Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

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

Application Of Super Encryption Using Rot 13 Algorithm Method and Algorithm Beaufort Cipher For Image Security Digital

Ayu Devia Pertiwi[1], Achmad Fauzi[2], Siswan Syahputra[3]

[1,2,3] Teknik Informatika, STMIK KAPUTAMA
Jl. Veteran No. 4A-9A, Binjai, Sumatera Utara, Indonesia
deviaayu688@gmail.com[1], fauzyrivai88@gmail.com[2], siswansyahputra90@gmail.com[3]*

Abstract

Digital image security is becoming increasingly critical in today's digital era, where sensitive information and data are often stored in image form. Therefore, an effective and secure encryption method is needed to protect the integrity and confidentiality of digital images. This study aims to implement a stronger security approach by combining classic encryption methods, namely the ROT13 algorithm and the Beaufort Cipher algorithm which produces an encryption called "Super Encryption".
In this study, first of all, the ROT13 encryption method will be applied to randomize digital image text by shifting characters as far as 13 positions in the alphabet. Then, the Beaufort Cipher algorithm will be used to apply additional encryption to the digital image, which involves using the key as input in the encryption process.
The results of this study indicate that the Super Encryption method which combines the ROT13 and Beaufort Cipher algorithms provides a higher level of security compared to using each method separately. Security testing and vulnerability analysis show that the combination of these two algorithms produces digital images that are more difficult to decrypt by commonly used decryption attacks.

***Keywords**: Cryptography, image, rot13 algorithm, beaufort cipher algorithm.*

1. Introduction

The rapid development of information and communication technology today which uses computers as its medium has a very negative impacton the security of a digital image from illegal access that allows it to be misused by certain parties who threaten the security of a digital image. Because in today's digital era digital images are often used in various fields such as art design, photography, security surveillance, to medical applications that present various information in them such as image data that is personal and confidential, image data that is private and confidential is very vulnerable to eavesdropping, theft and manipulation from other parties that can cause harm to the owner.

Using Rot13 and Beaufort Cipher is one way to secure images. Both of these methods can guarantee security so that the image does not leak which can harm the owner. To encrypt an image by changing it to make objects blurry, or not too clear so that many people don't know. Meanwhile, what has been encrypted or kept secret will be decrypted back into a digital image that is like the original. Rot13 is a classic algorithm that is commonly used in the UNIX operating system. In the encryption and decryption system, replace each letter with 13 characters before or after it according to the alphabet. Beaufort cipher is a classical algorithm that has a key length equal to the length of the message you want to encrypt and decrypt.

2. Research Methodology

2.1. Cryptography

The word cryptography or cryptography comes from the Greek. Crypto and graphia. Where crypto means hiding, while graphia means writing. So that it can be interpreted that cryptography is a science that studies mathematical techniques related to aspects of information security. Cryptography can also be interpreted as a science or art of maintaining message security. With two basic cryptographic processes in the form of encryption and decryption. Encryption is the process of processing plaintext (readable messages) into cipertext (unreadable random messages). While Decryption is a process of processing cipertext into plaintext. This process takes place using the same key and reverse algorithm [1].

2.2. Classical Algorithm

The classical algorithm is an algorithm that uses one key to protect data. This technique has been used for several centuries. This algorithm randomizes letters in bright words / plaintext. This algorithm only randomizes the letters A-Z and is not recommended for storing important data because it can be completed in a short time [2].

2.3. Rot 13 Algorithm

Rot 13 is a simple algorithm that is commonly used in the UNIX operating system that uses the emperor's code by using a shift of k = 13. The rot13 encryption process this time is by sliding the character forward 13 times. The decryption process, by sliding the character backwards 13 times, counting 1 is the character in front of it. [3]. The encryption and decryption process in the Rot 13 algorithm is as follows: Rot 13 Encryption Process: In this encryption process using the Rot13 Algorithm shifts the character forward as much as 13 steps in front according to the alphabet to be able to produce ciphertext. Suppose the alphabet "A" becomes "N".

Rot 13 Decryption Process: In this encryption process using the Rot13 Algorithm, shifting characters backwards is as much as 13 steps in front according to the alphabet to be able to produce ciphertext. Suppose the alphabet "N" becomes "A".

2.4. Beaufort Cipher Algorithm

The Beaufort cipher was invented by Admiral Sir Francis Beaufort, Royal Navy, who was also the creator of the Beaufort scale, which is an instrument meteorologists use to indicate wind speed. The difference in this method is the key role, in the Vigenere cipher it is used as an addition to plaintext and a subtraction of ciphertext. Whereas in the Beaufort cipher, the key is used to be reduced by plaintext or ciphertext [4].

The encryption and decryption process in the Beaufort cipher algorithm is as follows:
Rot 13 Encryption Formula:
$Ci = Ki – Pi = mod\ 256$

Rot 13 Decryption Formula:
$Pi = (Ki – Ci)\ mod\ 26$

Information :
Ci = Decimal value of the i-th Ciphertext character
Pi = Decimal value of the i-th Plaintext character
Ki = The decimal value of the ith key character

2.5. Definition of Image

Digital images are representative of images taken by machines (analog images) with an approach based on sampling and quantization. Sampling states the size of the boxes arranged in rows and columns. In other words, sampling on an image represents the size of the pixels (dots) in the image, and quantization represents the value of the brightness level expressed in grayscale according to the number of binary bits used by the machine. In other words, the quantization of the image represents the number of colors present in the image. From a mathematical point of view, the image is a continuous function of the light intensity in the two-dimensional plane. The light source illuminates the object, the object reflects back part of the light beam.[5]

3. Results

3.1. Rot 13 Algorithm Encryption Calculation

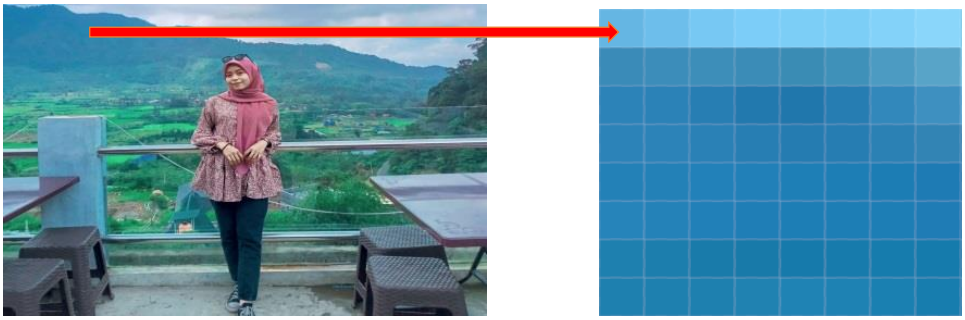

Figure 1: Image and Pixel Sample 8X8 Pixel Image

Figure 3.1 is the shape of the image that will be encrypted, to find the RGB value of the pixel the author reduces the image resolution to 8x8 pixels by using additional Photoshop software, which will start from the point pixel (0.0) to pixel (7, 7).

The steps for the Rot 13 Encryption Algorithm are:
Plaintext :

Table 1: Sample Results of RGB Values

(x,y)	0	1	2	3	4	5	6	7
0	R : 101 G : 182 B : 227	R : 109 G : 190 B : 235	R : 119 G : 200 B : 243	R : 124 G : 205 B : 248	R : 124 G : 206 B : 246	R : 124 G : 206 B : 246	R : 131 G : 210 B : 249	R : 138 G : 214 B : 250
1	R : 58 G : 139 B : 184	R : 60 G : 141 B : 186	R : 61 G : 142 B : 185	R : 59 G : 140 B : 183	R : 58 G : 140 B : 180	R : 63 G : 145 B : 185	R : 76 G : 155 B : 194	R : 88 G : 164 B : 200
2	R : 44 G : 131 B : 184	R : 43 G : 130 B : 183	R : 39 G : 126 B : 179	R : 34 G : 121 B : 174	R : 32 G : 119 B : 172	R : 38 G : 125 B : 178	R : 50 G : 136 B : 187	R : 62 G : 144 B : 192
3	R : 44 G : 131 B : 184	R : 44 G : 131 B : 184	R : 42 G : 129 B : 182	R : 39 G : 126 B : 179	R : 37 G : 124 B : 177	R : 38 G : 125 B :178	R : 43 G : 129 B : 180	R : 50 G : 132 B : 180
4	R : 35 G : 129 B : 183	R : 35 G : 129 B : 183	R : 34 G : 129 B : 185	R : 33 G : 128 B : 184	R : 30 G : 127 B : 182	R : 29 G : 126 B : 181	R : 28 G : 125 B : 180	R : 30 G : 123 B : 180
5	R : 38 G : 132 B : 186	R : 36 G : 130 B : 184	R : 33 G : 128 B : 184	R : 31 G : 126 B : 182	R : 29 G : 126 B : 181	R : 29 G : 126 B : 181	R : 29 G : 126 B : 181	R : 31 G : 124 B : 181
6	R : 30 G : 128 B : 175	R : 28 G : 126 B : 173	R : 25 G : 123 B : 170	R : 24 G : 122 B : 169	R : 22 G : 122 B : 171	R : 23 G : 123 B : 171	R : 22 G : 124 B : 173	R : 21 G : 123 B : 172
7	R : 30 G : 128 B : 175	R : 30 G : 128 B : 175	R : 30 G : 128 B : 175	R : 32 G : 130 B : 177	R : 31 G : 131 B : 180	R : 30 G : 130 B : 179	R : 26 G : 128 B : 177	R : 23 G : 125 B : 174

The encryption process uses the Rot 13 Algorithm by processing the resulting values in table III.1 which are plaintext by shifting the values forward 13 times and shifting based on the ASCII table order, namely as follows:

- The value of R in the table row 0 column 0 = 101 then it is shifted forward 13 times = 114
- The value of G in the table row 0 column 0 = 182 then it is shifted forward 13 times = 195
- Value B in table row 0 column 0 = 227 then it is shifted forward 13 times = 240
- The value of R in the table row 0 column 1 = 109 then it is shifted forward 13 times = 122
- The value of G in the table row 0 column 1 = 190 then it is shifted forward 13 times = 203
- Value B in table row 0 column 1 = 235 then it is shifted forward 13 times = 248
- The value of R in the table row 0 column 2 = 119 then it is shifted forward 13 times = 132
- The value of G in the row 0 column 2 table = 200, then it is shifted forward 13 times = 213
- Value B in table row 0 column 2 = 243 then it is shifted forward 13 times = 256
- The value of R in the table row 0 column 3 = 124 then it is shifted forward 13 times = 137
- The value of G in the table row 0 column 3 = 205 then it is shifted forward 13 times = 218
- Value B in table row 0 column 3 = 248 then it is shifted forward 13 times = 5
- The value of R in the table row 0 column 4 = 124 then it is shifted forward 13 times = 137
- The value of G in the table row 0 column 4 = 206 then it is shifted forward 13 times = 219
- Value B in table row 0 column 4 = 246 then it is shifted forward 13 times = 3
- The value of R in the table row 0 column 5 = 124 then it is shifted forward 13 times = 137
- The value of G in the table row 0 column 5 = 206 then it is shifted forward 13 times = 219
- Value B in table row 0 column 5 = 246 then it is shifted forward 13 times = 3
- The value of R in the table row 0 column 6 = 131 then it is shifted forward 13 times = 144
- The value of G in the table row 0 column 6 = 210 then it is shifted forward 13 times = 223
- Value B in table row 0 column 6 = 249 then it is shifted forward 13 times = 6
- The value of R in the table row 0 column 7 = 138 then it is shifted forward 13 times = 151
- The value of G in the table row 0 column 7 = 214 then it is shifted forward 13 times = 227
- Value B in table row 0 column 7 = 250 then it is shifted forward 13 times = 7

The calculation process continues until the end of the pixel value contained in table III.1. Then it can be obtained from the results of the Rot 13 Algorithm encryption process as follows:

Table 2: Encryption Results of the Rot 13 Algorithm

(x,y)	0	1	2	3	4	5	6	7
0	R : 114 G : 195 B : 240	R : 122 G : 203 B : 248	R : 132 G : 213 B : 256	R : 137 G : 218 B : 5	R : 137 G : 219 B : 3	R : 137 G : 219 B : 3	R : 144 G : 223 B : 6	R : 151 G : 227 B : 7
1	R : 71 G : 152 B : 199	R : 73 G : 154 B : 199	R : 74 G : 155 B : 198	R : 72 G : 153 B : 196	R : 71 G : 153 B : 193	R : 76 G : 158 B : 198	R : 89 G : 168 B : 207	R : 101 G : 177 B : 213
2	R : 57 G : 144 B : 197	R : 56 G : 143 B : 196	R : 52 G : 139 B : 192	R : 47 G : 134 B : 187	R : 45 G : 132 B : 185	R : 51 G : 138 B : 191	R : 63 G : 149 B : 200	R : 75 G : 157 B : 205
3	R : 57 G : 144 B : 197	R : 57 G : 144 B : 197	R : 55 G : 142 B : 195	R : 52 G : 139 B : 192	R : 50 G : 137 B : 190	R : 51 G : 138 B : 191	R : 56 G : 142 B : 193	R : 63 G : 145 B : 193

4	R : 48 G : 142 B : 196	R : 48 G : 142 B : 196	R : 47 G : 142 B : 198	R : 46 G : 141 B : 197	R : 43 G : 140 B : 195	R : 42 G : 139 B : 194	R : 41 G : 138 B : 193	R : 43 G : 136 B : 193
5	R : 51 G : 145 B : 199	R : 49 G : 143 B : 197	R : 46 G : 141 B : 197	R : 44 G : 139 B : 195	R : 42 G : 139 B : 194	R : 42 G : 139 B : 194	R : 42 G : 139 B : 194	R : 44 G : 137 B : 194
6	R : 43 G : 141 B : 188	R : 41 G : 139 B : 186	R : 38 G : 136 B : 183	R : 37 G : 135 B : 182	R : 35 G : 135 B : 184	R : 36 G : 136 B : 185	R : 35 G : 137 B : 186	R : 34 G : 136 B : 185
7	R : 43 G : 141 B : 188	R : 43 G : 141 B : 188	R : 43 G : 141 B : 188	R : 45 G : 143 B : 190	R : 44 G : 144 B : 193	R : 43 G : 143 B : 192	R : 39 G : 141 B : 190	R : 36 G : 138 B : 187

After obtaining the ciphertext results from Rot 13 encryption, the ciphertext will be processed again using the Beaufort Cipher algorithm.

3.2. Beaufort Cipher Algorithm Encryption Calculation

The following are the steps for encrypting the application of the Beaufort cipher algorithm, which are as follows:

1. Specify the message (plaintext) to be encrypted and the key.
   Plaintext = Result value from Rot13 encryption

Table 3: Plaintext Algoritma Beaufort cipher

Pixel (0,0) :	**Pixel (0,1) :**	**Pixel (0,2) :**	**Pixel (0,3) :**	**Pixel (0,4) :**	**Pixel (0,5) :**	**Pixel (0,6) :**	**Pixel (0,7) :**
R : 114	R : 122	R : 132	R : 137	R : 137	R : 137	R : 144	R : 151
G : 195	G : 203	G : 213	G : 218	G : 219	G : 219	G : 223	G : 227
B : 240	B : 248	B : 0	B : 5	B : 3	B : 3	B : 6	B : 7
Pixel (1,0) :	**Pixel (1,1) :**	**Pixel (1,2) :**	**Pixel (1,3) :**	**Pixel (1,4) :**	**Pixel (1,5) :**	**Pixel (1,6) :**	**Pixel (1,7) :**
R : 71	R : 73	R : 74	R : 72	R : 71	R : 76	R : 89	R : 101
G : 152	G : 154	G : 155	G : 153	G : 153	G : 158	G : 168	G : 177
B : 197	B : 199	B : 198	B : 196	B : 193	B : 198	B : 207	B : 213
Pixel (2,0) :	**Pixel (2,1) :**	**Pixel (2,2) :**	**Pixel (2,3) :**	**Pixel (2,4) :**	**Pixel (2,5) :**	**Pixel (2,6) :**	**Pixel (2,7) :**
R : 57	R : 56	R : 52	R : 47	R : 45	R : 51	R : 63	R : 75
G : 144	G : 143	G : 139	G : 134	G : 132	G : 138	G : 149	G : 157
B : 197	B : 196	B : 192	B : 187	B : 185	B : 191	B : 200	B : 205
Pixel (3,0) :	**Pixel (3,1) :**	**Pixel (3,2) :**	**Pixel (3,3) :**	**Pixel (3,4) :**	**Pixel (3,5) :**	**Pixel (3,6) :**	**Pixel (3,7) :**
R : 57	R : 57	R : 55	R : 52	R : 50	R : 51	R : 56	R : 63
G : 144	G : 144	G : 142	G : 139	G : 137	G : 138	G : 142	G : 145
B : 197	B : 197	B : 195	B : 192	B : 190	B : 191	B : 193	B : 193
Pixel (4,0) :	**Pixel (4,1) :**	**Pixel (4,2) :**	**Pixel (4,3) :**	**Pixel (4,4) :**	**Pixel (4,5) :**	**Pixel (4,6) :**	**Pixel (4,7) :**
R : 48	R : 48	R : 47	R : 46	R : 43	R : 42	R : 41	R : 43
G : 142	G : 142	G : 142	G : 141	G : 140	G : 139	G : 138	G : 136
B : 196	B : 196	B : 198	B : 197	B : 195	B : 194	B : 193	B : 193
Pixel (5,0) :	**Pixel (5,1) :**	**Pixel (5,2) :**	**Pixel (5,3) :**	**Pixel (5,4) :**	**Pixel (5,5) :**	**Pixel (5,6) :**	**Pixel (5,7) :**
R : 51	R : 49	R : 46	R : 44	R : 42	R : 42	R : 42	R : 44
G : 145	G : 143	G : 141	G : 139	G : 139	G : 139	G : 139	G : 137
B : 199	B : 197	B : 197	B : 195	B : 194	B : 194	B : 194	B : 194
Pixel (6,0) :	**Pixel (6,1) :**	**Pixel (6,2) :**	**Pixel (6,3) :**	**Pixel (6,4) :**	**Pixel (6,5) :**	**Pixel (6,6) :**	**Pixel (6,7) :**
R : 43	R : 41	R : 38	R : 37	R : 35	R : 36	R : 35	R : 34
G : 141	G : 139	G : 136	G : 135	G : 135	G : 136	G : 137	G : 136
B : 188	B : 186	B : 183	B : 182	B : 184	B : 185	B : 186	B : 185
Pixel (7,0) :	**Pixel (7,1) :**	**Pixel (7,2) :**	**Pixel (7,3) :**	**Pixel (7,4) :**	**Pixel (7,5) :**	**Pixel (7,6) :**	**Pixel (7,7) :**
R : 43	R : 43	R : 43	R : 45	R : 44	R : 43	R : 39	R : 36
G : 141	G : 141	G : 141	G : 143	G : 144	G : 143	G : 141	G : 138
B : 188	B : 188	B : 188	B : 190	B : 193	B : 192	B : 190	B : 187

Beaufort cipher key = AYUDEVIA
With Formula: $\mathbf{C_i = (K_i - P_i)}$

2. Convert the key into the decimal ASCII code that represents the letter

Table 4: Convert Beaufort Encryption Key To Decimal Value

Character	A	Y	U	D	E	V	I	A
Decimal	65	89	85	68	69	86	73	65

3. Encrypt the calculation using the formula Ci = (Ki – Pi) mod 256 then check the subtraction result, if the subtraction result is less than 0 then the subtraction result is added to 256.
   Then the image encryption process using the Beaufort cipher algorithm is as follows:
   Pixel (0,0) =
   Red= (65 – 114) = -49 Mod 256 = 207
   Green = (89 – 195) = -106 Mod 256 = 150
   Blue = (85 – 240) = -155 Mod 256 = 101

Pixel (0,1) =
Red= (68 – 122) = -54 Mod 256 = 202
Green = (69 – 203) = -134 Mod 256 = 122
Blue = (86 – 248) = -162 Mod 256 = 94
Pixel (0,2) =
Red= (73 – 132) = -59 Mod 256 = 197
Green = (65 – 213) = -148 Mod 256 = 108
Blue = (65 – 256) = -191 Mod 256 = 65
Pixel (0,3) =
Red= (89 – 137) = -48 Mod 256 = 208
Green = (85 – 218) = -133 Mod 256 = 123
Blue = (68 – 5) = 63 Mod 256 = 63
Pixel (0,4) =
Red= (69 – 137) = -68 Mod 256 = 188
Green = (86 – 219) = -133 Mod 256 = 123
Blue = (73 – 3) = 70 Mod 256 = 70
Pixel (0,5) =
Red= (65 – 137) = -72 Mod 256 = 184
Green = (65 – 219) = -154 Mod 256 = 102
Blue = (89 – 3) = 86 Mod 256 = 86
Pixel (0,6) =
Red= (85 – 144) = -59 Mod 256 = 197
Green = (68 – 223) = -155 Mod 256 = 101
Blue = (69 – 6) = 63 Mod 256 = 63
Pixel (0,7) =
Red= (86 – 151) = -65 Mod 256 = 191
Green = (73 – 227) = -154 Mod 256 = 102
Blue = (65 – 7) = 58 Mod 256 = 58

The calculation process continues until the end of the pixel value contained in table III.3. Then it can be obtained from the results of the Beaufort Cipher Algorithm encryption process as follows:

Table 5: Beaufort Cipher Algorithm Encryption Results

Pixel (0,0) :	**Pixel (0,1) :**	**Pixel (0,2) :**	**Pixel (0,3) :**	**Pixel (0,4) :**	**Pixel (0,5) :**	**Pixel (0,6) :**	**Pixel (0,7) :**
R : 207	R : 202	R : 197	R : 208	R : 188	R : 184	R : 197	R : 191
G : 150	G : 122	G : 108	G : 123	G : 123	G : 102	G : 101	G : 102
B : 101	B : 94	B : 65	B : 63	B : 70	B : 86	B : 63	B : 58
Pixel (1,0) :	**Pixel (1,1) :**	**Pixel (1,2) :**	**Pixel (1,3) :**	**Pixel (1,4) :**	**Pixel (1,5) :**	**Pixel (1,6) :**	**Pixel (1,7) :**
R : 250	R : 251	R : 255	R : 17	R : 254	R : 245	R : 252	R : 241
G : 193	G : 171	G : 166	G : 188	G : 189	G : 163	G : 156	G : 152
B : 144	B : 143	B : 123	B : 128	B : 136	B : 147	B : 118	B : 108
Pixel (2,0) :	**Pixel (2,1) :**	**Pixel (2,2) :**	**Pixel (2,3) :**	**Pixel (2,4) :**	**Pixel (2,5) :**	**Pixel (2,6) :**	**Pixel (2,7) :**
R : 8	R : 12	R : 21	R : 42	R : 24	R : 14	R : 22	R : 11
G : 201	G : 182	G : 182	G : 207	G : 210	G : 183	G : 175	G : 172
B : 144	B : 146	B : 129	B : 137	B : 144	B : 154	B : 125	B : 116
Pixel (3,0) :	**Pixel (3,1) :**	**Pixel (3,2) :**	**Pixel (3,3) :**	**Pixel (3,4) :**	**Pixel (3,5) :**	**Pixel (3,6) :**	**Pixel (3,7) :**
R : 8	R : 11	R : 18	R : 37	R : 19	R : 14	R : 29	R : 23
G : 201	G : 181	G : 179	G : 202	G : 205	G : 183	G : 182	G : 184
B : 144	B : 145	B : 126	B : 132	B : 139	B : 154	B : 132	B : 128
Pixel (4,0) :	**Pixel (4,1) :**	**Pixel (4,2) :**	**Pixel (4,3) :**	**Pixel (4,4) :**	**Pixel (4,5) :**	**Pixel (4,6) :**	**Pixel (4,7) :**
R : 17	R : 20	R : 26	R : 43	R : 26	R : 23	R : 44	R : 43
G : 203	G : 183	G : 179	G : 200	G : 202	G : 182	G : 186	G : 193
B : 145	B : 146	B : 123	B : 127	B : 134	B : 151	B : 132	B : 128
Pixel (5,0) :	**Pixel (5,1) :**	**Pixel (5,2) :**	**Pixel (5,3) :**	**Pixel (5,4) :**	**Pixel (5,5) :**	**Pixel (5,6) :**	**Pixel (5,7) :**
R : 11	R : 19	R : 27	R : 45	R : 27	R : 23	R : 43	R : 42
G : 200	G : 182	G : 180	G : 202	G : 203	G : 182	G : 185	G : 192
B : 142	B : 145	B : 124	B : 129	B : 135	B : 151	B : 131	B : 127
Pixel (6,0) :	**Pixel (6,1) :**	**Pixel (6,2) :**	**Pixel (6,3) :**	**Pixel (6,4) :**	**Pixel (6,5) :**	**Pixel (6,6) :**	**Pixel (6,7) :**
R : 22	R : 27	R : 35	R : 52	R : 34	R : 29	R : 50	R : 52
G : 204	G : 186	G : 185	G : 206	G : 207	G : 185	G : 187	G : 193
B : 153	B : 156	B : 138	B : 142	B : 145	B : 160	B : 139	B : 136
Pixel (7,0) :	**Pixel (7,1) :**	**Pixel (7,2) :**	**Pixel (7,3) :**	**Pixel (7,4) :**	**Pixel (7,5) :**	**Pixel (7,6) :**	**Pixel (7,7) :**
R : 22	R : 25	R : 30	R : 44	R : 25	R : 22	R : 46	R : 50
G : 204	G : 184	G : 180	G : 198	G : 198	G : 178	G : 183	G : 191
B : 153	B : 154	B : 133	B : 134	B : 136	B : 153	B : 135	B : 134

After obtaining the ciphertext results from the Beaufort Cipher encryption, the next process is to decrypt the ciphertext using the Beaufort Cipher algorithm.

Calculation of the Beaufort Cipher Algorithm Decryption, The following are the steps for the description of the application of the Beaufort cipher algorithm, which are as follows:

1. Specify the message (Ciphertext) to be decrypted and key.

Ciphertext = value result from Beaufort Cipher encryption

Tabel 6: Ciphertext Algoritma Beaufort Cipher

Pixel (0,0) :	**Pixel (0,1) :**	**Pixel (0,2) :**	**Pixel (0,3) :**	**Pixel (0,4) :**	**Pixel (0,5) :**	**Pixel (0,6) :**	**Pixel (0,7) :**
R : 207	R : 202	R : 197	R : 208	R : 188	R : 184	R : 197	R : 191
G : 150	G : 122	G : 108	G : 123	G : 123	G : 102	G : 101	G : 102
B : 101	B : 94	B : 65	B : 63	B : 70	B : 86	B : 63	B : 58
Pixel (1,0) :	**Pixel (1,1) :**	**Pixel (1,2) :**	**Pixel (1,3) :**	**Pixel (1,4) :**	**Pixel (1,5) :**	**Pixel (1,6) :**	**Pixel (1,7) :**
R : 250	R : 251	R : 255	R : 17	R : 254	R : 245	R : 252	R : 241
G : 193	G : 171	G : 166	G : 188	G : 189	G : 163	G : 156	G : 152
B : 144	B : 143	B : 123	B : 128	B : 136	B : 147	B : 118	B : 108
Pixel (2,0) :	**Pixel (2,1) :**	**Pixel (2,2) :**	**Pixel (2,3) :**	**Pixel (2,4) :**	**Pixel (2,5) :**	**Pixel (2,6) :**	**Pixel (2,7) :**
R : 8	R : 12	R : 21	R : 42	R : 24	R : 14	R : 22	R : 11
G : 201	G : 182	G : 182	G : 207	G : 210	G : 183	G : 175	G : 172
B : 144	B : 146	B : 129	B : 137	B : 144	B : 154	B : 125	B : 116
Pixel (3,0) :	**Pixel (3,1) :**	**Pixel (3,2) :**	**Pixel (3,3) :**	**Pixel (3,4) :**	**Pixel (3,5) :**	**Pixel (3,6) :**	**Pixel (3,7) :**
R : 8	R : 11	R : 18	R : 37	R : 19	R : 14	R : 29	R : 23
G : 201	G : 181	G : 179	G : 202	G : 205	G : 183	G : 182	G : 184
B : 144	B : 145	B : 126	B : 132	B : 139	B : 154	B : 132	B : 128
Pixel (4,0) :	**Pixel (4,1) :**	**Pixel (4,2) :**	**Pixel (4,3) :**	**Pixel (4,4) :**	**Pixel (4,5) :**	**Pixel (4,6) :**	**Pixel (4,7) :**
R : 17	R : 20	R : 26	R : 43	R : 26	R : 23	R : 44	R : 43
G : 203	G : 183	G : 179	G : 200	G : 202	G : 182	G : 186	G : 193
B : 145	B : 146	B : 123	B : 127	B : 134	B : 151	B : 132	B : 128
Pixel (5,0) :	**Pixel (5,1) :**	**Pixel (5,2) :**	**Pixel (5,3) :**	**Pixel (5,4) :**	**Pixel (5,5) :**	**Pixel (5,6) :**	**Pixel (5,7) :**
R : 11	R : 19	R : 27	R : 45	R : 27	R : 23	R : 43	R : 42
G : 200	G : 182	G : 180	G : 202	G : 203	G : 182	G : 185	G : 192
B : 142	B : 145	B : 124	B : 129	B : 135	B : 151	B : 131	B : 127
Pixel (6,0) :	**Pixel (6,1) :**	**Pixel (6,2) :**	**Pixel (6,3) :**	**Pixel (6,4) :**	**Pixel (6,5) :**	**Pixel (6,6) :**	**Pixel (6,7) :**
R : 22	R : 27	R : 35	R : 52	R : 34	R : 29	R : 50	R : 52
G : 204	G : 186	G : 185	G : 206	G : 207	G : 185	G : 187	G : 193
B : 153	B : 156	B : 138	B : 142	B : 145	B : 160	B : 139	B : 136
Pixel (7,0) :	**Pixel (7,1) :**	**Pixel (7,2) :**	**Pixel (7,3) :**	**Pixel (7,4) :**	**Pixel (7,5) :**	**Pixel (7,6) :**	**Pixel (7,7) :**
R : 22	R : 25	R : 30	R : 44	R : 25	R : 22	R : 46	R : 50
G : 204	G : 184	G : 180	G : 198	G : 198	G : 178	G : 183	G : 191
B : 153	B : 154	B : 133	B : 134	B : 136	B : 153	B : 135	B : 134

Beaufort cipher key = AYUDEVIA
With Formula: $\mathbf{P_i = (K_i - C_i) \bmod 256}$

2. Convert the key into the decimal ASCII code that represents

Table 7: Convert Beaufort Decryption Key Into Decimal Value

Character	A	Y	U	D	E	V	I	A
Decimal	65	89	85	68	69	86	73	65

3. Description of the calculation using the formula Pi = (Ai – Ci) mot 256 then check the subtraction result, if the subtraction result is less than 0 then the subtraction result is added to 256. So the image decryption process using the Beaufort Cipher algorithm is as follows:

Pixel (0,0) =
Red = (65 – 207) = -142 Mod 256 = 114
Green = (89 – 150) = -61 Mod 256 = 195
Blue = (85 – 101) = -16 Mod 256 = 240
Pixel (0,1) =
Red = (68 – 202) = -134 Mod 256 = 122
Green = (69 – 122) = -53 Mod 256 = 203
Blue = (86 – 94) = -8 Mod 256 = 248
Pixel (0,2) =
Red = (73 – 197) = -124 Mod 256 = 132
Green = (65 – 108) = -43 Mod 256 = 213
Blue = (65 – 65) = 0 Mod 256 = 0
Pixel (0,3) =
Red = (89 – 208) = -119 Mod 256 = 137
Green = (85 – 123) = -38 Mod 256 = 218
Blue = (68 – 63) = 5 Mod 256 = 5
Pixel (0,4) =
Red = (69 – 188) = -119 Mod 256 = 137
Green = (86 – 123) = -37 Mod 256 = 219
Blue = (73 – 70) = 3 Mod 256 = 3
Pixel (0,5) =
Red = (65 – 184) = -119 Mod 256 = 137
Green = (65 – 102) = -37 Mod 256 = 219
Blue = (89 – 86) = 3 Mod 256 = 3
Pixel (0,6) =

Red = (85 – 197) = -112 Mod 256 = 144
Green = (68 – 101) = -33 Mod 256 = 223
Blue = (69 – 63) = 6 Mod 256 = 6
Pixel (0,7) =
Red = (86 – 191) = -105 Mod 256 = 151
Green = (73 – 102) = -29 Mod 256 = 227
Blue = (65 – 58) = 7 Mod 256 = 7
The calculation process continues until the end of the pixel value contained in table III.6. Then it can be obtained from the results of the Beaufort Cipher Algorithm Decryption process as follows:

Table 8: Beaufort Algorithm Decryption Results

Pixel (0,0) :	**Pixel (0,1) :**	**Pixel (0,2) :**	**Pixel (0,3) :**	**Pixel (0,4) :**	**Pixel (0,5) :**	**Pixel (0,6) :**	**Pixel (0,7) :**
R : 114	R : 122	R : 132	R : 137	R : 137	R : 137	R : 144	R : 151
G : 195	G : 203	G : 213	G : 218	G : 219	G : 219	G : 223	G : 227
B : 240	B : 248	B : 0	B : 5	B : 3	B : 3	B : 6	B : 7
Pixel (1,0) :	**Pixel (1,1) :**	**Pixel (1,2) :**	**Pixel (1,3) :**	**Pixel (1,4) :**	**Pixel (1,5) :**	**Pixel (1,6) :**	**Pixel (1,7) :**
R : 71	R : 73	R : 74	R : 72	R : 71	R : 76	R : 89	R : 101
G : 152	G : 154	G : 155	G : 153	G : 153	G : 158	G : 168	G : 177
B : 197	B : 199	B : 198	B : 196	B : 193	B : 198	B : 207	B : 213
Pixel (2,0) :	**Pixel (2,1) :**	**Pixel (2,2) :**	**Pixel (2,3) :**	**Pixel (2,4) :**	**Pixel (2,5) :**	**Pixel (2,6) :**	**Pixel (2,7) :**
R : 57	R : 56	R : 52	R : 47	R : 45	R : 51	R : 63	R : 75
G : 144	G : 143	G : 139	G : 134	G : 132	G : 138	G : 149	G : 157
B : 197	B : 196	B : 192	B : 187	B : 185	B : 191	B : 200	B : 205
Pixel (3,0) :	**Pixel (3,1) :**	**Pixel (3,2) :**	**Pixel (3,3) :**	**Pixel (3,4) :**	**Pixel (3,5) :**	**Pixel (3,6) :**	**Pixel (3,7) :**
R : 57	R : 57	R : 55	R : 52	R : 50	R : 51	R : 56	R : 63
G : 144	G : 144	G : 142	G : 139	G : 137	G : 138	G : 142	G : 145
B : 197	B : 197	B : 195	B : 192	B : 190	B : 191	B : 193	B : 193
Pixel (4,0) :	**Pixel (4,1) :**	**Pixel (4,2) :**	**Pixel (4,3) :**	**Pixel (4,4) :**	**Pixel (4,5) :**	**Pixel (4,6) :**	**Pixel (4,7) :**
R : 48	R : 48	R : 47	R : 46	R : 43	R : 42	R : 41	R : 43
G : 142	G : 142	G : 142	G : 141	G : 140	G : 139	G : 138	G : 136
B : 196	B : 196	B : 198	B : 197	B : 195	B : 194	B : 193	B : 193
Pixel (5,0) :	**Pixel (5,1) :**	**Pixel (5,2) :**	**Pixel (5,3) :**	**Pixel (5,4) :**	**Pixel (5,5) :**	**Pixel (5,6) :**	**Pixel (5,7) :**
R : 51	R : 49	R : 46	R : 44	R : 42	R : 42	R : 42	R : 44
G : 145	G : 143	G : 141	G : 139	G : 139	G : 139	G : 139	G : 137
B : 199	B : 197	B : 197	B : 195	B : 194	B : 194	B : 194	B : 194
Pixel (6,0) :	**Pixel (6,1) :**	**Pixel (6,2) :**	**Pixel (6,3) :**	**Pixel (6,4) :**	**Pixel (6,5) :**	**Pixel (6,6) :**	**Pixel (6,7) :**
R : 43	R : 41	R : 38	R : 37	R : 35	R : 36	R : 35	R : 34
G : 141	G : 139	G : 136	G : 135	G : 135	G : 136	G : 137	G : 136
B : 188	B : 186	B : 183	B : 182	B : 184	B : 185	B : 186	B : 185
Pixel (7,0) :	**Pixel (7,1) :**	**Pixel (7,2) :**	**Pixel (7,3) :**	**Pixel (7,4) :**	**Pixel (7,5) :**	**Pixel (7,6) :**	**Pixel (7,7) :**
R : 43	R : 43	R : 43	R : 45	R : 44	R : 43	R : 39	R : 36
G : 141	G : 141	G : 141	G : 143	G : 144	G : 143	G : 141	G : 138
B : 188	B : 188	B : 188	B : 190	B : 193	B : 192	B : 190	B : 187

Setelah didapat hasil plaintext dari dekripsi Beaufort Cipher selesai maka proses selanjutnya plaintext tersebut akan di dekripsikan kembali menggunakan algoritma Rot 13.

3.4. Rot 13 Algorithm Decryption Process

The value to be processed is the result of the decryption process of the Beaufort Cipher algorithm.
Ciphertext =

Table 9: Rot13 Algorithm Ciphertext

(x,y)	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	R : 114	R : 122	R : 132	R : 137	R : 137	R : 137	R : 144	R : 151
	G : 195	G : 203	G : 213	G : 218	G : 219	G : 219	G : 223	G : 227
	B : 240	B : 248	B : 0	B : 5	B : 3	B : 3	B : 6	B : 7
1	R : 71	R : 73	R : 74	R : 72	R : 71	R : 76	R : 89	R : 101
	G : 152	G : 154	G : 155	G : 153	G : 153	G : 158	G : 168	G : 177
	B : 197	B : 199	B : 198	B : 196	B : 193	B : 198	B : 207	B : 213
2	R : 57	R : 56	R : 52	R : 47	R : 45	R : 51	R : 63	R : 75
	G : 144	G : 143	G : 139	G : 134	G : 132	G : 138	G : 149	G : 157
	B : 197	B : 196	B : 192	B : 187	B : 185	B : 191	B : 200	B : 205
3	R : 57	R : 57	R : 55	R : 52	R : 50	R : 51	R : 56	R : 63
	G : 144	G : 144	G : 142	G : 139	G : 137	G : 138	G : 142	G : 145
	B : 197	B : 197	B : 195	B : 192	B : 190	B : 191	B : 193	B : 193
4	R : 48	R : 48	R : 47	R : 46	R : 43	R : 42	R : 41	R : 43
	G : 142	G : 142	G : 142	G : 141	G : 140	G : 139	G : 138	G : 136
	B : 196	B : 196	B : 198	B : 197	B : 195	B : 194	B : 193	B : 193
5	R : 51	R : 49	R : 46 G :	R : 44	R : 42	R : 42	R : 42	R : 44
	G : 145	G : 143	141	G : 139	G : 139	G : 139	G : 139	G : 137
	B : 199	B : 197	B : 197	B : 195	B : 194	B : 194	B : 194	B : 194

6	R : 43 G : 141 B : 188	R : 41 G : 139 B : 186	R : 38 G : 136 B : 183	R : 37 G : 135 B : 182	R : 35 G : 135 B : 184	R : 36 G : 136 B : 185	R : 35 G : 137 B : 186	R : 34 G : 136 B : 185
7	R : 43 G : 141 B : 188	R : 43 G : 141 B : 188	R : 43 G : 141 B : 188	R : 45 G : 143 B : 190	R : 44 G : 144 B : 193	R : 43 G : 143 B : 192	R : 39 G : 141 B : 190	R : 36 G : 138 B : 187

The decryption process uses the Rot 13 Algorithm by processing the resulting value in table III.9 which is the Ciphertext by shifting the value backwards 13 times and the shift is based on the order of the ASCII table, namely as follows:

- The value of R in the table row 0 column 0 = 114 then it is shifted backwards 13 times = 101
- The value of G in the table row 0 column 0 = 195 then it is shifted backwards 13 times = 182
- Value B in table row 0 column 0 = 240 then it is shifted backwards 13 times = 227
- The value of R in the table row 0 column 1 = 122 then it is shifted backwards 13 times = 109
- The value of G in the table row 0 column 1 = 203 then it is shifted backwards 13 times = 190
- Value B in table row 0 column 1 = 248 then it is shifted backwards 13 times = 235
- The value of R in the table row 0 column 2 = 132 then it is shifted backwards 13 times = 119
- The value of G in the table row 0 column 2 = 213 then it is shifted backwards 13 times = 200
- Value B in table row 0 column 2 = 0 then it is shifted backwards 13 times = 243
- The value of R in the table row 0 column 3 = 137 then it is shifted backwards 13 times = 124
- The value of G in the table row 0 column 3 = 218 then it is shifted backwards 13 times = 205
- Value B in table row 0 column 3 = 5 then it is shifted backwards 13 times = 248
- The value of R in the table row 0 column 4 = 137 then it is shifted backwards 13 times = 124
- The value of G in the table row 0 column 4 = 219 then it is shifted backwards 13 times = 206
- Value B in table row 0 column 4 = 3 then it is shifted backwards 13 times = 246
- The value of R in the table row 0 column 5 = 137 then it is shifted backwards 13 times = 124
- The value of G in the table row 0 column 5 = 219 then it is shifted backwards 13 times = 206
- Value B in table row 0 column 5 = 3 then it is shifted backwards 13 times = 246
- The value of R in the table row 0 column 6 = 144 then it is shifted backwards 13 times = 131
- The value of G in the table row 0 column 6 = 223 then it is shifted backwards 13 times = 210
- Value B in table row 0 column 6 = 6 then it is shifted backwards 13 times = 249
- The value of R in the table row 0 column 7 = 151 then it is shifted backwards 13 times = 138
- The value of G in the table row 0 column 7 = 227 then it is shifted backwards 13 times = 214
- Value B in table row 0 column 7 = 7 then it is shifted backwards 13 times = 250

The calculation process continues until the end of the pixel value contained in table 10. Then it can be obtained from the results of the Rot 13 Algorithm Decryption process as follows:

Table 10: Rot 13 Algorithm Decryption Value Results

(x,y)	0	1	2	3	4	5	6	7
0	R : 101 G : 182 B : 227	R : 109 G : 190 B : 235	R : 119 G : 200 B : 243	R : 124 G : 205 B : 248	R : 124 G : 206 B : 246	R : 124 G : 206 B : 246	R : 131 G : 210 B : 249	R : 138 G : 214 B : 250
1	R : 58 G : 139 B : 184	R : 60 G : 141 B : 186	R : 61 G : 142 B : 185	R : 59 G : 140 B : 183	R : 58 G : 140 B : 180	R : 63 G : 145 B : 185	R : 76 G : 155 B : 194	R : 88 G : 164 B : 200
2	R : 44 G : 131 B : 184	R : 43 G : 130 B : 183	R : 39 G : 126 B : 179	R : 34 G : 121 B : 174	R : 32 G : 119 B : 172	R : 38 G : 125 B : 178	R : 50 G : 136 B : 187	R : 62 G : 144 B : 192
3	R : 44 G : 131 B : 184	R : 44 G : 131 B : 184	R : 42 G : 129 B : 182	R : 39 G : 126 B : 179	R : 37 G : 124 B : 177	R : 38 G : 125 B :178	R : 43 G : 129 B : 180	R : 50 G : 132 B : 180
4	R : 35 G : 129 B : 183	R : 35 G : 129 B : 183	R : 34 G : 129 B : 185	R : 33 G : 128 B : 184	R : 30 G : 127 B : 182	R : 29 G : 126 B : 181	R : 28 G : 125 B : 180	R : 30 G : 123 B : 180
5	R : 38 G : 132 B : 186	R : 36 G : 130 B : 184	R : 33 G : 128 B : 184	R : 31 G : 126 B : 182	R : 29 G : 126 B : 181	R : 29 G : 126 B : 181	R : 29 G : 126 B : 181	R : 31 G : 124 B : 181
6	R : 30 G : 128 B : 175	R : 28 G : 126 B : 173	R : 25 G : 123 B : 170	R : 24 G : 122 B : 169	R : 22 G : 122 B : 171	R : 23 G : 123 B : 171	R : 22 G : 124 B : 173	R : 21 G : 123 B : 172
7	R : 30 G : 128 B : 175	R : 30 G : 128 B : 175	R : 30 G : 128 B : 175	R : 32 G : 130 B : 177	R : 31 G : 131 B : 180	R : 30 G : 130 B : 179	R : 26 G : 128 B : 177	R : 23 G : 125 B : 174

4. Discussion

The stages that the authors do is the design of the software interface. So in this discussion, we will discuss some of the views of the existing menus using the Rot 13 and Beaufort Cipher algorithms, as follows:

4.1. Main Form

The main form is the display form which acts as an opening in the application process

Figure 2: Main Form

4.2. Encryption Form

The form of this encryption can be seen to retrieve the image by clicking the Browser button (search) and the image and file name will appear, then Rot 13 encryption, then click the process button on Rot 13, then the image will move to Beaufort Cipher and enter the key for Beaufort Cipher encryption and encryption results are successful, then click save.

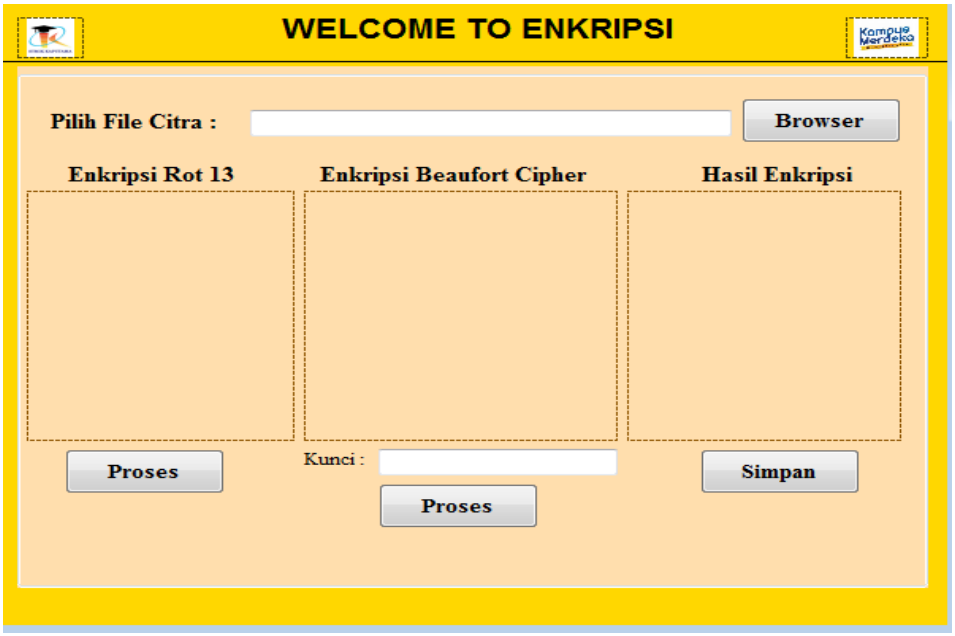

Figure 3: Encryption Form Design

4.3. Description Form

In this decryption form, you can see that you can retrieve the image by clicking on the Browser button (search) and an image will appear along with the name of the file that was encrypted earlier, then enter the key for decryption, then click the process button on Beaufort Cipher, then the image moves to Rot 13. the decryption results return to the original image, then click save.

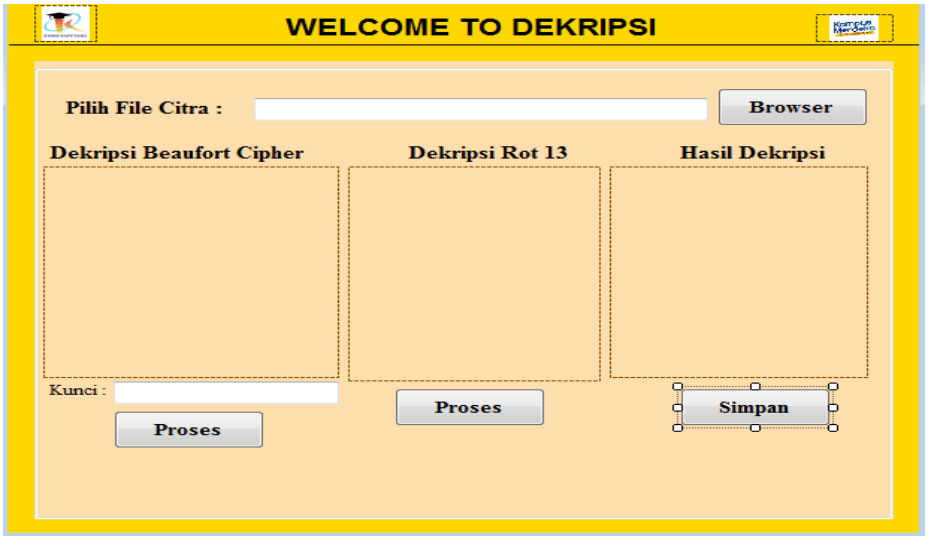

Figure 3: Design of the Decryption Form

5. Conclusion

With this digital image encryption and decryption application system, the authors can draw the following conclusions:

1. Combining these two algorithms can provide a higher level of security than using each algorithm separately. The combination of ROT13 and Beaufort Cipher creates a multiplexed encryption algorithm that complicates the decryption process for parties who do not have the secret key. This makes digital images safer from attacks and cryptanalytic cracking attempts.
2. Combining the ROT13 and Beaufort Cipher algorithms creates complexity in the encryption method. The process of repeating encryption more than once with different algorithms confuses the letter patterns that may exist in digital images, making it more difficult to predict or analyze and By using both algorithms simultaneously, attacks on digital images will be more difficult because the attacker must successfully crack both encryption simultaneously. This increases overall security and provides an additional layer of protection.
3. The combination of two cryptographic algorithms, namely ROT13 and Beaufort Cipher, in the super encryption method shows the potential to provide a stronger layer of security. This combination can increase resistance to different types of attacks and create a greater challenge for attackers.

References

[1] A, A. A. R. P. W., Maulana, M. H., Andini, C. D., Nadziroh, F., & Semen, K. (2018). ONLINE ROOM BORROWING SYSTEM (SPRO) WITH UML METHOD (UNFIELD MODELING LANGUAGE) Abstract The process of borrowing a room is done manually , which is Akademi Komunitas Semen. 1(1), 1–8.

[2] Aresta, R. M., Pratomo, E. W., Geraldino, V., Santoso, J. D., & Mulyatun, S. (2020). Implementation of Multi Encryption Rot 13 on the Whatsapp Symbol. Journal of Information System Management (JOISM), 2(1), 1–5. https://doi.org/10.24076/joism.2020v2i1.158

[3] Asraidah Linga. (2019). Analysis of the Implementation of Wav Audio File Security Applications by Applying the Beaufort Cipher and Root Algorithms 13. Journal of Pelita Informatics, 8, 33–40.

[4] HUTABARAT, J. (2018). Implementation of Rot13 Algorithm and Caesar Ciper in Web-Based Text Encoding. 13(Rotate 13), 38–41. http://repository.potential-utama.ac.id/jspui/handle/123456789/3242

[5] Josi, A. (2017). Application of the Prototyping Method in Building Village Websites (Case Study of Sugihan Village, Rambang District). Jti, 9(1), 50–57.

[6] Maria, R., Br, U., Fauzi, A., Sembiring, H., & Utara, S. (2021). VIGENERE CIPHER AND ONE TIME PAD ALGORITHM COMBINATION. 5(1), 137–146.

[7] Ndruru, E., & Zebua, T. (2022). Generation of Beaufort Cipher Keys Using the Blum-blum Shub Technique in Digital Image Security. Bulletin of Information Technology (BIT), 3(2), 149–154.

[8] Rachmadsyah, A., Perdana, A., & Budiman, A. (2020). Combination of Beaufort Cipher and Vigenere Cipher Algorithms for Mobile Application-Based Text Message Security. Polgan Minfo Journal, 9(2), 12–17.

[9] Rachmancto, A. (2021). Information Technology Sophistication and User Participation Impact on the Effectiveness of Accounting Information Systems. Nuevos Sistemas de Comunicación e Información, 2013–2015.

[10] Siregar, H. F., Siregar, Y. H., & Melani, M. (2018). (2018). Multimedia-Based Hadith Comic Application Design. JurTI (Information Technology Journal), 2(2), 113-121. JurTI (Information Technology Journal), 2(2), 113–121. http://www.jurnal.una.ac.id/index.php/jurti/article/view/425