Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th October 2024. Vol. 4. No. 1; e-ISSN: 2808-4519

Super Encryption of Rabin Cryptosystem Algorithm and Paillier Cryptosystem Algorithm on Digital Image Security Process

Dika Ramanda[1]*, Achmad Fauzi[2], Victor Maruli Pakpahan[3]

[1,2,3] *STMIK Kaputama*

dikaramanda2045@gmail.com[1], fauzyrivai88@gmail.com[2], victor.pakpahan@gmail.com[3]*

Abstract

Technological advances have given rise to the need for data protection, especially digital images, which are vulnerable to misuse. This research proposes a super encryption method that combines two cryptographic algorithms, namely Rabin Cryptosystem and Paillier Cryptosystem, to increase digital image security. Rabin's algorithm does not have homomorphism, so it is vulnerable to factorization attacks if the prime numbers used are too small. Meanwhile, the Paillier algorithm has homomorphism properties which allow arithmetic operations to be carried out directly on the ciphertext without decryption. By combining these two algorithms, this research aims to create a stronger and more efficient encryption method, and analyze its performance in terms of computational efficiency and complexity. It is hoped that the research results can improve the security and privacy of digital data, especially in the context of digital images.

Keywords: *Digital Image, Super Encryption, Rabin Cryptosystem Algorithm, Paillier Cryptosystem Algorithm.*

1. Introduction

The rapid advancement of technology has provided many benefits for humans in various fields of life, ranging from basic needs to lifestyle improvements. Digital images contain important and sensitive information such as personal photos, confidential documents and so on. The wider the use of digital images, the more vulnerable they are to attacks such as data retrieval and manipulation. Hence the importance of additional protection.

One way to maintain the security of digital image confidentiality is to use super encryption techniques which are a combination of two or more encryption techniques. The algorithms used are the Rabin Cryptosystem algorithm and the Paillier Cryptosystem algorithm. Rabin Cryptosystem is an algorithm that does not have homomorphism properties, which means that arithmetic operations cannot be performed directly on the ciphertext without decrypting it first. Meanwhile, the Paillier Cryptosystem has a homomorphism property that makes it possible to perform arithmetic operations on the ciphertext without the need to decrypt it first.

2. Research methodology

2.1. Cryptography

Cryptography is the science of keeping messages secret and there are two processes: encryption and decryption. The encrypted message is called plaintext. It is called this because this information can be easily read and understood by anyone [1].

2.2. Modern Algorithms

Modern cryptography is a complex algorithm that is operated using computers. These algorithms have a level of difficulty that makes it very difficult for cryptanalysts to crack ciphertexts without knowing the key [2].

2.3. Rabin Cryptosystem Algorithm

Rabin is often known as a variation of RSA in an attempt to improve the speed of RSA encryption. Rabin is basically RSA with an optimized choice of public key exponent (e), where encryption uses an integer of two as the public key exponent, which requires less computation time for encryption. This feature makes the Rabin cryptosystem relatively faster in encryption than Standard RSA. The Rabin

algorithm uses two keys like RSA. Here, the public key is the common modulus (n), and the private key is the prime factor used to calculate n. Using the Rabin cryptosystem, retrieving the plaintext from the encrypted text is considered to be as difficult as factoring the [3].

Randomly select two prime numbers p and q
p = 131
q = 151

1. Calculate the value of n.

n = p * q
n = 131 * 151 = 19781

2. Calculate Yp and Yq values

FPB (131, 151) :
151 = 1131 + 20
131 = 6.20 + 11
20 = 1.11 + 9
11 = 1.9 + 2
9 = 4.2 + 1
2 = 2.1 + 0
So that it can be stated that GCD (131, 151) = 1. Then to express 1 as a linear combination of 131 and 151, the Extended Euclidean algorithm (back substitution of Euclid's algorithm) is needed as follows.
1 = 9 - 4.2
1 = 9 - 4(11-1.9)
1 = 5.9 - 4.11
1 = 5 (20 - 1.11) - 4.11
1 = 5.20 - 9.11
1 = 5.20 - 9(131 - 6.20)
1 = 59.20 - 9.131
1= 59(151 - 1.131) - 9.131
1 = -68.131 + 59.151
Obtained Yp = -68 and Yq = 59

2.4. Paillier Cryptosystem Algorithm

The algorithm developed by Pascal Paillier in 1999 is a probability asymmetric algorithm for public key cryptography. The security of this algorithm is based on the difficulty in solving the nth residue problem. Paillier's cryptosystem algorithm consists of procedures for generating public and private keys, encryption, and decryption procedures [4].

Private key formation process:

1. Choose two prime numbers at random p and q
2. Calculate the value n = p * q and λ = 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: $c = g^m * r^n \bmod n^2$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
      randomp = 11
      q = 13
   b. Calculate the value of n
      and λn = p *q
      n = 11 * 13
      n = 143
      λ = 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

$< n^2g = 326$

d. Calculate the value of $\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$, where the function $L(x) = (x-1) / n.(L(g^{\lambda} \bmod n^2))^{-1} \bmod n$
$L(g^{\lambda} \bmod n^2) = L(257^{60} \bmod 143^2)$
$= L(257^{60} \bmod 20449)$
$= L(10869)$
$L(x) = (x-1) / n$
$L(x) = (10869 – 1) /143$
$L(x) = 76$
$\mu = 76^{-1} \bmod 143 = 32$

e. Public key (g, n) = (257, 143)
f. Private key (λ, μ) = (60, 32)

2.5. Image Definition

A digital image is a two-dimensional image that is generated from a continuous two-dimensional analog image through a sampling process. The analog image is divided into N rows and M columns so that it becomes a discrete image. Digital image is an image that can be processed by a computer. What is stored in the computer are only numbers that indicate the amount of intensity at each pixel. Because it is in the form of numerical data, digital images can be processed with a computer [5], [6], [7], [8].

3. Result

3.1. Calculation of The Rabin Cryptosystem Encryption Algorithn

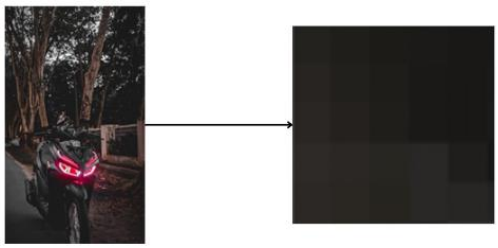

Fig. 1: Example Image and 5x5 Pixel Image Pixels

This process aims to secure the image. The process of securing this digital image will be sampled in an image with a size of 5 x 5 pixels and pixels converted to RGB values using an additional application, namely Photoshop, which will start from pixel point (0,0) to (4,4).

Table 1: 8x8 Pixel Sample

(x,y)	0	1	2	3	4
0	R = 36 G = 35 B = 31	R = 32 G = 31 B = 27	R = 29 G = 28 B = 24	R = 28 G = 28 B = 24	R = 26 G = 25 B = 23
1	R = 41 G = 37 B = 34	R = 34 G = 33 B = 29	R = 32 G = 30 B = 26	R = 27 G = 26 B = 24	R = 26 G = 25 B = 23
2	R = 43 G = 39 B = 36	R = 38 G = 34 B = 31	R = 32 G = 31 B = 27	R = 27 G = 26 B = 24	R = 26 G = 25 B = 23
3	R = 47 G = 43 B = 40	R = 44 G = 40 B = 37	R = 40 G = 39 B = 34	R = 41 G = 40 B = 38	R = 32 G = 31 B = 29
4	R = 45 G = 41 B = 38	R = 43 G = 40 B = 35	R = 40 G = 37 B = 32	R = 41 G = 40 B = 38	R = 40 G = 39 B = 37

1. Choose two prime numbers p and q at random
   p = 127 q = 191
2. Calculate the value of n.
   n = p * q
   n = 127 * 191 = 24257
3. Calculate Yp and Yq values
   FPB(127, 191) :
   191 = 1.127 + 64
   127 = 1.64 + 63
   64 = 1.63 + 1

63 = 63.1 +0
So it can be stated that GCD (127, 191) = 1. Then to express 1 as a linear combination of 127 and 191, the Extended Euclidean algorithm (back substitution of Euclid's algorithm) is needed as follows.
1 = 64 - 1.63
1 = 64 - 1(127 - 1.64)
1 = 2.64 - 1.127
1 = 2(191 - 1.127) - 1.127
1 = -3.127 + 2.191
Obtained Yp = -3 and Yq = 2

Encryption formula = $c = (m^2) \bmod n$

Pixel (0,0) :
Red = $36^2 \bmod 24257 = 1296$
Green = $35^2 \bmod 24257 = 1225$
Blue = $31^2 \bmod 24257 = 961$
Pixel (0,1) :
Red = $32^2 \bmod 24257 = 1024$
Green = $31^2 \bmod 24257 = 961$
Blue = $27^2 \bmod 24257 = 729$
Pixel (0,2) :
Red = $28^2 \bmod 24257 = 784$
Green = $27^2 \bmod 24257 = 729$
Blue = $25^2 \bmod 24257 = 625$
Pixel (0,3) :
Red = $28^2 \bmod 24257 = 784$
Green = $27^2 \bmod 24257 = 729$
Blue = $25^2 \bmod 24257 = 625$
Pixel (0,4) :
Red = $26^2 \bmod 24257 = 676$
Green = $25^2 \bmod 24257 = 625$
Blue = $23^2 \bmod 24257 = 529$

The calculation process will continue until the end of the pixel value (4,4), so that the results of the ciphertext in the rabin cryptosystem encryption process are known as follows:

Table 2: Rabin Cryptosystem Ciphertext Algorithm

(x,y)	0	1	2	3	4
0	R = 1296 G = 1225 B = 961	R = 1024 G = 961 B =729	R = 841 G = 784 B = 576	R = 784 G = 729 B = 625	R = 676 G = 625 B = 529
1	R = 1681 G = 1369 B = 1156	R = 1156 G = 1089 B = 841	R = 961 G = 900 B = 676	R = 729 G = 676 B = 576	R = 676 G = 625 B = 529
2	R = 1849 G = 1521 B = 1296	R = 1444 G = 1156 B = 961	R = 1024 G = 961 B = 729	R = 729 G = 676 B = 576	R = 676 G = 625 B = 529
3	R = 2209 G = 1849 B = 1600	R = 1936 G = 1600 B = 1369	R = 1600 G = 1521 B = 1156	R = 1681 G = 1600 B = 1444	R = 1024 G = 961 B = 841
4	R = 2025 G = 1681 B = 1444	R = 1849 G = 1600 B = 1225	R = 1600 G = 1369 B = 1024	R = 1681 G = 1600 B = 1444	R = 1600 G = 1521 B = 1369

3.2. Calculation Of The Paillier Crptosystem Encryption Algorithm

1. Randomly select two prime numbers p and q
   p = 29
   q = 89
2. Calculate the value of n and λ
   n = p*q
   n = 29 * 89
   n = 2581

   λ = KPK (p-1, q-1)
   = KPK (29-1, 89-1)
   = KPK (28, 88)
   = 161

3. Choose a random integer g, where g < n2
   g = 2582
4. Calculate the value of μ = (L(gλ mod n2))-1 mod n, with function L(x) = (x-1) / n.
   (L(gλ mod n2))-1 mod n
   (L(gλ mod n2)) = L(2582616 mod 25812)
   = L(1589897)
   L(x) = (x-1) / n
   L(x) = (1589897 - 1) / 2581
   L(x) = 616
   μ = 616-1 mod 2581 = 750
5. Public Key (g, n) = (2582, 2581)
6. Private Key (λ, μ) = (616, 750)
   r = 5

Table 3: Plaintext

(x,y)	0	1	2	3	4
0	R = 1296 G = 1225 B = 961	R = 1024 G = 961 B =729	R = 841 G = 784 B = 576	R = 784 G = 729 B = 625	R = 676 G = 625 B = 529
1	R = 1681 G = 1369 B = 1156	R = 1156 G = 1089 B = 841	R = 961 G = 900 B = 676	R = 729 G = 676 B = 576	R = 676 G = 625 B = 529
2	R = 1849 G = 1521 B = 1296	R = 1444 G = 1156 B = 961	R = 1024 G = 961 B = 729	R = 729 G = 676 B = 576	R = 676 G = 625 B = 529
3	R = 2209 G = 1849 B = 1600	R = 1936 G = 1600 B = 1369	R = 1600 G = 1521 B = 1156	R = 1681 G = 1600 B = 1444	R = 1024 G = 961 B = 841
4	R = 2025 G = 1681 B = 1444	R = 1849 G = 1600 B = 1225	R = 1600 G = 1369 B = 1024	R = 1681 G = 1600 B = 1444	R = 1600 G = 1521 B = 1369

Encryption formula = $c = g^m * r^n \bmod n^2$

Pixel (0,0) :
Red = $2582^{1296} * 5^{2581} * \bmod 2581^2 = 1826297$
Green = $2582^{1225} * 5^{2581} * \bmod 2581^2 = 1237829$
Blue = $2582^{961} * 53^{2581} * \bmod 2581^2 = 4585386$
Pixel (0,1) :
Red = $2582^{1024} * 5^{2581} * \bmod 2581^2 = 228658$
Green = $2582^{961} * 5^{2581} * \bmod 2581^2 = 4585386$
Blue = $2582^{729} * 53^{2581} * \bmod 2581^2 = 1067483$
Pixel (0,2) :
Red = $2582^{841} * 5^{2581} * \bmod 2581^2 = 3684617$
Green = $2582^{784} * 5^{2581} * \bmod 2581^2 = 5088681$
Blue = $2582^{576} * 53^{2581} * \bmod 2581^2 = 3083244$
Pixel (0,3) :
Red = $2582^{784} * 5^{2581} * \bmod 2581^2 = 5088681$
Green = $2582^{729} * 5^{2581} * \bmod 2581^2 = 1067483$
Blue = $2582^{625} * 53^{2581} * \bmod 2581^2 = 3395545$
Pixel (0,4) :
Red = $2582^{676} * 5^{2581} * \bmod 2581^2 = 4944145$
Green = $2582^{625} * 5^{2581} * \bmod 2581^2 = 3395545$
Blue = $2582^{529} * 53^{2581} * \bmod 2581^2 = 4007242$

The calculation process will continue until the end of the pixel value (4,4), so that the results of the ciphertext in the Paillier cryptosystem encryption process are known as follows:

Table 4: Paillier Cryptosystem Ciphertext Algorithm

(x,y)	0	1	2	3	4
0	R = 1826297 G = 1237829 B = 4585386	R = 228658 G = 4585386 B = 1067483	R = 3684617 G = 5088681 B = 3083244	R = 5088681 G = 1067483 B = 3395545	R = 4944145 G = 3395545 B = 4007242
1	R = 3328439 G = 3651064 B = 1885660	R = 1885660 G = 3769790 B = 3684617	R = 4585386 G = 3516852 B = 4944145	R = 1067483 G = 4944145 B = 3083244	R = 4944145 G = 3395545 B = 4007242
2	R = 592579 G = 4347934 B = 1826297	R = 50569 G = 1885660 B = 4585386	R = 228658 G = 4584386 B = 1067483	R = 1067483 G = 4944145 B = 3083244	R = 4944145 G = 3395545 B = 4007242
3	R = 3294886	R = 4409878	R = 3220037	R = 3328439	R = 228658

	G = 592579 B = 3220037	G = 3220037 B = 3651064	G = 4347934 B = 1885660	G = 3220037 B = 50569	G = 4585386 B = 3684617
4	R = 2801915 G = 3328439 B = 50569	R = 592579 G = 3220037 B = 1237829	R = 3220037 G = 3651064 B = 228658	R = 3328439 G = 3220037 B = 50569	R = 3220037 G = 4347934 B = 3651064

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 5: Ciphertext

(x,y)	0	1	2	3	4
0	R = 1826297 G = 1237829 B = 4585386	R = 228658 G = 4585386 B = 1067483	R = 3684617 G = 5088681 B = 3083244	R = 5088681 G = 1067483 B = 3395545	R = 4944145 G = 3395545 B = 4007242
1	R = 3328439 G = 3651064 B = 1885660	R = 1885660 G = 3769790 B = 3684617	R = 4585386 G = 3516852 B = 4944145	R = 1067483 G = 4944145 B = 3083244	R = 4944145 G = 3395545 B = 4007242
2	R = 592579 G = 4347934 B = 1826297	R = 50569 G = 1885660 B = 4585386	R = 228658 G = 4584386 B = 1067483	R = 1067483 G = 4944145 B = 3083244	R = 4944145 G = 3395545 B = 4007242
3	R = 3294886 G = 592579 B = 3220037	R = 4409878 G = 3220037 B = 3651064	R = 3220037 G = 4347934 B = 1885660	R = 3328439 G = 3220037 B = 50569	R = 228658 G = 4585386 B = 3684617
4	R = 2801915 G = 3328439 B = 50569	R = 592579 G = 3220037 B = 1237829	R = 3220037 G = 3651064 B = 228658	R = 3328439 G = 3220037 B = 50569	R = 3220037 G = 4347934 B = 3651064

Decryption formula = $L(c^{\lambda} \bmod n^2) * \mu \bmod n$

Pixel (0,0) :

Red = $L(1826297^{616} \bmod 2581^2) * 750 \bmod 2581$
= (2082868 - 1) / 2581 * 750 mod 2581 = 1296

Green = $L(1237829^{616} \bmod 2581^2) * 750 \bmod 2581$
= (2446789 - 1) / 2581 * 750 mod 2581 = 1225

Blue = $L(4585386^{616} \bmod 2581^2) * 750 \bmod 2581$
= (2392588 - 1) / 2581 * 750 mod 2581 = 961

Pixel (0,1) :

Red = $L(228658^{616} \bmod 2581^2) * 750 \bmod 2581$
= (2632621 - 1) / 2581 * 750 mod 2581 = 1024

Green = $L(4585386^{616} \bmod 2581^2) * 750 \bmod 2581$
= (2392588 - 1) / 2581 * 750 mod 2581 = 961

Blue = $L(1067483^{616} \bmod 2581^2) * 750 \bmod 2581$
= (- 1) / 2581 * 750 mod 2581 = 729

Pixel (0,2) :

Red = $L(3684617^{616} \bmod 2581^2) * 750 \bmod 2581$
= (4790337 - 1) / 2581 * 750 mod 2581 = 841

Green = $L(5088681^{616} \bmod 2581^2) * 750 \bmod 2581$
= (766558 - 1) / 2581 * 750 mod 2581 = 784

Blue = $L(3083244^{616} \bmod 2581^2) * 750 \bmod 2581$
= (3146240 - 1) / 2581 * 750 mod 2581 = 576

Pixel (0,3) :

Red = $L(5088681^{616} \bmod 2581^2) * 750 \bmod 2581$
= (766558 - 1) / 2581 * 750 mod 2581 = 784

Green = $L(1067483^{616} \bmod 2581^2) * 750 \bmod 2581$
= (1067483 - 1) / 2581 * 750 mod 2581 = 729

Blue = $L(3395545^{616} \bmod 2581^2) * 750 \bmod 2581$
= (1112412 - 1) / 2581 * 750 mod 2581 = 625

Pixel (0,4) :

Red = $L(4944145^{616} \bmod 2581^2) * 750 \bmod 2581$
= (2258376 - 1) / 2581 * 750 mod 2581 = 676

Green = $L(3395545^{616} \bmod 2581^2) * 750 \bmod 2581$
= (1112412 - 1) / 2581 * 750 mod 2581 = 625

Blue = $L(4007242^{616} \bmod 2581^2) * 750 \bmod 2581$
= (1698299 - 1) / 2581 * 750 mod 2581 = 529

The calculation process will continue until the end of the pixel value (4,4), so that the results of the ciphertext in the Paillier cryptosystem decryption process are known as follows:

Table 6: Decryption Results of the Paillier Cryptosystem Algorithm

(x,y)	0	1	2	3	4
0	R = 1296 G = 1225 B = 961	R = 1024 G = 961 B =729	R = 841 G = 784 B = 576	R = 784 G = 729 B = 625	R = 676 G = 625 B = 529
1	R = 1681 G = 1369 B = 1156	R = 1156 G = 1089 B = 841	R = 961 G = 900 B = 676	R = 729 G = 676 B = 576	R = 676 G = 625 B = 529
2	R = 1849 G = 1521 B = 1296	R = 1444 G = 1156 B = 961	R = 1024 G = 961 B = 729	R = 729 G = 676 B = 576	R = 676 G = 625 B = 529
3	R = 2209 G = 1849 B = 1600	R = 1936 G = 1600 B = 1369	R = 1600 G = 1521 B = 1156	R = 1681 G = 1600 B = 1444	R = 1024 G = 961 B = 841
4	R = 2025 G = 1681 B = 1444	R = 1849 G = 1600 B = 1225	R = 1600 G = 1369 B = 1024	R = 1681 G = 1600 B = 1444	R = 1600 G = 1521 B = 1369

3.4. Calculation of The Rabin Cryptosystem Decryption Algorithm

Table 7: Ciphertext

(x,y)	0	1	2	3	4
0	R = 1296 G = 1225 B = 961	R = 1024 G = 961 B =729	R = 841 G = 784 B = 576	R = 784 G = 729 B = 625	R = 676 G = 625 B = 529
1	R = 1681 G = 1369 B = 1156	R = 1156 G = 1089 B = 841	R = 961 G = 900 B = 676	R = 729 G = 676 B = 576	R = 676 G = 625 B = 529
2	R = 1849 G = 1521 B = 1296	R = 1444 G = 1156 B = 961	R = 1024 G = 961 B = 729	R = 729 G = 676 B = 576	R = 676 G = 625 B = 529
3	R = 2209 G = 1849 B = 1600	R = 1936 G = 1600 B = 1369	R = 1600 G = 1521 B = 1156	R = 1681 G = 1600 B = 1444	R = 1024 G = 961 B = 841
4	R = 2025 G = 1681 B = 1444	R = 1849 G = 1600 B = 1225	R = 1600 G = 1369 B = 1024	R = 1681 G = 1600 B = 1444	R = 1600 G = 1521 B = 1369

Decryption formula = $m_p = (c^{\left(\frac{p+1}{4}\right)} \ mod \ p$

$m_q = (c^{\left(\frac{p+1}{4}\right)} \ mod \ q$

Pixel (0,0) :

Red $= m_{p1} = (1296^{\left(\frac{127+1}{4}\right)} \bmod 127 = 36$

$m_{q1} = (1296^{\left(\frac{191+1}{4}\right)} \bmod 191 = 36$

Green $= m_{p2} = (1225^{\left(\frac{127+1}{4}\right)} \bmod 127 = 35$

$m_{q2} = (1225^{\left(\frac{191+1}{4}\right)} \bmod 191 = 156$

Blue $= m_{p3} = (961^{\left(\frac{127+1}{4}\right)} \bmod 127 = 31$

$m_{q3} = (961^{\left(\frac{191+1}{4}\right)} \bmod 191 = 160$

Pixel (0,1) :

Red $= m_{p1} = (1024^{\left(\frac{127+1}{4}\right)} \bmod 127 = 32$

$m_{q1} = (1024^{\left(\frac{191+1}{4}\right)} \bmod 191 = 32$

Green $= m_{p2} = (961^{\left(\frac{127+1}{4}\right)} \bmod 127 = 31$

$m_{q2} = (961^{\left(\frac{191+1}{4}\right)} \bmod 191 = 160$

Blue $= m_{p3} = (729^{\left(\frac{127+1}{4}\right)} \bmod 127 = 100$

$m_{q3} = (729^{\left(\frac{191+1}{4}\right)} \bmod 191 = 27$

Pixel (0,2) :

Red $= m_{p1} = (841^{\left(\frac{127+1}{4}\right)} \bmod 127 = 98$

$m_{q1} = (841^{\left(\frac{191+1}{4}\right)} \bmod 191 = 162$

Green $= m_{p2} = (784^{\left(\frac{127+1}{4}\right)} \bmod 127 = 99$

$m_{q2} = (784^{\left(\frac{191+1}{4}\right)} \bmod 191 = 163$

Blue $= m_{p3} = (576^{\left(\frac{127+1}{4}\right)} \bmod 127 = 103$

$m_{q3} = (576^{\left(\frac{191+1}{4}\right)} \bmod 191 = 24$

Pixel (0,3) :

Red $= m_{p1} = (784^{\left(\frac{127+1}{4}\right)} \bmod 127 = 99$

$m_{q1} = (784^{\left(\frac{191+1}{4}\right)} \bmod 191 = 163$

Green $= m_{p2} = (729^{\left(\frac{127+1}{4}\right)} \bmod 127 = 100$

$m_{q2} = (729^{\left(\frac{191+1}{4}\right)} \bmod 191 = 27$

Blue $= m_{p3} = (625^{\left(\frac{127+1}{4}\right)} \bmod 127 = 25$

$m_{q3} = (625^{\left(\frac{191+1}{4}\right)} \bmod 191 = 25$

Pixel (0,4) :

Red $= m_{p1} = (676^{\left(\frac{127+1}{4}\right)} \bmod 127 = 26$

$m_{q1} = (676^{\left(\frac{191+1}{4}\right)} \bmod 191 = 26$

Green $= m_{p2} = (625^{\left(\frac{127+1}{4}\right)} \bmod 127 = 25$

$m_{q2} = (625^{\left(\frac{191+1}{4}\right)} \bmod 191 = 25$

Blue $= m_{p3} = (529^{\left(\frac{127+1}{4}\right)} \bmod 127 = 104$

$m_{q3} = (529^{\left(\frac{191+1}{4}\right)} \bmod 191 = 23$

The calculation process will continue until the end of the pixel value (4,4), next is to calculate the value using the Chinese Remainder Theorem with the following equation:

Formula = $v_1 = Y_p * p * m_{q1}$

$w_1 = Y_q * q * m_{p1}$

Pixel (0,0) :

Red $= v_1 = (-3) . 127 . 36 = -13716$

$w_1 = 2 . 191 . 36 = 13752$

Green $= v1 = (-3) . 127 . 156 = -59436$

$w1 = 2 . 191 . 35 = 13370$

Blue $= v1 = (-3) . 127 . 160 = -60960$

$w_1 = 2 . 191 . 31 = 11842$

Pixel (0,1) :

Red $= v_1 = (-3) . 127 . 3 = -12192$

$w_1 = 2 . 191 . 3 = 12224$

Green $= v_1 = (-3) . 127 . 1 = -60960$

$w_1 = 2 . 191 . 3 = 11842$

Blue $= v_1 = (-3) . 127 . 1 = -10287$

$w_1 = 2 . 191 . 31 = 38200$

Pixel (0,2) :

Red $= v_1 = (-3) . 127 . 162 = -61722$

$w_1 = 2 . 191 . 98 = 37436$

Green $= v_1 = (-3) . 127 . 163 = -62103$

$w_1 = 2 . 191 . 99 = 37818$

Blue $= v_1 = (-3) . 127 . 24 = -9144$

$w_1 = 2 . 191 . 103 = 39346$

Pixel (0,3) :

Red $= v_1 = (-3) . 127 . 163 = -62103$

$w_1 = 2 . 191 . 99 = 37818$

Green $= v_1 = (-3) . 127 . 27 = -10287$

$w_1 = 2 . 191 . 100 = 38200$

Blue $= v_1 = (-3) . 127 . 25 = -9424$

$w_1 = 2 . 191 . 25 = 9550$

Pixel (0,4) :

Red $= v_1 = (-3) . 127 . 26 = -9906$

$w_1 = 2 . 191 . 26 = 9932$

Green $= v_1 = (-3) . 127 . 25 = -9525$

$w_1 = 2 . 191 . 25 = 9550$

Blue $= v_1 = (-3) . 127 .23 = -8763$

$w_1 = 2 . 191 . 104 = 39728$

The calculation process will continue until the end of the pixel value (4,4). The next process is to find the values of r, s, t, u with the following formula: $r_1 = (v_1 + w_1) \bmod n$

$s_1 = (v_1 - w_1) \bmod n$

$t_1 = (-v_1 + w_1) \bmod n$

$u_1 = (-v_1 - w_1) \bmod n$

Pixel (0,0) :

Red $= r_1 = (-13716 + 13752) \bmod 24257$

$= 36$

$s_1 = (-13716 - 13752) \bmod 24257$

= 21946
t_1 = (-(-13716) + 13752) mod 24257
= 3211
u_1 = (- (-13716) - 13752) mod 24257
= 24221

Green = r_1 = (-59436 + 13370) mod 24257
= 2448
s_1 = (-59436 - 13370) mod 24257
= 24222
t_1 = (-(-59436) + 13370) mod 24257
= 35
u_1 = (- (-59436) - 13370) mod 24257
= 21809

Blue = r_1 = (-60960 + 11842) mod 24257
= 23653
s_1 = (-60960 - 11842) mod 24257
= 24226
t_1 = (-(-60960) + 11842) mod 24257
= 31
u_1 = (- (-60960) - 11842) mod 24257
= 604

Pixel (0,1) :

Red = r_1 = (-12192 + 12224) mod 24257
= 32
s_1 = (-12192 - 12224) mod 24257
= 24098
t_1 = (-(-12192) + 12224) mod 24257
= 159
u_1 = (- (-12192) - 12224) mod 24257
= 24225

Green = r_1 = (-60960 + 11842) mod 24257
= 23653
s_1 = (-60960 - 11842) mod 24257
= 24226
t_1 = (-(-60960) + 11842) mod 24257
= 31
u_1 = (- (-60960) - 11842) mod 24257
= 604

Blue = r_1 = (-10287 + 38200) mod 24257
= 3656
s_1 = (-10287 - 38200) mod 24257
= 27
t_1 = (-(-10287) + 38200) mod 24257
= 24230
u_1 = (- (-10287) - 38200) mod 24257
= 20601

Pixel (0,2) :

Red = r_1 = (-61722 + 37436) mod 24257
= 24228
s_1 = (-61722 - 37436) mod 24257
=22127
t_1 = (-(-61722) + 37436) mod 24257
= 2130
u_1 = (- (-61722) - 37436) mod 24257
= 29

Green = r_1 = (-62103 + 37818) mod 24257
= 24229
s_1 = (-62103 - 37818) mod 24257
= 21364
t_1 = (-(-62103) + 37818) mod 24257
= 2893
u_1 = (- (-62103) - 37818) mod 24257
= 28

Blue = r_1 = (-9144 + 39346) mod 24257
= 5945
s_1 = (-9144 - 39346) mod 24257
= 24
t_1 = (-(-9144) + 39346) mod 24257
= 24233
u_1 = (- (-9144) - 39346) mod 24257

= 18312

Pixel (0,3) :

Red = r_1 = (-62103 + 37818) mod 24257
= 24229
s_1 = (-62103 - 37818) mod 24257
= 21364
t_1 = (-(-62103) + 37818) mod 24257
= 2893
u_1 = (- (-62103) - 37818) mod 24257
= 28

Green = r_1 = (-10287 + 38200) mod 24257
= 3656
s_1 = (-10287 - 38200) mod 24257
= 27
t_1 = (-(-10287) + 38200) mod 24257
= 24230
u_1 = (- (-10287) - 38200) mod 24257
= 20601

Blue = r_1 = (-9525 + 9550) mod 24257
= 25
s_1 = (-9525 - 9550) mod 24257
= 5182
t_1 = (-(-9525) + 9550) mod 24257
= 1
u_1 = (- (-9525) - 9550) mod 24257
= 24232

Pixel (0,4) :

Red = r_1 = (-9906 + 9932) mod 24257
= 26
s_1 = (-9906 - 9932) mod 24257
= 4419
t_1 = (-(-9906) + 9932) mod 24257
= 19838
u_1 = (- (-9906) - 9932) mod 24257
= 356

Green = r_1 = (-9525 + 9550) mod 24257
= 25
s_1 = (-9525 - 9550) mod 24257
= 5182
t_1 = (-(-9525) + 9550) mod 24257
= 1
u_1 = (- (-9525) - 9550) mod 24257
= 24232

Blue = r_1 = (-8763 + 39728) mod 24257
= 6708
s_1 = (-8763 - 39738) mod 24257
= 23
t_1 = (-(-8763) + 39738) mod 24257
= 24234
u_1 = (- (-8763) - 39738) mod 24257
= 17549

The calculation process will continue until the end of the pixel value (4,4). From the decryption process there are 4 solutions namely r, s, t, u. After that we will compare the values and the decryption result will be found among the 4 solutions. so that the results of the ciphertext in the rabin cryptosystemdecryption process are known as follows:

Table 8: Result

(x,y)	0	1	2	3	4
0	R = 36 G = 35 B = 31	R = 32 G = 31 B = 27	R = 29 G = 28 B = 24	R = 28 G = 28 B = 24	R = 26 G = 25 B = 23
1	R = 41 G = 37 B = 34	R = 34 G = 33 B = 29	R = 32 G = 30 B = 26	R = 27 G = 26 B = 24	R = 26 G = 25 B = 23
2	R = 43 G = 39 B = 36	R = 38 G = 34 B = 31	R = 32 G = 31 B = 27	R = 27 G = 26 B = 24	R = 26 G = 25 B = 23
3	R = 47 G = 43	R = 44 G = 40	R = 40 G = 39	R = 41 G = 40	R = 32 G = 31

	B = 40	B = 37	B = 34	B = 38	B = 29
4	R = 45 G = 41 B = 38	R = 43 G = 40 B = 35	R = 40 G = 37 B = 32	R = 41 G = 40 B = 38	R = 40 G = 39 B = 37

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:

Fig. 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:

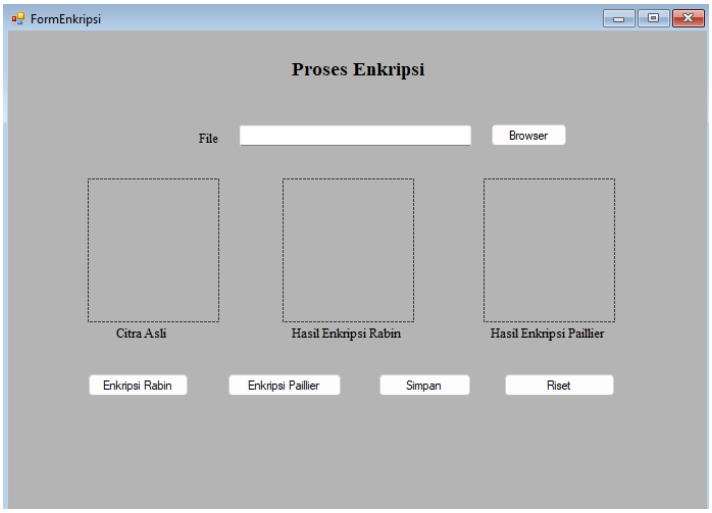

Fig. 3 : Form of Encryption

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

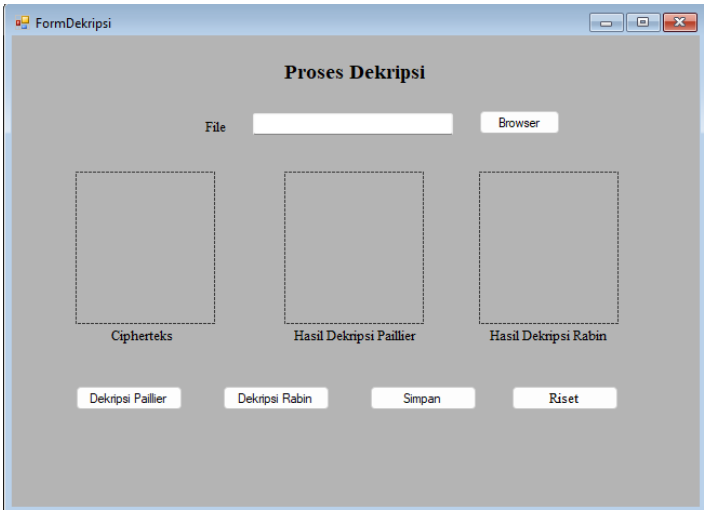

Fig. 4: Form Decryption

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

Based on the analysis conducted, Rabin and Paillier algorithms have different but complementary encryption characteristics in maintaining digital image security. Rabin Cryptosystem, which is based on the square number factorization difficulty, produces a strong level of security but requires special handling in decryption due to the possibility of multiple plaintexts. Meanwhile, the Paillier Cryptosystem, which is based on the homomorphic additive problem, provides an advantage in processing encrypted data and supports certain mathematical operations without having to perform decryption. Combining these two algorithms in the digital image encryption process provides an additional layer of security and strengthens the protection against cryptographic attacks.

6. Suggestion

1. I hope for further research to further refine the program implementation in the Rabin Cryptosystem decryption process.

2. Given that the Rabin Algorithm requires special handling in the decryption process due to the possibility of multiple plaintexts, further research is needed to find methods or supporting algorithms that can speed up and simplify the decryption process without reducing security. This is important so that the application of super encryption can be more efficient and practical in real-world applications.

Acknowledgement

I would like to express my heartfelt thanks to my supervisor and friends who have helped me complete this thesis, allowing me to publish this journal.

References

[1] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.

[2] A. C. Frobenius and E. R. Hidayat S. H. S, "Steganografi LSB Dengan Modifikasi Kriptografi: Caesar, Vigenere, Hill Cipher dan Playfair Pada Image," *Melek IT Inf. Technol. J.*, vol. 6, no. 1, pp. 33–40, 2020, doi: 10.30742/melek-it.v6i1.301.

[3] R. K. Ramesh, R. Dodmane, S. Shetty, G. Aithal, M. Sahu, and A. K. Sahu, "A Novel and Secure Fake-Modulus Based Rabin-3 Cryptosystem," *Cryptography*, vol. 7, no. 3, 2023, doi: 10.3390/cryptography7030044.

[4] EVAPIONA, Achmad Fauzi, and Milli Alfhi Syari, "Digital Image Security Implementation With Uses Super Encryption Algorithm Myszkowski And The Algorithm Paillier Cryptosystem," *J. Artif. Intell. Eng. Appl.*, vol. 3, no. 1, pp. 70–82, 2023, doi: 10.59934/jaiea.v3i1.262.

[5] N. Z. Munantri, H. Sofyan, and M. Y. Florestiyanto, "Aplikasi Pengolahan Citra Digital Untuk Identifikasi Umur Pohon," *Telematika*, vol. 16, no. 2, p. 97, 2020, doi: 10.31315/telematika.v16i2.3183.

[6] S. Hariati, A. M. H. Pardede, and M. Sihombing, "Application of the DCT Algorithm to Protect Image Files with Key Symbols", *j. of artif. intell. and eng. appl.*, vol. 3, no. 3, pp. 618–623, Jun. 2024.

[7] S. Hadi Keswara, A. Fauzi, and Nurhayati, "Image Processing for Freshness Identification Tilapia Using Backpropagation Algorithm (Case Study: Binjai City Food Security and Agriculture Office)", *j. of artif. intell. and eng. appl.*, vol. 3, no. 3, pp. 650–658, Jun. 2024.

[8] R. Puspadini and M. P. U. Sitompul, "Implementation of the Laplacian of Gaussian Algorithm in Edge Detection Image Processing of Zebra Cross Damage on Highways in the Langkat Regency Area", *j. of artif. intell. and eng. appl.*, vol. 3, no. 2, pp. 601–605, Feb. 2024.