B : 114	B : 106	B : 114	B : 117	B : 114	B : 114	B : 108	B : 112
	R : 154	R : 150	R : 156	R : 155	R : 152	R : 151	R : 147	R : 155
4	G : 145	G : 140	G : 148	G : 149	G : 143	G : 142	G : 141	G : 145
	B : 116	B : 104	B : 112	B : 117	B : 112	B : 113	B : 109	B : 109
	R : 155	R : 151	R : 156	R : 155	R : 152	R : 152	R : 151	R : 155
5	G : 146	G : 141	G : 148	G : 149	G : 143	G : 143	G : 145	G : 145
	B : 117	B : 105	B : 112	B : 117	B : 112	B : 114	B : 113	B : 109
	R : 152	R : 151	R : 154	R : 154	R : 151	R : 151	R : 155	R : 153
6	G : 147	G : 146	G : 148	G : 150	G : 145	G : 146	G : 151	G : 148
	B : 115	B : 108	B : 112	B : 121	B : 113	B : 117	B : 122	B : 110
	R : 151	R : 154	R : 154	R : 156	R : 153	R : 152	R : 160	R : 154
7	G : 146	G : 149	G : 148	G : 152	G : 147	G : 147	G : 156	G : 149
	B : 114	B : 111	B : 112	B : 123	B : 115	B : 118	B : 127	B : 111

a. Enter a value for r, where r is taken from a random prime number.
   Suppose r = 71
b. Encrypyion formula
   $c = g^m * r^n \bmod n^2$

Pixel (0,0) =
Red= 257133 * 71187 * mod 1872
= 257133 * 71187 * mod 34969 = 10169
Green = 257119 * 71187 * mod 1872
= 257119 * 71187 * mod 34969 = 33944
Blue = 25793 * 71187 * mod 1872
= 25793 * 71187 * mod 34969 = 27747
Pixel (0,1) =
Red= 257149 * 71187 * mod 1872
= 257149 * 71187 * mod 34969 = 16663
Green = 257136 * 71187 * mod 1872
= 257136 * 71187 * mod 34969 = 28975
Blue = 257102 * 71187 * mod 1872
= 257102 * 71187 * mod 34969 = 12467
Pixel (0,2) =
Red= 257146 * 71187 * mod 1872
= 257146 * 71187 * mod 34969 = 33892
Green = 257132 * 71187 * mod 1872
= 257132 * 71187 * mod 34969 = 9156
Blue = 257102 * 71187 * mod 1872
= 257102 * 71187 * mod 34969 = 12467
Pixel (0,3) =
Red= 257162 * 71187 * mod 1872
= 257162 * 71187 * mod 34969 = 27262
Green = 257148 * 71187 * mod 1872
= 257148 * 71187 * mod 34969 = 27142
Blue = 257121 * 71187 * mod 1872
= 257121 * 71187 * mod 34969 = 34728
Pixel (0,4) =
Red= 257153 * 71187 * mod 1872
= 257153 * 71187 * mod 34969 = 13359
Green = 257139 * 71187 * mod 1872
= 257139 * 71187 * mod 34969 = 22020
Blue = 257113 * 71187 * mod 1872
= 257113 * 71187 * mod 34969 = 2139
Pixel (0,5) =
Red= 257154 * 71187 * mod 1872
= 257154 * 71187 * mod 34969 = 6301
Green = 257140 * 71187 * mod 1872
= 257140 * 71187 * mod 34969 = 29131
Blue = 257114 * 71187 * mod 1872
= 257114 * 71187 * mod 34969 = 25188
Pixel (0,6) =
Red = 257160 * 71187 * mod 1872
= 257160 * 71187 * mod 34969 = 25116
Green = 257147 * 71187 * mod 1872
= 257147 * 71187 * mod 34969 = 2963
Blue = 257115 * 71187 * mod 1872
= 257115 * 71187 * mod 34969 = 4051
Pixel (0,7) =
Red = 257153 * 71187 * mod 1872
= 257153 * 71187 * mod 34969 = 13359
Green = 257140 * 71187 * mod 1872
= 257140 * 71187 * mod 34969 = 29131
Blue = 257106 * 71187 * mod 1872
= 257106 * 71187 * mod 34969 = 33705

The calculation process will continue until the end of the pixel value (7.7), so that the results of the ciphertext in the paillier cryptosystem encryption process are known as follows:

Table 6: Paillier Cryptosystem Ciphertext Algorithm

Pos Pixel	0	1	2	3	4	5	6	7
0	R : 10169	R : 16663	R : 33892	R : 27262	R : 13359	R : 6301	R : 25116	R : 13359
	G : 33944	G : 28975	G : 9156	G : 27142	G : 22020	G : 29131	G : 2963	G : 29131
	B : 27747	B : 12467	B : 12467	B : 34728	B : 2139	B : 25188	B : 4051	B : 33705
1	R : 22020	R : 30119	R : 16173	R : 27262	R : 6301	R : 6301	R : 23534	R : 8680
	G : 32354	G : 21312	G : 28975	G : 27142	G : 29131	G : 29131	G : 2445	G : 31003
	B : 12109	B : 17840	B : 24842	B : 34728	B : 25188	B : 25188	B : 2139	B : 8809
2	R : 2445	R : 13359	R : 13359	R : 33570	R : 13359	R : 12434	R : 12434	R : 23534

	G : 10169	G : 29131	G : 9101	G : 27142	G : 9101	G : 29131	G : 3301	G : 2445
	B : 24842	B : 33705	B : 25897	B : 20542	B : 25188	B : 25188	B : 11419	B : 11419
3	R : 12434	R : 13359	R : 27713	R : 23534	R : 13359	R : 12434	R : 16663	R : 33570
	G : 29131	G : 29131	G : 33892	G : 2963	G : 9101	G : 29131	G :21312	G : 33892
	B : 25188	B : 33705	B : 25188	B : 16680	B : 25188	B : 25188	B : 20036	B : 32256
4	R : 6301	R : 16173	R : 8680	R : 10783	R : 12434	R : 30119	R : 2963	R : 10783
	G : 2445	G : 29131	G : 27142	G : 16663	G : 31003	G : 9101	G : 3301	G : 2445
	B : 27006	B : 17840	B : 32256	B : 16680	B : 32256	B : 2139	B : 8809	B : 8809
5	R : 10783	R : 30119	R : 8680	R : 10783	R : 12434	R : 12434	R : 30119	R : 10783
	G : 18139	G : 3301	G : 27142	G : 16663	G : 31003	G : 31003	G : 2445	G : 2445
	B : 16680	B : 3941	B : 32256	B : 16680	B : 32256	B : 25188	B : 2139	B : 8809
6	R : 12434	R : 30119	R : 6301	R : 6301	R : 30119	R : 30119	R : 10783	R : 13359
	G : 2963	G : 33892	G : 27142	G : 16173	G : 2445	G : 33892	G :30119	G : 27142
	B : 4051	B : 20036	B : 32256	B : 34728	B : 2139	B : 16680	B : 8001	B : 25897
7	R : 30119	R : 6301	R : 6301	R : 8680	R : 13359	R : 12434	R : 25116	R : 6301
	G : 33892	G : 16663	G : 27142	G : 12434	G : 2963	G : 2963	G : 8680	G : 16663
	B : 25188	B : 11419	B : 32256	B : 28055	B : 4051	B : 20542	B : 28725	B : 11419

3.3. Calculation of the paillier cryptosystem decryption algorithm

After obtaining the ciphertext from the paillier cryptosystem encryption process, the decryption process will then be carried out with plaintext as follows:

Table 7: Plaintext

Pos Pixel	0	1	2	3	4	5	6	7
0	R : 10169	R : 16663	R : 33892	R : 27262	R : 13359	R : 6301	R : 25116	R : 13359
	G : 33944	G : 28975	G : 9156	G : 27142	G : 22020	G : 29131	G : 2963	G : 29131
	B : 27747	B : 12467	B : 12467	B : 34728	B : 2139	B : 25188	B : 4051	B : 33705
1	R : 22020	R : 30119	R : 16173	R : 27262	R : 6301	R : 6301	R : 23534	R : 8680
	G : 32354	G : 21312	G : 28975	G : 27142	G : 29131	G : 29131	G : 2445	G : 31003
	B : 12109	B : 17840	B : 24842	B : 34728	B : 25188	B : 25188	B : 2139	B : 8809
2	R : 2445	R : 13359	R : 13359	R : 33570	R : 13359	R : 12434	R : 12434	R : 23534
	G : 10169	G : 29131	G : 9101	G : 27142	G : 9101	G : 29131	G : 3301	G : 2445
	B : 24842	B : 33705	B : 25897	B : 20542	B : 25188	B : 25188	B : 11419	B : 11419
3	R : 12434	R : 13359	R : 27713	R : 23534	R : 13359	R : 12434	R : 16663	R : 33570
	G : 29131	G : 29131	G : 33892	G : 2963	G : 9101	G : 29131	G :21312	G : 33892
	B : 25188	B : 33705	B : 25188	B : 16680	B : 25188	B : 25188	B : 20036	B : 32256
4	R : 6301	R : 16173	R : 8680	R : 10783	R : 12434	R : 30119	R : 2963	R : 10783
	G : 2445	G : 29131	G : 27142	G : 16663	G : 31003	G : 9101	G : 3301	G : 2445
	B : 27006	B : 17840	B : 32256	B : 16680	B : 32256	B : 2139	B : 8809	B : 8809
5	R : 10783	R : 30119	R : 8680	R : 10783	R : 12434	R : 12434	R : 30119	R : 10783
	G : 18139	G : 3301	G : 27142	G : 16663	G : 31003	G : 31003	G : 2445	G : 2445
	B : 16680	B : 3941	B : 32256	B : 16680	B : 32256	B : 25188	B : 2139	B : 8809
6	R : 12434	R : 30119	R : 6301	R : 6301	R : 30119	R : 30119	R : 10783	R : 13359
	G : 2963	G : 33892	G : 27142	G : 16173	G : 2445	G : 33892	G :30119	G : 27142
	B : 4051	B : 20036	B : 32256	B : 34728	B : 2139	B : 16680	B : 8001	B : 25897
7	R : 30119	R : 6301	R : 6301	R : 8680	R : 13359	R : 12434	R : 25116	R : 6301
	G : 33892	G : 16663	G : 27142	G : 12434	G : 2963	G : 2963	G : 8680	G : 16663
	B : 25188	B : 11419	B : 32256	B : 28055	B : 4051	B : 20542	B : 28725	B : 11419

Formula Description:
$m = L(c^{\lambda} \bmod n^2) * \mu \bmod n$
Pixel (0,0) =
Red = L(1016980 mod 1872) * 116 mod 187
= L(1016980 mod 34969) * 116 mod 187
= L(6546) * 116 mod 187
= (6546 – 1) / 187 * 116 mod 187
= 35 * 116 mod 187 = 133
Green = L(3394480 mod 1872) * 116 mod 187
= L(3394480 mod 34969) * 116 mod 187
= L(9538) * 116 mod 187
= (9538 – 1) / 187 * 116 mod 187
= 51 * 116 mod 187 = 119
Blue = L(2774780 mod 1872) * 116 mod 187
= L(2774780 mod 34969) * 116 mod 187
= L(10099) * 116 mod 187
= (10099 – 1) / 187 * 116 mod 187
= 54 * 116 mod 187 = 93

Pixel (0,1) =
Red = L(1666380 mod 1872) * 116 mod 187
= L(1666380 mod 34969) * 116 mod 187
= L(33100) * 116 mod 187
= (33100 – 1) / 187 * 116 mod 187
= 177 * 116 mod 187 = 149
Green = L(2897580 mod 1872) * 116 mod 187
= L(2897580 mod 34969) * 116 mod 187
= L(15896) * 116 mod 187
= (15896 – 1) / 187 * 116 mod 187
= 85 * 116 mod 187 = 136
Blue = L(1246780 mod 1872) * 116 mod 187
= L(1246780 mod 34969) * 116 mod 187
= L(3180) * 116 mod 187
= (3180 – 1) / 187 * 116 mod 187
= 17 * 116 mod 187 = 102
Pixel (0,2) =
Red = L(3389280 mod 1872) * 116 mod 187
= L(3389280 mod 34969) * 116 mod 187
= L(23750) * 116 mod 187
= (23750 – 1) / 187 * 116 mod 187
= 127 * 116 mod 187 = 146
Green = L(915680 mod 1872) * 116 mod 187
= L(915680 mod 34969) * 116 mod 187
= L(26742) * 116 mod 187
= (26742 – 1) / 187 * 116 mod 187
= 143 * 116 mod 187 = 132
Blue = L(1246780 mod 1872) * 116 mod 187
= L(1246780 mod 34969) * 116 mod 187
= L(3180) * 116 mod 187
= (3180 – 1) / 187 * 116 mod 187
= 17 * 116 mod 187 = 102
Pixel (0,3) =
Red = L(2726280 mod 1872) * 116 mod 187
= L(2726280 mod 34969) * 116 mod 187
= L(15335) * 116 mod 187
= (15335 – 1) / 187 * 116 mod 187
= 82 * 116 mod 187 = 162
Green = L(2714280 mod 1872) * 116 mod 187
= L(2714280 mod 34969) * 116 mod 187
= L(18327) * 116 mod 187
= (18327– 1) / 187 * 116 mod 187
= 98 * 116 mod 187 = 148
Blue = L(3472880 mod 1872) * 116 mod 187
= L(3472880 mod 34969) * 116 mod 187
= L(4115) * 116 mod 187
= (4115 – 1) / 187 * 116 mod 187
= 22 * 116 mod 187 = 121
Pixel (0,4) =
Red = L(1335980 mod 1872) * 116 mod 187
= L(1335980 mod 34969) * 116 mod 187
= L(22254) * 116 mod 187
= (22254– 1) / 187 * 116 mod 187
= 119 * 116 mod 187 = 153
Green = L(2202080 mod 1872) * 116 mod 187
= L(2202080 mod 34969) * 116 mod 187
= L(25246) * 116 mod 187
= (25246 – 1) / 187 * 116 mod 187
= 135 * 116 mod 187 = 139
Blue = L(213980 mod 1872) * 116 mod 187
= L(213980 mod 34969) * 116 mod 187
= L(25807) * 116 mod 187
= (25807 – 1) / 187 * 116 mod 187
= 138 * 116 mod 187 = 113
Pixel (0,5) =
Red = L(630180 mod 1872) * 116 mod 187
= L(630180 mod 34969) * 116 mod 187
= L(2058) * 116 mod 187
= (2058 – 1) / 187 * 116 mod 187
= 11 * 116 mod 187 = 154

Green = L(2913180 mod 1872) * 116 mod 187
= L(2913180 mod 34969) * 116 mod 187
= L(5050) * 116 mod 187
= (5050 – 1) / 187 * 116 mod 187
= 27 * 116 mod 187 = 140
Blue = L(2518880 mod 1872) * 116 mod 187
= L(2518880 mod 34969) * 116 mod 187
= L(5611) * 116 mod 187
= (5611– 1) / 187 * 116 mod 187
= 30 * 116 mod 187 = 114
Pixel (0,6) =
Red = L(2511680 mod 1872) * 116 mod 187
= L(2511680 mod 34969) * 116 mod 187
= L(20758) * 116 mod 187
= (20758 – 1) / 187 * 116 mod 187
= 111 * 116 mod 187 = 160
Green = L(296380 mod 1872) * 116 mod 187
= L(296380 mod 34969) * 116 mod 187
= L(3554) * 116 mod 187
= (3554 – 1) / 187 * 116 mod 187
= 19 * 116 mod 187 = 147
Blue = L(405180 mod 1872) * 116 mod 187
= L(405180 mod 34969) * 116 mod 187
= L(20384) * 116 mod 187
= (20384 – 1) / 187 * 116 mod 187
= 109 * 116 mod 187 = 115
Pixel (0,7) =
Red = L(1335980 mod 1872) * 116 mod 187
= L(1335980 mod 34969) * 116 mod 187
= L(22254) * 116 mod 187
= (22254– 1) / 187 * 116 mod 187
= 119 * 116 mod 187 = 153
Green = L(2913180 mod 1872) * 116 mod 187
= L(2913180 mod 34969) * 116 mod 187
= L(5050) * 116 mod 187
= (5050 – 1) / 187 * 116 mod 187
= 27 * 116 mod 187 = 140
Blue = L(3370580 mod 1872) * 116 mod 187
= L(3370580 mod 34969) * 116 mod 187
= L(27303) * 116 mod 187
= (27303 – 1) / 187 * 116 mod 187
= 146 * 116 mod 187 = 106

The calculation process will continue until the end of the pixel value (7.7), so that the results of the ciphertext in the paillier cryptosystem decryption process are known, namely as follows:

Table 8: Decryption Results of the Paillier Cryptosystem Algorithm

Pos Pixel	0	1	2	3	4	5	6	7
0	R : 133	R : 149	R : 146	R : 162	R : 153	R : 154	R : 160	R : 153
	G : 119	G: 136	G : 132	G : 148	G : 139	G : 140	G : 147	G : 140
	B : 93	B: 102	B : 102	B : 121	B : 113	B : 114	B : 115	B : 106
1	R : 139	R : 151	R : 150	R : 162	R : 154	R : 154	R : 158	R : 156
	G : 125	G : 138	G : 136	G : 148	G : 140	G : 140	G : 145	G : 143
	B : 99	B : 104	B : 107	B : 121	B : 114	B : 114	B : 113	B : 109
2	R : 145	R : 153	R : 153	R : 159	R : 153	R : 152	R : 152	R : 158
	G : 133	G : 140	G : 142	G : 148	G : 142	G : 140	G : 141	G : 145
	B : 107	B : 106	B : 110	B : 118	B : 114	B : 114	B : 111	B : 111
3	R : 152	R : 153	R : 157	R : 158	R : 153	R : 152	R : 149	R : 159
	G : 140	G : 140	G : 146	G : 147	G : 142	G : 140	G : 138	G : 146
	B : 114	B : 106	B : 114	B : 117	B : 114	B : 114	B : 108	B : 112
4	R : 154	R : 150	R : 156	R : 155	R : 152	R : 151	R : 147	R : 155
	G : 145	G : 140	G : 148	G : 149	G : 143	G : 142	G : 141	G : 145
	B : 116	B : 104	B : 112	B : 117	B : 112	B : 113	B : 109	B : 109
5	R : 155	R : 151	R : 156	R : 155	R : 152	R : 152	R : 151	R : 155
	G : 146	G : 141	G : 148	G : 149	G : 143	G : 143	G : 145	G : 145
	B : 117	B : 105	B : 112	B : 117	B : 112	B : 114	B : 113	B : 109
6	R : 152	R : 151	R : 154	R : 154	R : 151	R : 151	R : 155	R : 153
	G : 147	G : 146	G : 148	G : 150	G : 145	G : 146	G : 151	G : 148
	B : 115	B : 108	B : 112	B : 121	B : 113	B : 117	B : 122	B : 110

7	R : 151 G : 146 B : 114	R : 154 G : 149 B : 111	R : 154 G : 148 B : 112	R : 156 G : 152 B : 123	R : 153 G : 147 B : 115	R : 152 G : 147 B : 118	R : 160 G : 156 B : 127	R : 154 G : 149 B : 111

3.4. Myszkowski algorithm decryption calculation

Untuk melakukan proses dekripsi dengan algoritma Myszkowski dapat dilakukan dengan menuliskan ciphertext secara vertikal dari atas ke bawah secara berurutan sesuai dengan nomor kuncinya. Untuk penomoran kunci yang sama, ciphertext harus ditulis secara horizontal.
Key : TEHMANIS
Ciphertext :

Table 9: Ciphertext

Pos Pixel	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	R : 133 G : 119 B : 93	R : 149 G: 136 B: 102	R : 146 G : 132 B : 102	R : 162 G : 148 B : 121	R : 153 G : 139 B : 113	R : 154 G : 140 B : 114	R : 160 G : 147 B : 115	R : 153 G : 140 B : 106
1	R : 139 G : 125 B : 99	R : 151 G : 138 B : 104	R : 150 G : 136 B : 107	R : 162 G : 148 B : 121	R : 154 G : 140 B : 114	R : 154 G : 140 B : 114	R : 158 G : 145 B : 113	R : 156 G : 143 B : 109
2	R : 145 G : 133 B : 107	R : 153 G : 140 B : 106	R : 153 G : 142 B : 110	R : 159 G : 148 B : 118	R : 153 G : 142 B : 114	R : 152 G : 140 B : 114	R : 152 G : 141 B : 111	R : 158 G : 145 B : 111
3	R : 152 G : 140 B : 114	R : 153 G : 140 B : 106	R : 157 G : 146 B : 114	R : 158 G : 147 B : 117	R : 153 G : 142 B : 114	R : 152 G : 140 B : 114	R : 149 G : 138 B : 108	R : 159 G : 146 B : 112
4	R : 154 G : 145 B : 116	R : 150 G : 140 B : 104	R : 156 G : 148 B : 112	R : 155 G : 149 B : 117	R : 152 G : 143 B : 112	R : 151 G : 142 B : 113	R : 147 G : 141 B : 109	R : 155 G : 145 B : 109
5	R : 155 G : 146 B : 117	R : 151 G : 141 B : 105	R : 156 G : 148 B : 112	R : 155 G : 149 B : 117	R : 152 G : 143 B : 112	R : 152 G : 143 B : 114	R : 151 G : 145 B : 113	R : 155 G : 145 B : 109
6	R : 152 G : 147 B : 115	R : 151 G : 146 B : 108	R : 154 G : 148 B : 112	R : 154 G : 150 B : 121	R : 151 G : 145 B : 113	R : 151 G : 146 B : 117	R : 155 G : 151 B : 122	R : 153 G : 148 B : 110
7	R : 151 G : 146 B : 114	R : 154 G : 149 B : 111	R : 154 G : 148 B : 112	R : 156 G : 152 B : 123	R : 153 G : 147 B : 115	R : 152 G : 147 B : 118	R : 160 G : 156 B : 127	R : 154 G : 149 B : 111

Process description:

Table 10: First Decryption Process From Letter A

T	**E**	**H**	**M**	**A**	**N**	**I**	**S**
8	**2**	**3**	**5**	**1**	**6**	**4**	**7**
				R : 133 G : 119 B : 93 R : 139 G : 125 B : 99 R : 145 G : 133 B : 107 R : 152 G : 140 B : 114 R : 154 G : 145 B : 116 R : 155 G : 146 B : 117 R : 152 G : 147 B : 115 R : 151 G : 146 B : 114			

Table 11: Second Decryption Process From Letter E

T	**E**	**H**	**M**	**A**	**N**	**I**	**S**
8	**2**	**3**	**5**	**1**	**6**	**4**	**7**
	R : 149 G: 136			R : 133 G : 119			

B: 102	B : 93
R : 151	R : 139
G : 138	G : 125
B : 104	B : 99
R : 153	R : 145
G : 140	G : 133
B : 106	B : 107
R : 153	R : 152
G : 140	G : 140
B : 106	B : 114
R : 150	R : 154
G : 140	G : 145
B : 104	B : 116
R : 151	R : 155
G : 141	G : 146
B : 105	B : 117
R : 151	R : 152
G : 146	G : 147
B : 108	B : 115
R : 154	R : 151
G : 149	G : 146
B : 111	B : 114

The calculation process will continue until the end of the letter "T" so that the results of the ciphertext in the Myszkowski decryption process are known as follows:

Table 12: Decryption Results

T	**E**	**H**	**M**	**A**	**N**	**I**	**S**
8	**2**	**3**	**5**	**1**	**6**	**4**	**7**
R : 153	R : 149	R : 146	R : 153	R : 133	R : 154	R : 162	R : 160
G : 140	G: 136	G : 132	G : 139	G : 119	G : 140	G : 148	G : 147
B : 106	B: 102	B : 102	B : 113	B : 93	B : 114	B : 121	B : 115
R : 156	R : 151	R : 150	R : 154	R : 139	R : 154	R : 162	R : 158
G : 143	G : 138	G : 136	G : 140	G : 125	G : 140	G : 148	G : 145
B : 109	B : 104	B : 107	B : 114	B : 99	B : 114	B : 121	B : 113
R : 158	R : 153	R : 153	R : 153	R : 145	R : 152	R : 159	R : 152
G : 145	G : 140	G : 142	G : 142	G : 133	G : 140	G : 148	G : 141
B : 111	B : 106	B : 110	B : 114	B : 107	B : 114	B : 118	B : 111
R : 159	R : 153	R : 157	R : 153	R : 152	R : 152	R : 158	R : 149
G : 146	G : 140	G : 146	G : 142	G : 140	G : 140	G : 147	G : 138
B : 112	B : 106	B : 114	B : 114	B : 114	B : 114	B : 117	B : 108
R : 155	R : 150	R : 156	R : 152	R : 154	R : 151	R : 155	R : 147
G : 145	G : 140	G : 148	G : 143	G : 145	G : 142	G : 149	G : 141
B : 109	B : 104	B : 112	B : 112	B : 116	B : 113	B : 117	B : 109
R : 155	R : 151	R : 156	R : 152	R : 155	R : 152	R : 155	R : 151
G : 145	G : 141	G : 148	G : 143	G : 146	G : 143	G : 149	G : 145
B : 109	B : 105	B : 112	B : 112	B : 117	B : 114	B : 117	B : 113
R : 153	R : 151	R : 154	R : 151	R : 152	R : 151	R : 154	R : 155
G : 148	G : 146	G : 148	G : 145	G : 147	G : 146	G : 150	G : 151
B : 110	B : 108	B : 112	B : 113	B : 115	B : 117	B : 121	B : 122
R : 154	R : 154	R : 154	R : 153	R : 151	R : 152	R : 156	R : 160
G : 149	G : 149	G : 148	G : 147	G : 146	G : 147	G : 152	G : 156
B : 111	B : 111	B : 112	B : 115	B : 114	B : 118	B : 123	B : 127

4. Discussion

This design will discuss several existing menu views such as the design of the main form, the design of the encryption form and the design of the decryption form.

4.1. Main form design

Here is the main form design:

Figure 2: Main Shape

4.2. Encryption form design and decryption form design

In the design form, the encryption form and the decryption form are display forms that are designed as meeting points so that users can interact with the system. Here is the form design for the encryption form and decryption form:

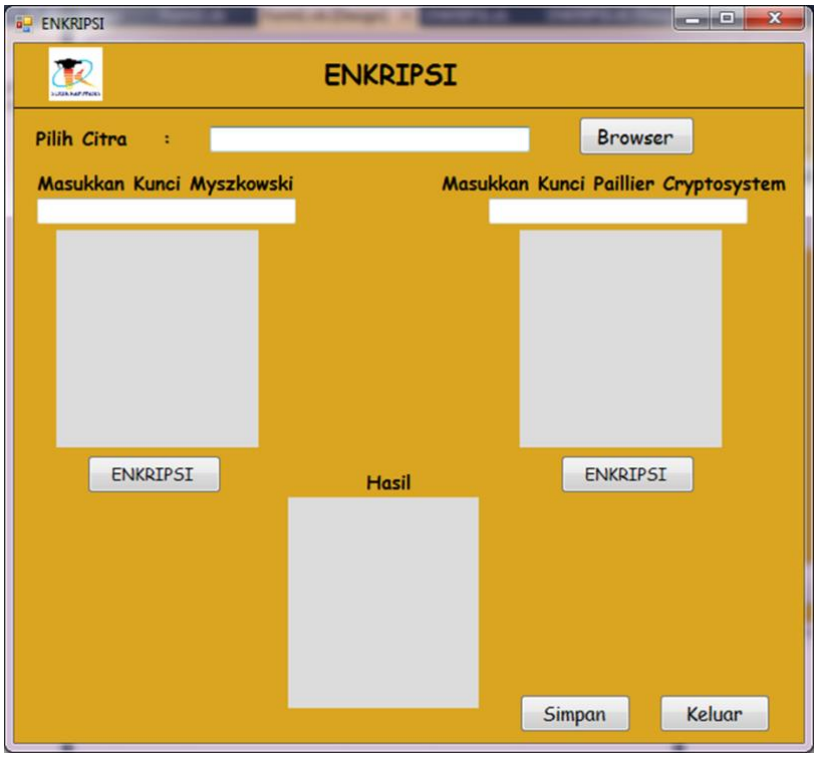

Figure 3: Form of encryption

In Figure 3 is the design on the encryption form page, on this page the image encryption process can be carried out using the Myszkowski key algorithm and the Paillier Cryptosystem algorithm.

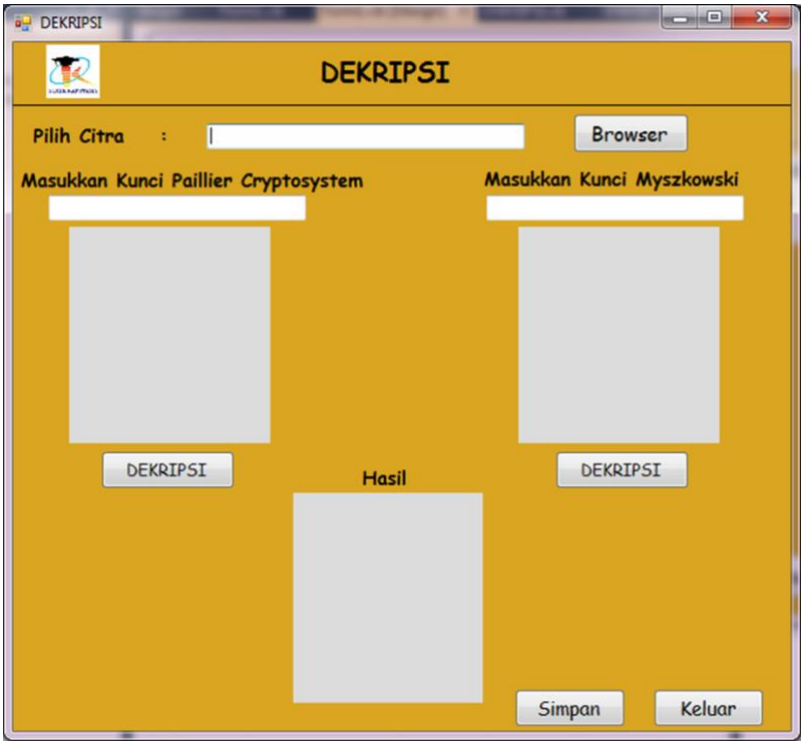

Figure 4: Form description

In Figure 4 is the design for the Decryption form, on this page you can perform the image decryption process with the Paillier Cryptosystem algorithm key and the Myszkowski algorithm so that the image will return to its original state.

5. Conclusion

In this study a super encryption technique has been used which combines the Myszkowski Algorithm and the Paillier Cryptosystem Algorithm to increase the level of security of digital images so that it can be concluded as follows:

1. Myszkowski's algorithm is an efficient method of scrambling text. This algorithm is used as a first step in performing super encryption techniques to encrypt digital images. The encryption process with the Myszkowski Algorithm is carried out by randomizing the order of the image pixels based on the secret key. This scrambling technique aims to hide patterns or structures in digital images, making it difficult for unauthorized parties to restore the original image.
2. The Paillier Cryptosystem algorithm is an asymmetric cryptographic algorithm that is used as the second step in performing super encryption techniques. This algorithm has the ability to perform mathematical operations on encrypted data, without the need to decrypt it first. This enables encrypted data processing, such as performing computations or statistical analysis, without compromising data security. Paillier Cryptosystem's algorithm is also resistant to key recovery and other cryptanalysis attacks, making it a good choice for securing digital images.

References

[1] Dony Ariyus, *Pengantar Ilmu Kriptografi*. 2008.
[2] Rinaldi Munir, *Kriptografi*, Kedua. Bandung: Informatika Bandung, 2019.
[3] S. Murdowo, "Mengenal Kriptografi Modern Sederhana Menggunakan Electronik Code Book (Ecb)," *Infokam*, no. 2006, pp. 29–37, 2019, [Online]. Available: http://amikjtc.com/jurnal/index.php/jurnal/article/view/166
[4] S. M. Hardi, D. Rachmawati, F. Chairinnisa, I. Jaya, and J. T. Tarigan, "Combination of myszkowski transposition algorithm and modified least significant bit (mlsb) green channel on png image security," *J. Phys. Conf. Ser.*, vol. 1235, no. 1, 2019, doi: 10.1088/1742-6596/1235/1/012080.
[5] Yazirwan, "Perancangan Aplikasi Pengamanan File Menggunakan Algoritma Paillier Berbasis Android," vol. 2, pp. 137–140, 2021, doi: 10.30865/json.v2i2.2625.
[6] S. Ratna, "Pengolahan Citra Digital Dan Histogram Dengan Phyton Dan Text Editor Phycharm," *Technol. J. Ilm.*, vol. 11, no. 3, p. 181, 2020, doi: 10.31602/tji.v11i3.3294.
[7] D. Putra, *Pengolahan Citra Digital*. 2010.