Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15 yrs june 202 3 . Vol. 2 . No. 3; e-ISSN : 2808-4519

A Combination Of A Rail Fence Cipher And Merkle Hellman Algorithm For Digital Image Security

Irwansyah[1*], Achmad Fauzi[2], Siswan Syahputra[3]

[1,2,3] Informatics Engineering, STMIK KAPUTAMA
Jl. Veterans No. 4A-9A, Binjai, North Sumatra, Indonesia
Email: irwansyahboy28@gmail.com[1], fauzyrivai88@gmail.com[2], siswansyahputra90@gmail.com[3]

Abstract

Image is a combination of planes, points, lines and colors to create a physical or human object. Images can be in the form of 2-dimensional images, such as photographs and paintings. 3-dimensional image like a statue. The use of image media information has several weaknesses, one of which is the ease with which it can be manipulated by certain parties with the help of increasingly developing technology. In this study, the Rail Fence Cipher and Merkle Hellman methods were applied which aimed to obtain a stronger cipher by utilizing two key levels where an asymmetric algorithm was used to protect the symmetric key. The asymmetric algorithm used is Merkle Hellman and the symmetrical algorithm used is Rail Fence Cipher. The results of this study indicate that applying the Rail Fence Cipher and Merkle Hellman algorithms can secure image files and secure keys for data integrity. Encryption and description processing time is affected by the size and resolution of the image file.

Keywords: *Combination, Cipher, Algorithm, Image Security.*

1. Introduction

Image security is one of the important things in everyday life. Digital image as a form of digital data is currently widely used to store photos or images in digital format. Therefore the image must be secured because it is feared that the data can fall into the hands of irresponsible parties, which are then misused for negative things. The Rail Fence Cipher algorithm is a classic algorithm of the transposition algorithm model. Rail Fence Cipher uses a position change technique based on levels, where the level values are called encryption and decryption keys in this algorithm. The encoding results of the Rail Fence Cipher algorithm are still vulnerable to brute force attacks because the rail fence cipher does not change each letter, so the frequency pattern of letters in the plaintext remains visible in the ciphertext. because the Rail Fence Cipher only changes the order of the plaintext letters and does not substitute each letter, it will be combined or strengthened again with the Merkle-Hellman Algorithm. The Merkle-Hellman algorithm is cryptography that uses an asymmetric algorithm and has 2 main keys, namely the public key and the private key. The private key is the key that is kept by the parties who have the right to know it . In this Merkle Hellman system, the keys used are 2 different keys. One key for encryption and one key for decryption.

2. Research methodology

Research methodology refers to the set of steps or procedures used to plan, conduct, and analyze research. Research methodology involves selecting appropriate approaches, techniques, and tools to collect and analyze relevant data to answer research questions.

2.1. Cryptography

The word cryptography or cryptography is known to come from the Greek, crypto and graphia. Where crypto means hiding, while graphia means writing. According to the terminology, cryptography is the science and art of maintaining the security of messages sent from one place to another [1].

2.2. Classic Cryptography And Modern Cryptography

Classical cryptography is an algorithm that uses one key to secure data. This technique has been used several centuries ago. This cryptography performs randomization of letters / plaintext. This cryptography only randomizes the letters A – Z [2].

Modern cryptography is an improvement that refers to classical cryptography. This algorithm uses binary symbol processing which is formed from ASCII (American Standard Code for Information Interchange) code because it follows digital computer operations, so it requires basic knowledge of mathematics to master it. This algorithm has a complex level of difficulty that makes it very difficult for cryptanalysts to crack the ciphertext without knowing the key [3].

2.3. Rail Fence Cipher Algorithm

The Rail Fence Cipher Algorithm is one of the classical algorithms of transposition cipher implementation variations. In Rail Fence Cipher, plaintext is written vertically down along the n-rails, and writes again to a new column when it reaches the nth character. The resulting ciphertext is a sequence of characters that is read horizontally [4].
The encryption and decryption formulas for the Rail Fence Cipher algorithm are as follows:

Rail Fence Cipher Encryption Formula:
Cycle = (2 x rail) – 2 ..... (1)
rpos = { mod{i, cycle}
{mod{-{mod{i,cycle}, cycle} ..... (2)

Rail Fence Cipher Decryption Formula:
The decryption process is carried out by placing each letter back in the appropriate position on its respective rail. After that it is read in a zig-zag direction starting from the first letter on the 0th rail to the last letter.

2.4. Markle Hellman's Algorithm

Merkle Hellman is a cryptographic system that uses asymmetric key types. This Merkle Hellman system uses two different locks. One key for encryption and one key for decryption. The Merkle-Hellman algorithm system uses an asymmetric encryption key type. Therefore, the keys used to encrypt and decrypt messages are different. In this case, if Alice is to decrypt messages received from Bob, for example, Alice must first know her secret key to get Bob's public key. For example, Alice has the following increasing integer sequence w = 1 + 3 + 6 + 11 + 32 + 87 + 141 + 354 = 635. Since the sum is 281, Alice chooses any prime q that is greater than 635, say 881, and any number r with a value between 1-w-1, namely 588 [5].

So the secret key that Alice has is:
w = (1, 3, 6, 11, 32, 87, 141, 354)
q = 881
r = 588

Information:
w = super increasing number
r = private key
q = divisor number
To get the public key, use the formula:

$$t_i = r * w \bmod q$$

Information:
t_i = public key
r = secret key
w = super increasing number
q = number of divisors and calculate like the way below:

Table 1: Public Key Search Process

r		W		q		t_i
588	*	1	mods	881	=	588
588	*	3	against	881	=	2

588	*	5	against	881	=	297
588	*	11	against	881	=	301
588	*	32	against	881	=	315
588	*	87	against	881	=	58
588	*	141	mods	881	=	94
588	*	354	mods	881	=	236

From the table above, the public key results are obtained as follows:
t_i= (588, 2, 297, 301, 315, 58, 94, 236)
For the encryption process, each character is converted into an ASCII number and then changed return be a binary number. For example, the character to be encrypted is the letter "A". The letter "A" is converted to ASCII (A=65) so that it can be decomposed into a binary number. Number binary for the letter "A" is 1000001 .
After getting the binary number of the character in question, the encryption process is carried out with the formula:

$$t_{i^*}x = \sum y$$

Information :
t_(i) = public key
x = binary number of characters
y = multiplication result

Merkle Hellman's Decryption Formula:

z = y mod q

Information:
z = target sum / multiplication result
r = private key
= inverse of r
y = received ciphertext
q = divisor number

2.5 Definition of Image

Image is a picture or likeness of an object. The output image from a data recording system can be optical, analog or digital. Optical image can be a photo. Analog images are continuous images, such as images on television monitors, x-ray photos, CT scan results, and so on. Analog images are generated from several tools such as analog video cameras, analog photo cameras, webcams, ultrasound sensors in ultrasound systems, and others.

3. Results and discussion

3.1. Rail Fence Cipher Algorithm Encryption Calculation

Figure 1 Figure 3.1 8X8 Pixel Images and Samples

Figure 1 is an image that will be encrypted, the first step is to take the RGB value from the image to be encrypted, the process of taking the RGB value is done using Photoshop software, the resulting value is very large, for that in the initial test the author took an RGB value of 8x8 pixels which starting from (0,0), here are the pixels that will take the RGB.

Table 2: Plaintext

R=120 G=171 B=66	R=134 G=185 B=80	R=133 G=187 B=65	R=124 G=178 B=56	R=160 G=209 B=92	R=196 G=243 B=139	R=100 G=165 B=63	R=100 G=166 B=78
R=113 G=164 B=59	R=120 G=171 B=66	R=137 G=191 B=69	R=131 G=85 B=63	R=149 G=198 B=81	R=199 G=246 B=142	R=134 G=199 B=97	R=118 G=184 B=94
R=118 G=171 B=57	R=111 G=164 B=50	R=139 G=191 B=64	R=156 G=205 B=79	R=163 G=210 B=98	R=190 G=233 B=143	R=140 G=207 B=130	R=141 G=206 B=142
R=118 G=171 B=57	R=127 G=180 B=66	R=153 G=105 B=78	R=167 G=216 B=90	R=181 G=228 B=116	R=189 G=232 B=142	R=140 G=207 B=130	R=134 G=199 B=135
R=110 G=166 B=65	R=124 G=180 B=79	R=157 G=211 B=97	R=165 G=215 B=102	R=179 G=222 B=130	R=202 G=242 B=171	R=161 G=229 B=180	R=108 G=176 B=127
R=137 G=193 B=92	R=92 G=148 B=47	R=115 G=169 B=55	R=158 G=208 B=95	R=182 G=225 B=133	R=192 G=232 B=161	R=177 G=245 B=196	R=122 G=190 B=141
R=161 G=223 B=150	R=91 G=153 B=80	R=61 G=115 B=40	R=103 G=153 B=80	R=180 G=220 B=158	R=179 G=218 B=165	R=165 G=235 B=181	R=148 G=218 B=164
R=162 G=224 B=151	R=143 G=205 B=132	R=49 G=103 B=28	R=27 G=77 B=40	R=162 G=202 B=140	R=189 G=228 B=175	R=157 G=227 B=173	R=149 G=219 B=165

The process of encrypting the rail fence cipher algorithm in the picture above will use the key = 8 (8 columns), move the character position from the first rail line to the last line down sequentially in a zig-zag manner so as to form an imaginary fence. as in the table below:

Table 3: Process of encrypting

R=120 G=171 B=66	R=134 G=199 B=97		R=181 G=228 B=116		R=115 G=169 B=55		R=162 G=224 B=151	
R=134 G=185 B=80	R=199 G=246 B=142	R=118 G=184 B=94	R=167 G=216 B=90	R=189 G=232 B=142	R=92 G=148 B=47	R=158 G=208 B=95	R=148 G=218 B=164	R=143 G=205 B=132
R=133 G=187 B=65	R=149 G=198 B=81	R=118 G=171 B=57	R=153 G=105 B=78	R=140 G=207 B=130	R=137 G=193 B=92	R=182 G=225 B=133	R=165 G=235 B=181	R=49 G=103 B=28
R=124 G=178 B=56	R=131 G=85 B=63	R=111 G=164 B=50	R=127 G=180 B=66	R=134 G=199 B=135	R=108 G=176 B=127	R=192 G=232 B=161	R=179 G=218 B=165	R=27 G=77 B=40
R=160 G=209 B=92	R=137 G=191 B=69	R=139 G=191 B=64	R=118 G=171 B=57	R=110 G=166 B=65	R=161 G=229 B=180	R=177 G=245 B=196	R=180 G=220 B=158	R=162 G=202 B=140
R=196 G=243 B=139	R=120 G=171 B=66	R=156 G=205 B=79	R=134 G=199 B=135	R=124 G=180 B=79	R=202 G=242 B=171	R=122 G=190 B=141	R=103 G=153 B=80	R=189 G=228 B=175
R=100 G=165 B=63	R=113 G=164 B=59	R=163 G=210 B=98	R=140 G=207 B=130	R=157 G=211 B=97	R=179 G=222 B=130	R=161 G=223 B=150	R=61 G=115 B=40	R=157 G=227 B=173
R=100 G=166 B=78		R=190 G=233 B=143		R=165 G=215 B=102		R=91 G=153 B=80		R=149 G=219 B=165

the encryption results are obtained by reading each letter on the rail horizontally from left to right here starting from pixel (0.0) to (0.7) then the ciphertext results will be obtained on each rail and each RGB value will also be displayed as a binary number :

Ciphertext:
Pixels (0,0)
R=120=0111 1000
G=171=1010 1011
B=66 =0100 0010
Pixels (0.1)

R=134=1000 0110
G=199=1100 0111
B=97 =0110 0001
Pixels (0.3)
R=181=1011 0101
G=228=1110 0100
B=116=0111 0100
Pixels (0.5)
R=115=0111 0011
G=169=1010 1001
B=55 =0011 0111
Pixels (0.7)
R=162=1010 0010
G=224=1110 0000
B=151=1001 0111

3.2. Calculation of the Merkle Hellman Algorithm Encryption

plaintext from the results of the rail fence cipher encryption will be converted to a binary number and the results are as follows
Plaintext :
01111000 10101011 01000010 10000110 11000111 01100001 10110101 11100100 01110100 01110011 10101001 00110111 10100010 1110 0000 10010111

Determining Superincreasing:
w = 2 + 3 + 6 + 13 + 27 + 52 + 104 + 208 = 415
q = 419, r = 31
The formula for finding the public key is ie

t = w * r mod q

w1 = 2 * 31 mod 419= 62
w2 = 3 * 31 mod 419= 93
w3 = 6 * 31 mod 419= 186
w4 = 13 * 31 mod 419= 403
w5 = 27 * 31 mod 419= 418
w6 = 52 * 31 mod 419= 355
w7 = 104 * 31 mod 419= 291
w8 = 208 * 31 mod 419= 163
so that the public key is obtained, namely:
{:62,93,186,403,418,355,291,163}

Encryption is done by splitting the ciphertext into blocks of bits that are the same length as the cardinality of the public key sequence. The ciphertext is divided into blocks that are 8 long, then each bit in the block is multiplied by the corresponding element in the public key, the encryption will be done according to rail and rgb on each line.:
Formula :

$$x * t_i = \sum y$$

Pixels (0,0)
Plaintext Block 1 : 0111 1000
Public Key : 62,93,186,403,418,355,291,163
Cryptogram : (1x93)+(1x186)+(1x403)+(1x418)=1100
Plaintext Blocks 2 : 1010 1011
Public Key : 62,93,186,403,418,355,291,163
Cryptogram : (1x62)+ (1x186)+ (1x418)+ (1x291)+ (1x163)=1120
Plaintext Block 3 : 0100 0010
Public Key : 62,93,186,403,418,355,291,163
Cryptogram : (1x93)+(1x291)=384

Pixels (0.1)
Plaintext Blocks 1 : 1000 0110
Public Key : 62,93,186,403,418,355,291,163
Cryptogram : (1x62)+(1x355)+(1x291)= 708
Plaintext Blocks 2 : 1100 0111
Public Key : 62,93,186,403,418,355,291,163
Cryptogram : (1x62)+(1x93)+(1x355)+(1x291)+(1x163)= 964
Plaintext Blocks 3 : 0110 0001
Public Key : 62,93,186,403,418,355,291,163
Cryptogram : (1x93)+(1x186)+(1x163)= 442

Pixel (0,3)
Plaintext Block 1 : 1011 0101
Public Key : 62,93,186,403,418,355,291,163
Cryptogram : (1x62)+(1x186)+(1x403)+(1x355)+(1x163)= 1169
Plaintext Block 2 : 1110 0100
Public Key : 62,93,186,403,418,355,291,163
Cryptogram : (1x62)+(1x93)+(1x186)+(1x355)= 696
Plaintext Block 3 : 0111 0100
Public Key : 62,93,186,403,418,355,291,163
Cryptogram : (1x93)+(1x186)+(1x403)+(1x355)=1037

Pixel (0,5)
Plaintext Block 1 : 0111 0011
Public Key : 62,93,186,403,418,355,291,163
Cryptogram : (1x93)+(1x186)+(1x403)+(1x291)+(1x163)=1136
Plaintext Block 2 : 1010 1001
Public Key : 62,93,186,403,418,355,291,163
Cryptogram : (1x62)+(1x186)+(1x418)+(1x163)=829
Plaintext Block 3 : 0011 0111
Public Key : 62,93,186,403,418,355,291,163
Cryptogram : (1x186)+(1x403)+(1x355)+(1x291)+(1x163)=1398

Pixel (0,7)
Plaintext Block 1 : 1010 0010
Public Key : 62,93,186,403,418,355,291,163
Cryptogram : (1x62)+(1x186)+(1x291)=539
Plaintext Block 2 : 1110 0000
Public Key : 62,93,186,403,418,355,291,163
Cryptogram : (1x62)+(1x93)+(1x186)=341
Plaintext Block 3 : 1001 0111
Public Key : 62,93,186,403,418,355,291,163
Cryptogram : (1x62)+(1x403)+(1x355)+(1x291)+(1x163)=1274

After encryption, the ciphertext is as follows:

Pixels (0,0) = 1100,1120,384
Pixels (0,1) = 708,964,442
Pixels (0,3) = 1169,696,1037
Pixels (0.5) = 1136,829,1398
Pixels (0.7) = 539,341,1274

3.3. Calculation Description of the Merkle Hellman Algorithm

The description process will be carried out first using Merkle Hellman with the private keys namely '2,3,6,13,27,52,104,208' and the ciphertext as follows:

Pixels (0,0) = 1100,1120,384
Pixels (0,1) = 708,964,442
Pixels (0,3) = 1169,696,1037
Pixels (0.5) = 1136,829,1398
Pixels (0.7) = 539,341,1274

n formula. n^(-1) ≡ 1 (mod m) then:
n^(-1) can be obtained from: n^(-1) = (1 + 419 k) / 31, try k = 0,1,2,.....,29 to get an integer, namely n^(-1) = 392. Next do the description:

Formula **z * n mod q**

Pixels (0,0)
1100.392 mod 419 = 49 = 3+6+13+27 =0111 1000
1120.392 mod 419 = 347 = 2+6+27+104+208 =1010 1011
384.392 mod 419 = 107 = 3+104 =0100 0010

Pixels (0.1)
708.392 mod 419 = 158 = 2+52+104 =1000 0110
964,392 mod 419 = 369 = 2+3+52+104+208 =1100 0111
442.392 mod 419 = 217 = 3+6+208 =0110 0001

Pixels (0.3)
1169,392 mod 419 = 281 = 2+6+13+52+208 =1011 0101
696.392 mod 419 = 63 = 2+3+6+52 =1110 0100
1037.392 mod 419 = 74 = 3+6+13+52 =0111 0100
Pixels (0.5)
1136.392 mod 419 = 334 = 3+6+13+104+208 =0111 0011
829,392 mod 419 = 243 = 2+6+27+208 =1010 1001
1398.392 mod 419 = 383 = 6+13+52+104+208 =0011 0111
Pixels (0.7)
539.392 mod 419 = 112 = 2+6+104 =1010 0010
341.392 mod 419 = 11 = 2+3+6 =1110 0000
1274.392 mod 419 = 379 = 2+13+52+104+208 =1001 0111

Then proceed to pixel (7,7) so that the results of the ciphertext in the Merkle Hellman Decryption process are known as follows:
01111000 10101011 01000010 10000110 11000111 01100001 10110101 11100100 01110100 01110011 10101001 00110111 10100010 11100000 10010111 10000110 10111001 01010000 11000111 11110110 10001110 01110110 10111000 01011110 10100111 11011000 01011010 10111101 11101000 10001110 01011100 10010100 00101111 10011110 11010000 01011111 10010100 11011010 10100100 10001111 11001101 10000100 10000101 10111011 01000001 10010101 11000110 01010001 01110110 10101011 00111001 10011001 01101001 01001110 10001100 11001111 10000010 10001001 11000001 01011100 10110110 11100001 10000101 10100101 11101011 10110101 00110001 01100111 00011100 01111100 10110010 00111000 10000011 01010101 00111111 01101111 10100100 00110010 01111111 10110100 01000010 10000110 11000111 10000111 01101100 10110000 01111111 11000000 11101000 10100001 10110011 11011010 10100101 00011011 01001101 00101000 10100000 11010001 01011100 10001001 10111111 01000101 10001011 10111111 01000000 01110110 10101011 00111001 01101110 10100110 01000001 10100001 11100101 10110100 10110001 11110101 11000100 10110100 11011100 10011110 10100010 11001010 10001100 11000100 11110011 10001011 01111000 10101011 01000010 10011100 11001101 01001111 10000110 11000111 10000111 01111100 10110100 01001111 11001010 11110010 10101011 01111010 10111110 10001101 01100111 10011001 01010000 10111101 11100100 10101111 01100100 10100101 00111111 01110001 10100100 00111011 10100011 11010010 01100010 10001100 11001111 10000010 10011101 11010011 01100001 10110011 11011110 10000010 10100001 11011111 10010110 00111101 01110011 00101000 10011101 11100011 10101101 01100100 10100110 01001110 10111110 11101001 10001111 10100101 11010111 01100110 01011011 10011001 01010000 10010101 11011011 10100101.

3.4. Calculation Description of the Rail Fence Cipher Algorithm

The ciphertext results that have been described by the Merkle Hellman algorithm will then be described again using the rail fence cipher algorithm, by sorting by rail and the number of each, changing the binary number to a decimal number first then putting back each RGB in the appropriate position on each rail, do it horizontally from left to right

Table 4: Ciphertext results

R=120 G=171 B=66	R=134 G=199 B=97		R=181 G=228 B=116		R=115 G=169 B=55		R=162 G=224 B=151	
R=134 G=185 B=80	R=199 G=246 B=142	R=118 G=184 B=94	R=167 G=216 B=90	R=189 G=232 B=142	R=92 G=148 B=47	R=158 G=208 B=95	R=148 G=218 B=164	R=143 G=205 B=132
R=133 G=187 B=65	R=149 G=198 B=81	R=118 G=171 B=57	R=153 G=105 B=78	R=140 G=207 B=130	R=137 G=193 B=92	R=182 G=225 B=133	R=165 G=235 B=181	R=49 G=103 B=28
R=124 G=178 B=56	R=131 G=85 B=63	R=111 G=164 B=50	R=127 G=180 B=66	R=134 G=199 B=135	R=108 G=176 B=127	R=192 G=232 B=161	R=179 G=218 B=165	R=27 G=77 B=40
R=160 G=209 B=92	R=137 G=191 B=69	R=139 G=191 B=64	R=118 G=171 B=57	R=110 G=166 B=65	R=161 G=229 B=180	R=177 G=245 B=196	R=180 G=220 B=158	R=162 G=202 B=140
R=196 G=243 B=139	R=120 G=171 B=66	R=156 G=205 B=79	R=134 G=199 B=135	R=124 G=180 B=79	R=202 G=242 B=171	R=122 G=190 B=141	R=103 G=153 B=80	R=189 G=228 B=175
R=100 G=165 B=63	R=113 G=164 B=59	R=163 G=210 B=98	R=140 G=207 B=130	R=157 G=211 B=97	R=179 G=222 B=130	R=161 G=223 B=150	R=61 G=115 B=40	R=157 G=227 B=173
R=100 G=166 B=78		R=190 G=233 B=143		R=165 G=215 B=102		R=91 G=153 B=80		R=149 G=219 B=165

After that it is read in a zig-zag direction starting from the first RGB on the 0th rail to the RGB on the last rail, and the results of the description will be like the table below.

Table 5: Results of the description

R=120 G=171 B=66	R=134 G=185 B=80	R=133 G=187 B=65	R=124 G=178 B=56	R=160 G=209 B=92	R=196 G=243 B=139	R=100 G=165 B=63	R=100 G=166 B=78

R=113 G=164 B=59	R=120 G=171 B=66	R=137 G=191 B=69	R=131 G=85 B=63	R=149 G=198 B=81	R=199 G=246 B=142	R=134 G=199 B=97	R=118 G=184 B=94
R=118 G=171 B=57	R=111 G=164 B=50	R=139 G=191 B=64	R=156 G=205 B=79	R=163 G=210 B=98	R=190 G=233 B=143	R=140 G=207 B=130	R=141 G=206 B=142
R=118 G=171 B=57	R=127 G=180 B=66	R=153 G=105 B=78	R=167 G=216 B=90	R=181 G=228 B=116	R=189 G=232 B=142	R=140 G=207 B=130	R=134 G=199 B=135
R=110 G=166 B=65	R=124 G=180 B=79	R=157 G=211 B=97	R=165 G=215 B=102	R=179 G=222 B=130	R=202 G=242 B=171	R=161 G=229 B=180	R=108 G=176 B=127
R=137 G=193 B=92	R=92 G=148 B=47	R=115 G=169 B=55	R=158 G=208 B=95	R=182 G=225 B=133	R=192 G=232 B=161	R=177 G=245 B=196	R=122 G=190 B=141
R=161 G=223 B=150	R=91 G=153 B=80	R=61 G=115 B=40	R=103 G=153 B=80	R=180 G=220 B=158	R=179 G=218 B=165	R=165 G=235 B=181	R=148 G=218 B=164
R=162 G=224 B=151	R=143 G=205 B=132	R=49 G=103 B=28	R=27 G=77 B=40	R=162 G=202 B=140	R=189 G=228 B=175	R=157 G=227 B=173	R=149 G=219 B=165

3.5. Discussion

The design stage that the author does is design the software interface. So in this discussion, we will discuss some of the views of the existing menus using the Rail Fence cipher and Merkle Hellman algorithms, as follows:

3.5.1. Initial Form Design

The initial form is a display form designed as an opening in the application process:

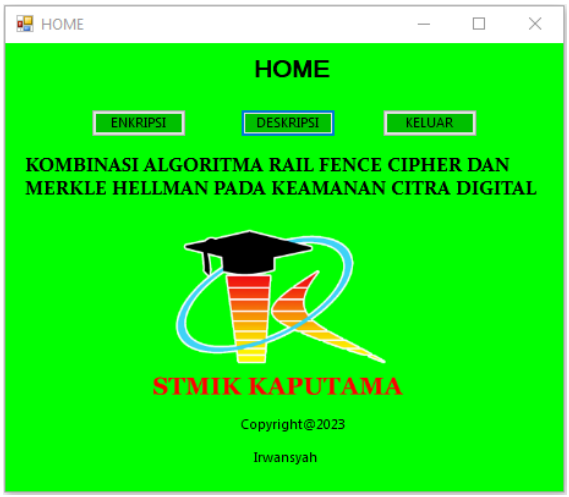

Figure 2: Main Form

3.5.2. Encryption Form

The form of digital image encryption and decryption is a display that is designed as an interface so that the user can interact with the system. When interacting with the user, the form uses buttons that can be selected by the user. The design forms for digital image encryption and decryption are as follows:

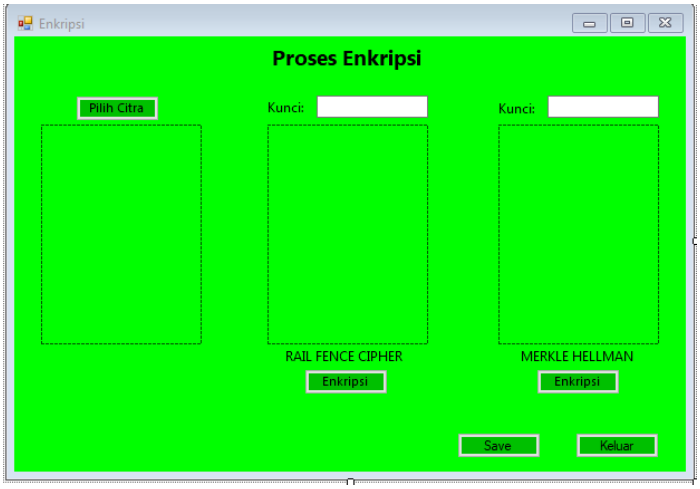

Figure 3: Encryption Form

3.5.3. Description Form

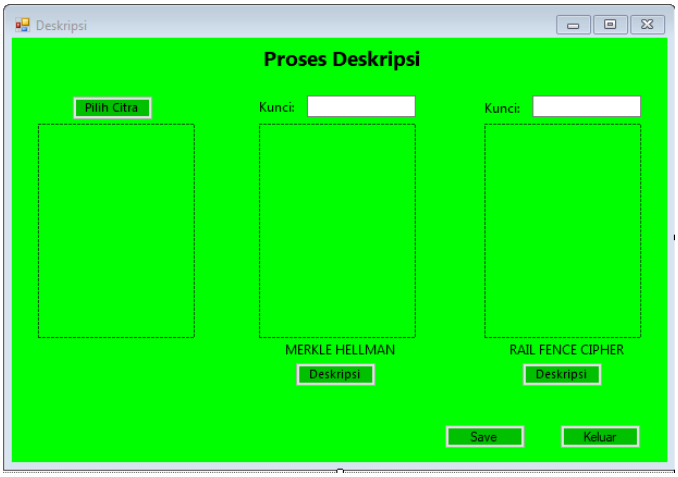

Figure 4: Description Form

4. Conclusion

With this digital image encryption and description application system, the authors can draw conclusions as follows:

1.Rail Fence Cipher is a simple encryption method that involves shifting the characters in a message into a zigzag pattern. This is a relatively easy substitution method to solve mathematically, but by combining it with other algorithms, such as Merkle-Hellman, the security of digital images can be improved.

2.Merkle-Hellman is a public key algorithm used for data encryption. This algorithm has high security strength because the encryption key is very difficult to find through mathematical analysis. By combining the Merkle-Hellman with the Rail Fence Cipher, digital images can be encrypted with more complex methods, increasing their level of security.

3.In this combination, Rail Fence Cipher can be used as a pre-image conversion step before implementing Merkle-Hellman encryption. This provides an additional layer of security, since the messages to be encrypted cannot be easily identified through simple patterns or character frequency analysis.

Bibliography

[1] H. Mukhtar, *Cryptography for Data Security* . Yogyakarta, 2018.

[2] S. Aripin and M. Syahrizal, "Securing Video Files Using the Merkle Hellman Knapsack Algorithm," *J. Media Inform. Budidarma* , vol. 4, no. 2, p. 461, 2020, doi: 10.30865/mib.v4i2.2039.

[3] Sumandri, "Cryptographic Algorithmic Model Studies," *Semin. Matt. And Educator. Matt. Uny* , pp. 265–272, 2017, [Online]. Available: http://seminar.uny.ac.id/semnasmatematika/sites/seminar.uny.ac.id.semnasmatematika/files/full/T-37.pdf

[4] D. Ratna, "Implementation of the Rail Fence Cipher Algorithm in 2D Image Data Security," *Pelita Inform. inf. and …* , vols. 7, pp. 38–42, 2018, [Online]. Available: https://ejurnal.stmik-budidarma.ac.id/index.php/pelita/article/view/881

[5] M. Simanjuntak, T. Pasaribu, and S. Rahmadilla, "Implementation of the Merkle Hellman Algorithm for Database Security," *MEANS (Media Inf. Anal. and Sist.* , vol. 4, no. 1, pp. 46–50 , 2019, doi: 10.54367/means.v4i1.327.