Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

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

Super Encryption Feal Algorithm and Base64 Algorithm Image File Security

Tiara Br Bangun[1], Achmad Fauzi[2], I Gusti Prahmana[3]

[1,2,3] *STMIK Kaputama Binjai*
tiarabrbangun8@gmail.com [1], *fauzyrivai88@gmail.com* [2], *igustiprahmana4@gmail.com* [3],

Abstract

In the rapidly advancing digital era, image file security has become a critical issue, especially with the increasing risks of data breaches and attacks on digital files. This study aims to enhance the security of image files by implementing a combination of two cryptographic algorithms: Fast Data Encipherment Algorithm- 4 (FEAL-4) and Base64. FEAL-4 is a symmetric encryption algorithm known for its high speed and processing efficiency, while Base64 is used for encoding binary data into ASCII format to ensure safer transmission. This research develops a super encryption system that integrates these two algorithms to protect the integrity and confidentiality of image files, particularly for BMP, JPEG, and PNG formats. The implementation was carried out using the Visual Basic programming language. The results of the study show that the combination of FEAL-4 and Base64 algorithms significantly enhances the security of image files, with a high success rate in the encryption and decryption processes.

Keyword: *Security, Image Files, Algorithms, FEAL-4, Base64, Cryptography*

1. Introduction

Image files often contain sensitive or confidential information, such as personal data, company documents, or medical data. Weaknesses in the protection of the integrity and confidentiality of image files can result in great losses for the individuals or organizations concerned. To strengthen the background of the problem, the authors include journals related to the FEAL algorithm and the Base64 algorithm. Base64 algorithm in the context of cryptography and encryption has the disadvantage that base64 is only an encoding method, so encoded data can be easily decoded without the need for a special key. In addition, base64 increases data size by about 33%, increasing storage space and bandwidth requirements. Base64 also has no mechanism to detect or prevent data modification, making it vulnerable to frequency analysis attacks and providing no protection against eavesdropping. The base64 encoding and decoding process can also be inefficient for large data.

Therefore, the Base6 algorithm must be combined with other algorithms, such as the FEAL-4 algorithm. FEAL-4 (Fast Data Encipherment Algorithm) is a variant of a data encryption algorithm that has a high speed in the encryption and decryption process, FEAL-4 has a data block length of 64 bits and a key of 64 bits, and uses 4 rounds of iterations for the encryption and decryption process. making it efficient for applications that require fast processing. FEAL-4's simple structure makes it easy to implement and maintain, and as a symmetric cryptographic algorithm, it uses the same key for encryption and decryption, simplifying key management.

2. Research Methods

There are several stages in completing this research, namely:

1. Research Preparation; This stage is the initial activity, namely by determining the background of the problem, then identifying the problem and then making a problem boundary that will help the author to the next stage.
2. Formulating Problems and Objectives; After looking for identification and problem boundaries, the author will formulate problems and objectives that will provide benefits to users.
3. Objectives of research;
   a. To implement a system used to secure image files from irresponsible parties.
   b. To produce a super encryption system using the FEAL-4 algorithm and the Base 64 algorithm for securing image files.
4. Benefits of research;
   a. This research improves the security of image files by applying FEAL-4 and Base 64 methods, protecting sensitive information from attacks and data leakage.
   b. The application of FEAL-4 and Base 64 methods in this research helps to maintain data integrity in image files, reducing the risk of unauthorized modification or manipulation of the information in these files.

c. This research contributes to the development of security technologies by exploring and applying new encryption and security methods to image files, expanding the understanding of protecting data in the context of image files.

2.1. Cryptography

Cryptography is the study of mathematical techniques that deal with aspects of information security such as confidence, data integrity, entity authentication and data authenticity. According to Menezes, Oorscho and Vanstonee, art is defined by the historical fact that everyone has their own way of securing data, so that messages have their own aesthetic value related to art and culture, if you look deeply Grafy in cryptography means an art. Security also requires techniques and art as well as security on data, the reliability of security depends on how each person understands the importance of the data.

2.2. FEAL-4 Algorithm

Fast Data Encipherment Algorithm-4 (FEAL-4) is an encryption method that uses a symmetric approach to protect data. It converts plain text into encrypted text that can only be read using the appropriate key. FEAL-4 has a data block length of 64 bits and a key of 64 bits, and uses 4 rounds of iterations for the encryption and decryption process. Despite its simple design and fast execution, the security of FEAL-4 is debatable as it is vulnerable to several cryptanalysis attacks, making it more suitable for applications that require a modest level of security.

Encryption Process Of FEAL-4

Plainteks: (54 49 41 52 41 42 47 4E) (kelipatan 8 karakter)
32-bit subkeys (K1¬¬, K2, …, K6):
00010203 04050607 08090A0B 0C0D0E0F 00020406 01030509

ENKRIPSI
i = L ⊕ K5 = 54 49 41 52 ⊕ 00 02 04 06 = 54 4B 45 54
j = i ⊕ (R ⊕ K6) = 54 4B 45 54 ⊕ (41 42 47 4E ⊕ 01 03 05 09)
j = 54 4B 45 54 ⊕ 40 41 42 47 = 14 0A 07 13
54 4B 45 54 14 0A 07 13

ROUND 1
k = j = 14 0A 07 13
j = i + f(j ⊕ K1) = 54 4B 45 54 ⊕ f(14 0A 07 13 ⊕ 00 01 02 03)
j = 54 4B 45 54 ⊕ f(14 0B 05 10)
j = 54 4B 45 54 ⊕ A3 D4 A7 E2
j = F7 9F E2 B6
i = k = 14 0A 07 13
14 0A 07 13 F7 9F E2 B6

RUMUS FEAL-4 ROUND FUNCTION
G0(a,b) = (a + b (mod 256)) <<< 2
G1(a,b) = (a + b + 1 (mod 256)) <<< 2
y1 = G1(x0 ⊕ x1, x2 ⊕ x3)
y2 = G1(y1, x2 ⊕ x3)
y0 = G0(x0, y1)
y3 = G1(y2, x3)

f(14 0B 05 10)

y1 = G1(14 ⊕ 0B, 05 ⊕ 10)
y1 = G1(1F, 15)
y1 = (1F + 15 + 1 (mod 256)) <<< 2
y1 = (31 + 21 + 1 (mod 256)) <<< 2
y1 = 53 <<< 2
y1 = 110101 <<< 2
y1 = 11010100
y1 = D4
y2 = G0(y1, 05 ⊕ 10)
y2 = G0(D4, 15)
y2 = (D4 + 15 (mod 256)) <<< 2
y2 = (212 + 21 (mod 256)) <<< 2
y2 = 233 <<< 2
y2 = 11101001 <<< 2
y2 = 10100111
y2 = A7
y0 = G0(x0, y1)
y0 = G0(14, D4)

y0 = (14 + D4 (mod 256)) <<< 2
y0 = (20 + 212 (mod 256)) <<< 2
y0 = 232 <<< 2
y0 = 11101000 <<< 2
y0 = 10100011
y0 = A3
y3 = G1(y2, x3)
y3 = G1(A7, 10)
y3 = (A7 + 10 + 1 (mod 256)) <<< 2
y3 = (167 + 16 + 1 (mod 256)) <<< 2
y3 = 184 <<< 2
y3 = 10111000 <<< 2
y3 = 11100010
y3 = E2
f(14 0B 05 10) = (y0, y1, y2, y3) = A3 D4 A7 E2

ROUND 2
k = j = F7 9F E2 B6
j = i + f(j ⊕ K1) = 14 0A 07 13 ⊕ f(F7 9F E2 B6 ⊕ 04 05 06 07)
j = 14 0A 07 13 ⊕ f(F3 9A E4 B1)
j = 54 4B 45 54 ⊕ C7 FE 4D FF
j = D3 F4 4A EC
i = k = F7 9F E2 B6
F7 9F E2 B6 D3 F4 4A EC

ROUND 3
k = j = D3 F4 4A EC
j = i + f(j ⊕ K1) = F7 9F E2 B6 ⊕ f(D3 F4 4A EC ⊕ 08 09 0A 0B)
j = F7 9F E2 B6 ⊕ f(DB FD 40 E7)
j = F7 9F E2 B6 ⊕ 58 3B 8B CD
j = AF A4 69 7B
i = k = D3 F4 4A EC
D3 F4 4A EC AF A4 69 7B

ROUND 4
k = j = AF A4 69 7B
j = i + f(j ⊕ K1) = D3 F4 4A EC ⊕ f(AF A4 69 7B ⊕ 0C 0D 0E 0F)
j = D3 F4 4A EC ⊕ f(A3 A9 67 74)
j = D3 F4 4A EC ⊕ 6C 78 2E 8E
j = BF 8C 64 62
i = k = AF A4 69 7B
AF A4 69 7B BF 8C 64 62

i = i ⊕ j
i = AF A4 69 7B ⊕ BF 8C 64 62
i = 10 28 0D 19
j = BF 8C 64 62

hasil ciphertext: j + i
hasil ciphertext: **BF 8C 64 62 10 28 0D 19**

Decryption Process of FEAL-4

Ciphertext: **BF 8C 64 62 10 28 0D 19**
Key: 00010203 04050607 08090A0B 0C0D0E0F 00020406 01030509

j = L
j = BF 8C 64 62
i = R ⊕ j
i = 10 28 0D 19 ⊕ BF 8C 64 62
i = AF A4 69 7B

ROUND 1
k = i = AF A4 69 7B
i = j ⊕ f(i ⊕ K4)
i = BF 8C 64 62 ⊕ f(AF A4 69 7B ⊕ 0C 0D 0E 0F)
i = BF 8C 64 62 ⊕ f(A3 A9 67 74)
i = BF 8C 64 62 ⊕ 6C 78 2E 8E

i = D3 F4 4A EC
j = k = AF A4 69 7B
D3 F4 4A EC AF A4 69 7B

ROUND 2
k = i = D3 F4 4A EC
i = j ⊕ f(i ⊕ K3)
i = AF A4 69 7B ⊕ f(D3 F4 4A EC ⊕ 08 09 0A 0B)
i = AF A4 69 7B ⊕ f(DB FD 40 E7)
i = AF A4 69 7B ⊕ 58 3B 8B CD
i = F7 9F E2 B6
j = k = D3 F4 4A EC
F7 9F E2 B6 D3 F4 4A EC

ROUND 3
k = i = F7 9F E2 B6
i = j ⊕ f(i ⊕ K2)
i = D3 F4 4A EC ⊕ f(F7 9F E2 B6 ⊕ 04 05 06 07)
i = D3 F4 4A EC ⊕ f(F3 9A E4 B1)
i = D3 F4 4A EC ⊕ C7 FE 4D FF
i = 14 0A 07 13
j = k = F7 9F E2 B6
14 0A 07 13 F7 9F E2 B6

ROUND 4
k = i = 14 0A 07 13
i = j ⊕ f(i ⊕ K1)
i = F7 9F E2 B6 ⊕ f(14 0A 07 13 ⊕ 00 01 02 03)
i = F7 9F E2 B6 ⊕ f(14 0B 05 10)
i = F7 9F E2 B6 ⊕ A3 D4 A7 E2
i = 54 4B 45 54
j = i = 14 0A 07 13
14 0A 07 13 14 0A 07 13

j = j ⊕ i = 14 0A 07 13 ⊕ 54 4B 45 54 = 40 41 42 47
i = i ⊕ K5 = 54 4B 45 54 ⊕ 00 02 04 06 = 54 49 41 52
j = j ⊕ K6 = 40 41 42 47 ⊕ 01 03 05 09 = **41 42 47 4E**
54 49 41 52 41 42 47 4E

2.3. Base64 Algorithm

Base64 is an encoding technique that converts binary data into ASCII strings, allowing binary data to be transmitted over text-only enabled media, such as web applications and email. Base64 works by dividing binary data into 24-bit blocks, which are then divided into four 6-bit groups. Each 6-bit group is mapped to one character in the Base64 set of 64 characters (A-Z, a-z, 0-9, +, /). If the data is not 24-bit enough, padding with zeros is added, and if the data length is not a multiple of 3 bytes, padding "=" is added at the end of the string. For example, the string "hello" is encoded as "aGVsbG8=". Base64 is often used to send email attachments as text, encode data in URLs, and send images or binary files over text protocols such as HTTP.

Stages of Base64 Encoding

84 73 65 82 65 66 71 78
01010100 01001001 01000001 01010010 01000001 01000010 01000111 01001110
010101 000100 100101 000001 010100 100100 000101 000010 010001 110100 111000 _____
21 4 37 1 20 36 5 2 17 52 56 _
VElBUkFCR04=

Stage of Base64 Decoding

Ciphertext: VElBUkFCR04=
010101 000100 100101 000001 010100 100100 000101 000010 010001 110100 111000 _____
01010100 01001001 01000001 01010010 01000001 01000010 01000111 01001110
84 73 65 82 65 66 71 78

3. Result and Discussion

The results show that the combination of FEAL-4 and Base64 algorithms can significantly improve the security of image files. FEAL-4, with its 4-round encryption process, provides a high level of protection to image files, while Base64 adds an additional encoding layer. Test results on image files with *.bmp, *.jpeg, and *.png formats show that this encryption method is effective in maintaining data confidentiality, while preserving file integrity. The encryption process with FEAL-4 utilizes an XOR operation with a predefined key, while the decryption process returns the original data using the same key. The combination of these two algorithms ensures that the image file cannot be accessed or modified by unauthorized parties.

3.1. Research Methods

1. Preparation, this stage is the initial activity in conducting research, namely by making the background of the problem then formulating the next problem limiting the problems to be solved and determining the objectives and benefits of this research. After that, the author determines the security of the image file which will be encrypted encoding and decoding decrypted which later the image file is encrypted and cannot be opened by a third person.
2. Theory Study, in this stage the author collects various theories both from books borrowed from the library, journals and the internet to support the research to be carried out. The theories collected include image file security, FEAL Algorithm and Base64 Algorithm and Visual Basic.
3. Collection of Theory, at this stage the author conducts a Library study (Library research) Library studies are carried out with the aim of knowing what methods will be used to solve the problems studied, as well as getting a strong reference base in applying a method that will be used in this thesis, namely by studying books, journals or internet sites related to the problems to be discussed.
4. Design, at this stage the author performs or makes calculations manually with the FEAL Algorithm and Base64 Algorithm which then designs the system to be built.
    a. Testing and Implementation
       This stage is a very important stage, namely testing and implementing the system that has been made. This stage is based on the design that has been done. Implementing the FEAL Algorithm and Base64 Algorithm into a Visual Basic programming language.
    b. Perform and run the program to see the results of image file security, whether there are still errors.
    c. Make revisions to the design of program applications that experience errors.
5. Final Stage
   At this stage, the author will discuss conclusions and also suggestions from the results of the research that has been done.

3.2. System Analysis

System analysis is defined as a technique used to understand and make detailed specifications of what the system should do. With the system analysis, the system to be designed is expected to be better and easier in further system development. The purpose of this system analysis itself is to help model the design of the system that will be implemented in real form.

3.3. System Design

In this image file security application system, the author uses the Feal algorithm and Base64 algorithm in solving the problem. Where this design uses a flowchart to find out how the encoding encryption and decoding decryption process will be designed in a system.

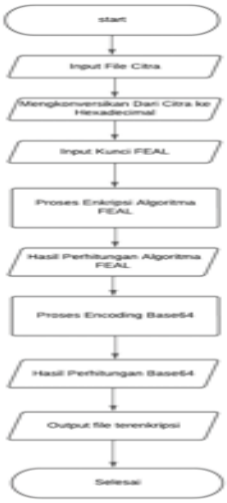

Figure 1: Encryption Encoding Flowchart

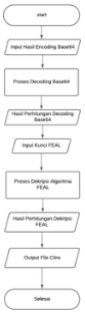

Figure 2: Decryption Decoding Flowchart

3.4. Convert Images to Hexadecimal Numbers

Fig. 3: Convert

Figure 3: is an image that will be encrypted, to find the ifile value by using additional binary viewer software with a size of 1,213 KB. Figures must be numbered using Arabic numerals. Figure captions must be in 8 pt Regular font. Captions of a single line must be centered whereas multi-line captions must be justified. Captions with figure numbers must be placed after their associated figures, as shown in Figure 4.

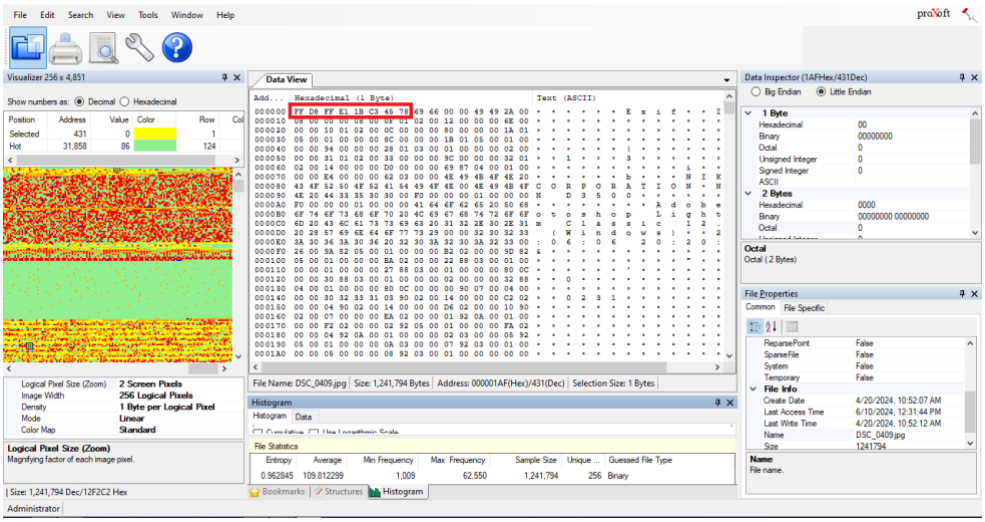

Fig. 4: From this image, several hexadecimal numbers are taken, namely FF D8 FF E1 1B C3 45 78

3.6. Calculation process of super encryption of FEAL algorithm and Base64 Algorithm

- **FEAL-4 Algorithm Encryption Calculation**

Plain HEX: FF D8 FF E1 1B C3 45 78
32-bit subkeys (K1, K2, …, K6):
00010203 04050607 08090A0B 0C0D0E0F 00020406 01030509
i = L ⊕ K5 = FF D8 FF E1 ⊕ 00 02 04 06 = FF DA FB E7

j = i ⊕ (R ⊕ K6) = FF DA FB E7 ⊕ (1B C3 45 78 ⊕ 01 03 05 09)
j = FF DA FB E7 ⊕ 1A C0 40 71 = E5 1A BB 96
FF DA FB E7 E5 1A BB 96

ROUND 1
k = j = E5 1A BB 96
j = i + f(j ⊕ K1) = FF DA FB E7 ⊕ f(E5 1A BB 96 ⊕ 00 01 02 03)
j = FF DA FB E7 ⊕ f(E5 1B B9 95)
j = FF DA FB E7 ⊕ 46 AC 63 E7
j = B9 76 98 00
i = k = E5 1A BB 96
E5 1A BB 96 B9 76 98 00
FEAL-4 ROUND FUNCTION
G0(a,b) = (a + b (mod 256)) <<< 2
G1(a,b) = (a + b + 1 (mod 256)) <<< 2
y1 = G1(x0 ⊕ x1, x2 ⊕ x3)
y2 = G1(y1, x2 ⊕ x3)
y0 = G0(x0, y1) y3 = G1(y2, x3)
f(E5 1B B9 95)
y1 = G1(E5 ⊕ 1B, B9 ⊕ 95) y1 = G1(FE, 2C)
y1 = (FE + 2C + 1 (mod 256)) <<< 2
y1 = (254 + 44 + 1 (mod 256)) <<< 2
y1 = 43 <<< 2
y1 = 00101011 <<< 2
y1 = 10101100
y1 = AC
y2 = G0(y1, B9 ⊕ 95) y2 = G0(AC, 2C)
y2 = (AC + 2C (mod 256)) <<< 2
y2 = (172 + 44 (mod 256)) <<< 2
y2 = 216 <<< 2
y2 = 11011000 <<< 2
y2 = 01100011
y2 = 63
y0 = G0(x0, y1) y0 = G0(E5, AC)
y0 = (E5 + AC (mod 256)) <<< 2
y0 = (229 + 172 (mod 256)) <<< 2
y0 = 145 <<< 2
y0 = 10010001<<< 2
y0 = 01000110
y0 = 46
y3 = G1(y2, x3) y3 = G1(63, 95)
y3 = (63 + 95 + 1 (mod 256)) <<< 2
y3 = (99 + 149 + 1 (mod 256)) <<< 2
y3 = 249 <<< 2
y3 = 11111001 <<< 2
y3 = 11100111
y3 = E7
f(14 0B 05 10) = (y0, y1, y2, y3) = 46 AC 63 E7

ROUND 2
k = j = B9 76 98 00
j = i + f(j ⊕ K1) = E5 1A BB 96 ⊕ f(B9 76 98 00 ⊕ 04 05 06 07)
j = E5 1A BB 96 ⊕ f(BD 73 9E 07)
j = E5 1A BB 96 ⊕ 79 A1 E8 C3
j = 9C BB 53 55
i = k = B9 76 98 00
B9 76 98 00 9C BB 53 55

ROUND 3
k = j = 9C BB 53 55
j = i + f(j ⊕ K1) = B9 76 98 00 ⊕ f(9C BB 53 55 ⊕ 08 09 0A 0B)
j = B9 76 98 00 ⊕ f(94 B2 59 5E)
j = B9 76 98 00 ⊕ 31 B8 FE 75
j = 88 CE 66 75
i = k = 9C BB 53 55
9C BB 53 55 88 CE 66 75

ROUND 4
k = j = 88 CE 66 75
j = i + f(j ⊕ K1) = 9C BB 53 55 ⊕ f(88 CE 66 75 ⊕ 0C 0D 0E 0F)
j = 9C BB 53 55 ⊕ f(84 C3 68 7A)
j = 9C BB 53 55 ⊕ B7 69 ED A1
j = 2B D2 BE F4
i = k = 88 CE 66 75
88 CE 66 75 2B D2 BE F4
i = i ⊕ j
i = 88 CE 66 75 ⊕ 2B D2 BE F4
i = A3 1C D8 81
j = 2B D2 BE F4
Cipher HEX: j + i
Cipher HEX: 2B D2 BE F4 A3 1C D8 81

Encoding Algorithm Base64

Plain HEX: 2B D2 BE F4 A3 1C D8 81
00101011 11010010 10111110 11110100 10100011 0001110011 01100010 000001 001010 111101 001010 111110 111101 001010 001100 011100 110110 001000 000100
10 61 10 62 61 10 12 28 54 8 4
K9K+9KMc2IE=

Base64 Algorithm Decoding

Base64 Encoded: K9K+9KMc2IE=
10 61 10 62 61 10 12 28 54 8 4
001010 111101 001010 111110 111101 001010 001100 011100 110110 001000 000100 00101011 11010010 10111110 11110100 10100011 0001110011 01100010 000001
2B D2 BE F4 A3 1C D8 81

Decryption Process of FEAL-4

Cipher HEX: 2B D2 BE F4 A3 1C D8 81
Key: 00010203 04050607 08090A0B 0C0D0E0F 00020406 01030509
j = L
j = 2B D2 BE F4
i = R ⊕ j
i = A3 1C D8 81 ⊕ 2B D2 BE F4
i = 88 CE 66 75
ROUND 1
k = i = 88 CE 66 75
i = j ⊕ f(i ⊕ K4)
i = 2B D2 BE F4 ⊕ f(88 CE 66 75 ⊕ 0C 0D 0E 0F)
i = 2B D2 BE F4 ⊕ f(84 C3 68 7A)
i = 2B D2 BE F4 ⊕ B7 69 ED A1
i = 9C BB 53 55

j = k = 88 CE 66 75
9C BB 53 55 88 CE 66 75
ROUND 2
k = i = 9C BB 53 55
i = j ⊕ f(i ⊕ K3)
i = 88 CE 66 75 ⊕ f(9C BB 53 55 ⊕ 08 09 0A 0B)
i = 88 CE 66 75 ⊕ f(94 B2 59 5E)
i = 88 CE 66 75 ⊕ 31 B8 FE 75
i = B9 76 98 00
j = k = 9C BB 53 55
B9 76 98 00 9C BB 53 55

ROUND 3
k = i = B9 76 98 00
i = j ⊕ f(i ⊕ K2)
i = 9C BB 53 55 ⊕ f(B9 76 98 00 ⊕ 04 05 06 07)
i = 9C BB 53 55 ⊕ f(BD 73 9E 07)
i = 9C BB 53 55 ⊕ 79 A1 E8 C3
i = E5 1A BB 96
j = k = B9 76 98 00

E5 1A BB 96 B9 76 98 00

ROUND 4
k = i = E5 1A BB 96
i = j ⊕ f(i ⊕ K1)
i = B9 76 98 00 ⊕ f(E5 1A BB 96 ⊕ 00 01 02 03)
i = B9 76 98 00 ⊕ f(E5 1B B9 95)
i = B9 76 98 00 ⊕ 46 AC 63 E7
i = FF DA FB E7
j = i = E5 1A BB 96
FF DA FB E7 E5 1A BB 96
j = j ⊕ i = E5 1A BB 96 ⊕ FF DA FB E7 = 1A C0 40 71
i = i ⊕ K5 = FF DA FB E7 ⊕ 00 02 04 06 = FF D8 FF E1
j = j ⊕ K6 = 1A C0 40 71 ⊕ 01 03 05 09 = 1B C3 45 78
FF D8 FF E1 1B C3 45 7.

The test of the program was carried out using Microsoft Visual Basic 2022 so that the application made can run and be tested directly into the computer. To run the application a user must click on the FEAL_Base64 application icon. Next, an initial screen will appear containing the main form, encryption form, and decryption form.

4.1. Testing

The test of the program was carried out using Microsoft Visual Basic 2022 so that the application made can run and be tested directly into the computer. To run the application a user must click on the FEAL_Base64 application icon. Next, an initial screen will appear containing the main form, encryption form, and decryption form.

FEAL_4 Encryption Steps

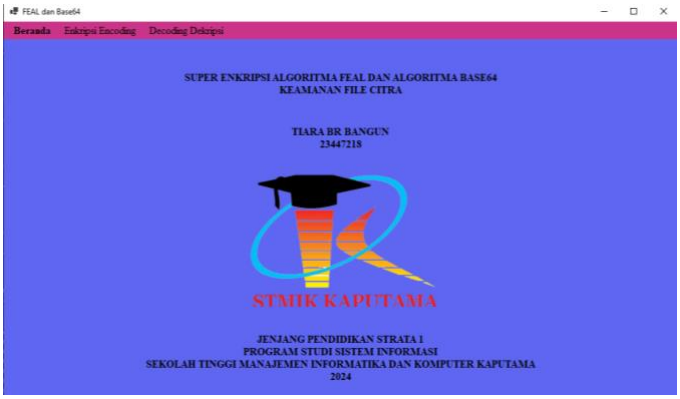

Fig. 5: Main Menu Display

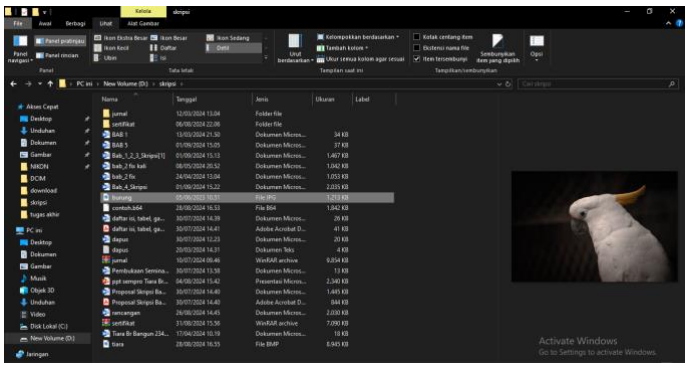

Fig. 6: Before encrypting data. The user must press the image file search button to find the image file to be encrypted. Once selected then click the OPEN button.

FEAL_4 Encryption Steps

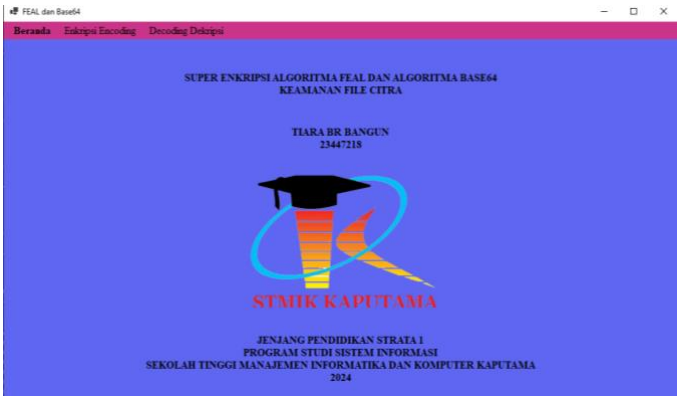

Fig. 7: Main Menu Display

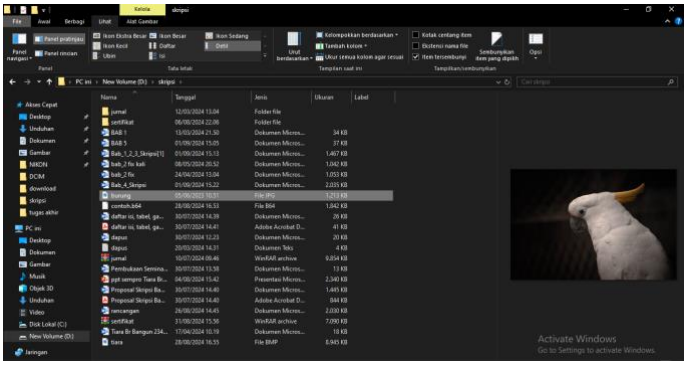

Fig. 8: Before encrypting data. The user must press the image file search button to find the image file to be encrypted. Once selected then click the OPEN button.

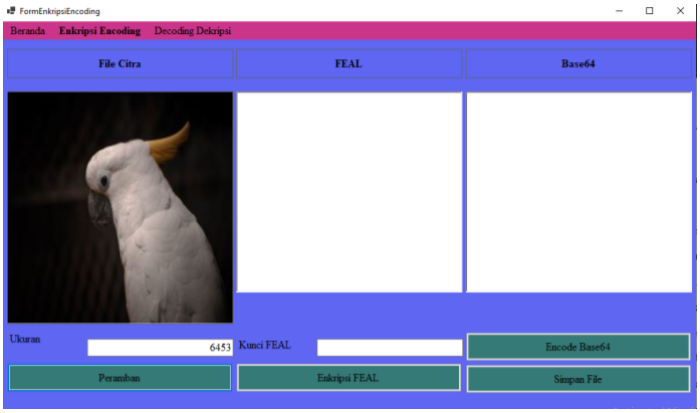

Fig. 9: Selanjutnya tekan tombol enkripsi untuk melakukan proses enkripsi dengan algoritma FEAL-4 dan Base64 untuk mengubah file citra menjadi output file terenkripsi.

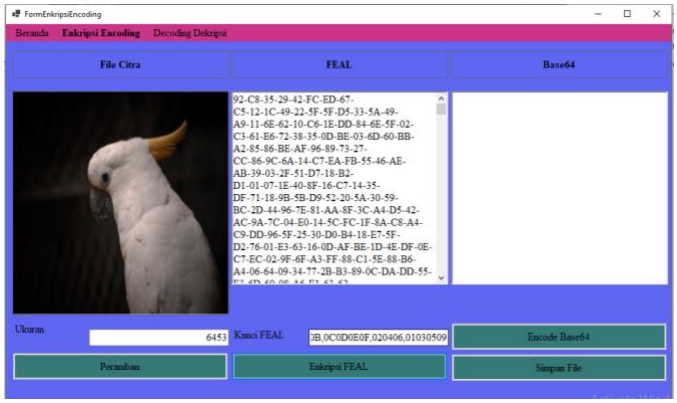

Fig. 10: Encryption view using FEAL-4 algorithm.

After encrypting with the FEAL-4 algorithm, it is then encrypted again using the Base64 algorithm. But first input the key for encryption of the Base64 algorithm and can be seen in the image below.

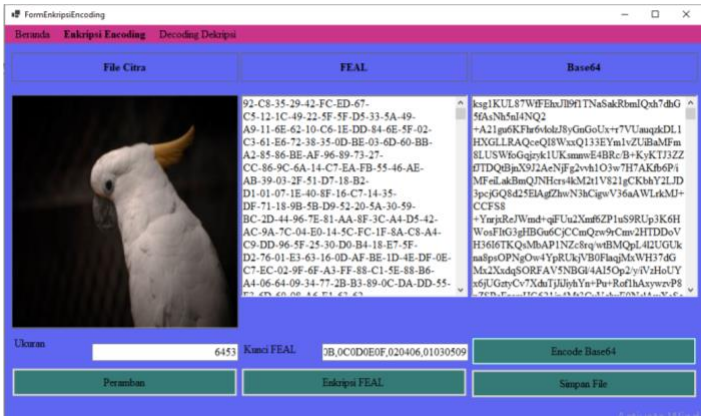

Fig.11: Encryption display using the Base64 algorithm

After being encrypted with the FEAL-4 and Base64 algorithms, it will produce an encrypted output file that cannot be recognized anymore, when you want to see the results, the encrypted output file is first saved by pressing the save button. Below is the process of saving the encrypted output file.

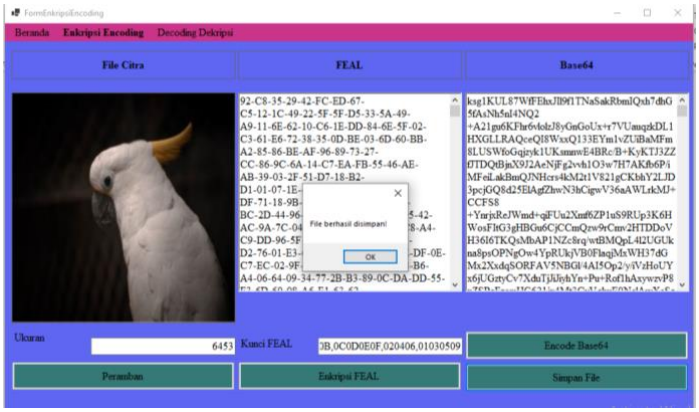

Fig.12: Process View Save Output Encrypted Image File

After encrypting with the FEAL-4 and Base64 algorithms and producing an encrypted file output. Next enter the decryption process, the first decryption is done with the Base64 algorithm, by opening the data from the previous encryption, can be seen in the image below.

FEAL-4 Decryption Steps

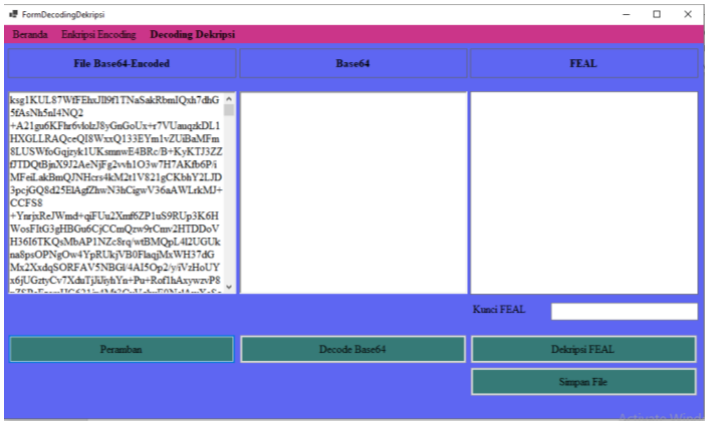

Fig. 13: Decryption display

After that, do the Base64 decryption process, as can be seen in the image below.

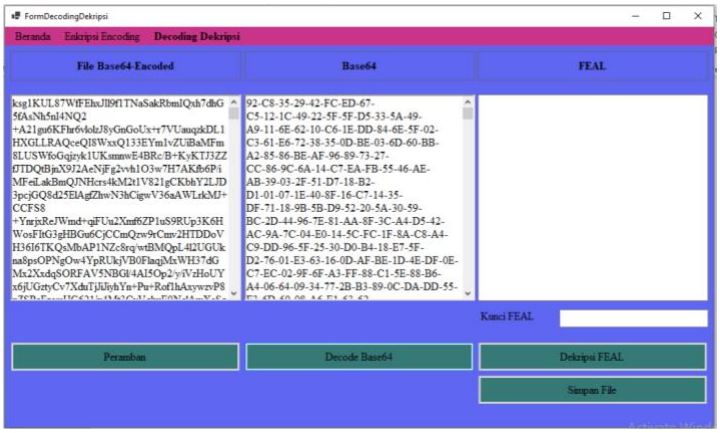

Fig. 14: Decryption display using the Base64 algorithm

Setelah didekripsi dengan Base64 kemudian didekripsi kembali dengan menggunakan algoritma FEAL-4, tetapi terlebih dahulu inputkan kunci untuk dekripsi dari algoritma FEAL-4 dan dapat dilihat pada gambar di bawah ini.

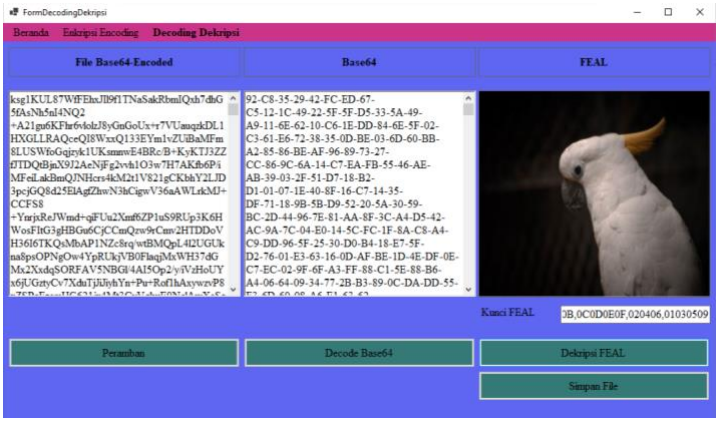

Fig. 15: Decryption view using FEAL-4 algorithm.

After the decryption process with the FEAL-4 and Base64 algorithms, the image file will be returned.

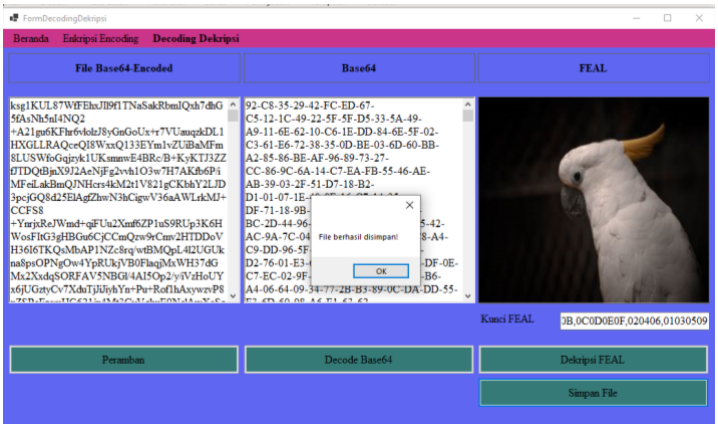

Fig. 16: Display Process Save Output Decrypted Image File

6. Conclusion

Based on the analysis from Chapter 1 to Chapter 4, this research focuses on developing an image file security system using a combination of FEAL-4 and Base64 algorithms. The FEAL-4 algorithm is used because it has a high speed and simple structure that allows efficient encryption and decryption, although the security of this algorithm is still debatable. While Base64 is used for encoding data into ASCII format, although this algorithm does not provide cryptographic security directly.

This research successfully designed and implemented a super encryption system that uses both algorithms to secure image files. The process

involves several steps from encryption using FEAL-4 to encoding using Base64. The resulting system is able to protect sensitive information from unauthorized access by hiding the data in a format that is not easily recognizable.

References

[1] Azlin, Ripto Sudiyarno. Modifikasi Metode Base64 Menggunakan Caesar Cipher Dan Kunci Rahasia. Yogyakarta. 2018
[2] D Rachmawati, M A Budiman and W S E Siburian. Hybrid cryptosystem implementation using fast data encipherment algorithm (FEAL) and goldwasser-micali algorithm for file security. IOP Publishing. 2018
[3] Dian Asmarajati. SISTEM REFERENSI BUKU MENGGUNAKAN ALGORITMA BASE 64 PADA GENERATE DAN SCAN QR CODEDI DINAS ARPUSDA WONOSOBO. Universitas Sains Al-Qur'an. 2020
[4] Dony Ariyus, Universitas Amikom. Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi. Penerbit Andi. Yogyakarta, 2008
[5] Muhammad Adli Rizqulloh, Yoyo Somantri, Resa Pramudita, Agus Ramelan. Implementasi algoritma block cipher four pada mikrokontroler STM32F103C8T6. Implementasi algoritma block cipher four pada mikrokontroler STM32F103C8T6. Bandung, 2021
[6] Mukhtar. Kriptografi untuk Keamanan Data. Deepublish.Yogyakarta, 2018
[7] Oris Krianto Sulaiman, Khairuddin Nasution, Satria Yudha Prayogi. BASE64 SEBAGAI KUNCI KEAMANAN PADA ONE TIME PAD (OTP). CESS (Journal of Computer Engineering System and Science). Medan, 2020