Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

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

Superencryption of BASE 64 Algorithm and ELGAMAL Algorithm on Android Based Image Security

Usman Gumanti[1*], A M H Pardede[2], Husnul Khair[3]

[1,2,3] *Informatics Engineering, STMIK Kaputama*
Jl. Veteran No. 4A-9A, Binjai, North Sumatra, Indonesia
ugumantu@gmail.com[1], akimmhp@live.com[2], husnul.khair@gmail.com [3]

Abstract

In the current era of globalization, the development of information technology is growing rapidly, there is a possibility that there will be data leaks when the process of exchanging information is carried out, then security becomes a very important aspect which will cause unwanted things, for example manipulation of images in the form of information systems. If this important information falls into the hands of the wrong person, it can be negative and can be detrimental to the image owner. So a security system is designed that functions to protect the data that is sent while maintaining its authenticity and authenticity. Various ways have been developed for data security, one of which is by using cryptography. Cryptography is the science of securing data by using data transformation so that the resulting data cannot be understood by other parties. This transformation can provide a solution to two data security problems, namely the problem of privacy and data authentication. Cryptographic techniques can be used to ensure data security, one of which can be utilized is encryption and description of data or in other words encoding data so that only the person concerned can understand the contents of the data. The proper use of information technology is very important to send private and confidential images to certain parties. These images are still in the form of PNG and JPG extensions, for this reason a security system is needed that can protect images that are transmitted through a communication network, one way that can be done to secure images is using the BASE 64 algorithm and the ELGAMAL algorithm.

Keywords: *Cryptography, Base64, Elgamal, Image*

1. Introduction

In the current era of globalization, the development of information technology is growing rapidly, there is a possibility that there will be data leaks when the process of exchanging information is carried out, then security becomes a very important aspect which will cause unwanted things, for example manipulation of images in the form of information systems. If this important information falls into the hands of the wrong person, it can be negative and can be detrimental to the image owner. So a security system is designed that functions to protect the data that is sent while maintaining its authenticity and authenticity. The proper use of information technology is very important to send private and confidential images to certain parties. These images are still in the form of PNG and JPG extensions, for this reason a security system is needed that can protect images that are transmitted through a communication network, one way that can be done to secure images is using the BASE 64 algorithm and the ELGAMAL algorithm.

2. Theoretical basis

2.1. Cryptography

Cryptography is a method for securing data, both text data and image data. This method is carried out by encoding or scrambling the original data, so that other parties who do not have access rights to the data cannot obtain the information contained therein. In general there are two types of cryptographic algorithms based on the key, namely symmetric algorithms and asymmetric algorithms. A symmetric algorithm is an algorithm that has the same encryption and decryption keys, while an asymmetric algorithm consists of 2 keys, namely a public key for encryption and a private key for decryption [1] .

2.2. Base64

Base64 transformation is one of the algorithms for encoding and decoding data into ASCII format, which is based on base 64 or can be said to be one of the methods used to encode binary data. The characters generated in this base64 transformation consist of A..Z, a..z and 0..9, plus the "+" and "/" symbols as well as one equal character (=) in the last two characters used for filling in or in other

words adjusting and completing binary data. The symbol character that will be generated will depend on the running algorithm process. base64 encryption is surprisingly simple, if there is a string and you want it to be encrypted to base64 [2]

Encryption Techniques in the Base 64 Algorithm

1 Split the bytes string into 3 bytes.
2 Combine 3 bytes to make 24 bits. Note that 1 bytes = 8 bits, so 3 x 8 = 24 bits.
3 Then the 24 bits that are stored in the buffer (unified) are broken into 6 bits, it will produce 4 fractions.
4 Each fraction is converted to a decimal value, where the maximum 6 bit value is 63.
5 Finally, make these decimal values into indexes to select a maximum index of 64 using the ASCII table.

Decryption Technique in Base 64 Algorithm

1. Convert ASCII characters to decimal numbers representing each character's ASCII value.
2. Convert decimal numbers to 8-bit binary numbers.
3. Merge all numbers-
4. Convert each 8-bit block to a decimal number.
5. Convert the decimal number to the appropriate ASCII character.
6. Combines all ASCII characters into one text string the binary number into one binary string.
7. Cut the binary string into 8-bit blocks.

2.3. Elgamal Algorithm

The security of Elgamal's algorithm lies in the difficulty of calculating discrete logarithms at large prime modulo, so efforts to solve this logarithm problem are difficult to solve. This algorithm has the advantage of generating keys that use discrete logarithms and encryption and decryption methods that use large computational processes so that the encryption results are twice the size of the original. The drawback of this algorithm is that it requires large resources so that the encryption results are twice the size of the original. The disadvantages of this algorithm are that it requires large resources because the resulting ciphertext is twice the length of the plaintext and requires a processor capable of performing large computations for large power logarithm calculations [3] .
A character represented using an ASCII butal number will generate a code in the form of a block consisting of two values (a, b).

1. Take a character in the message to be encrypted and transform that character into ASCII code to get an integer m. The plaintext is arranged into blocks m1, m2, …, such that each block represents a value in the range 0 (zero) to p-1.
2. Choose a random number k, which in this case $0 < k < p-1$, such that k is relatively prime with p-1.
3. Calculate the value of a and b with the following equation:
   $a = g^k \pmod p$ .....(2.1)
   $b = ykm \pmod p$(2.2)
4. The ciphertext for the m characters is obtained in block (a, b). Decryption from ciphertext to plaintext uses the key a which is kept confidential by the recipient of the message.
   Given (p,g,y) as the public key and x as the secret key in the ElGamal algorithm. If given ciphertext (a, b), then
   $m = b/ax \bmod p$(2.3)
   where M is plaintext.
   Where is the value
   $(ax)^{-1} = r^{-a} = rp^{-1-a} \bmod p$ .....(2.4)
5. Retrieve a ciphertext block from the sender's encrypted message.
6. Using a which is kept secret by the recipient, calculate the plaintext value using "equation (2)" and "equation (3)".

The ElGamal algorithm requires a pair of keys which are generated by choosing a prime number p and two random numbers g and x, provided that the value of g and x is less than p which satisfies the equation.

$$y = g^x \bmod p$$

From this equation the values y, g and p are public key pairs while x, p are private key pairs. The quantities used in the Elgamal cryptographic algorithm are:

1. The prime number p is not secret provided that p> 255.
2. The random number g ($g < p$) is not secret.
3. Random number x with condition $1 < x < p - 2$.
4. Calculate $y = g^x \bmod p$.

The public key is y, g, p while the private key is x. the values of y, g, and p are not kept secret while the value of x must be kept secret because.

Procedure Make Install Key

1. Choose any prime number p.
2. Choose two random numbers, g and x, provided that $g < p$ and $1< x < p-2$.
3. Calculate $y = g^x \bmod p$.

The public key is y, the secret key is x. The g and p values are not kept secret and can be announced to group members.

Technique Encryption On Algorithm Elgamal

Plaintext is organized into blocks m1, m2,…, such that each block represents a value in the range 0 to p-1.
Choose a random number, which in this case is 0 kp – 1, such that it is relatively prime with p-1.
Each m block is encrypted with a formula.

$$a = g^k \bmod p$$
$$b = y^k m \bmod p$$

Technique Decryption On Algorithm Elgamal

The decryption process uses the private keys x and p to decrypt a and b into plaintext m with the equation:

$$(ax)^{-1} = a^{p-1-x} \bmod p$$

$$m = b * a^{x} \bmod p$$

So that the plaintext can be recovered from ciphertext pairs a and b.

2.4. Image

Understanding the image in general is an image, photo or a variety of two-dimensional displays that describe an object visualization. Image can be realized in printed or digital form. A digital image is a two-dimensional array of numbers. Digital images are stored in an array of digital numbers which are the result of quantification of the brightness level of each pixel composing the image [4] .

3. Analysis And Design

3.1. Calculation Analysis

An image or image consists of a collection of several pixels which are usually initialized in the form of coordinates (x, y) where (x) is the coordinate axis of the image width and (y) is the coordinate axis of the image length. Each pixel contains a color that has 3 values, namely a red value , *a green* value , and a blue value *where* each of these colors has a value in the range 0 to 255 which is expressed in binary form. The images selected to take matrix values are as follows:

Figure 1: JPEG Format Image

Figure 1 is an image that will be encrypted, before performing manual calculations, the image is converted first into a binary number using additional binary viewer software with the size of the photo being 6 x 6. The image that has been converted into a binary number will be like following:

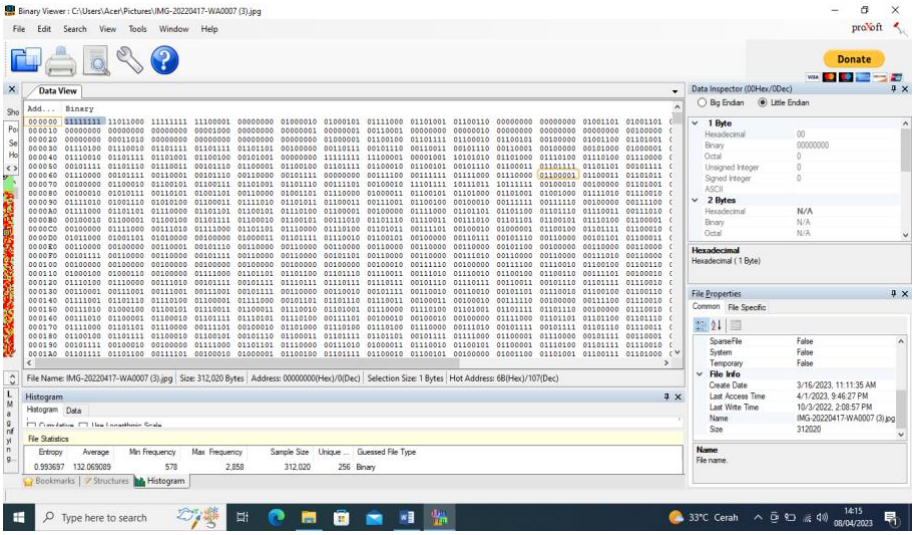

Figure 2: Table binary

Figure 2 table is the result of the binary value converted to decimal, which will be encrypted (*plaintext*)

3.2. Calculation Encryption Base64 Algorithm

In the encryption process, it is useful for changing plaintext (original message) into ciphertext (secret message). The following is an example of a calculation using the base64 algorithm.

1. Code decimal

Desimal	255	216	255

2. Decimal code converted to binary code:

Decimal	255	216	255
Bit Patterns	11111111	11011000	11111111

3. Divide the binary code into 6 bits/block and apply multiples of 4 blocks onwards.

Decimal	255								216								255							
Bit Patterns	1	1	1	1	1	1	1	1	1	1	0	1	1	0	0	0	1	1	1	1	1	1	1	1
Index	63				61				35				63											

4. These blocks are converted back into Index table Decimal numbers:

Decimal	255								216								255							
Bit Patterns	1	1	1	1	1	1	1	1	1	1	0	1	1	0	0	0	1	1	1	1	1	1	1	1
Index	63				61				35				63											
Base64 Encoded	?				=				#				?											

5. Fifth step: So you get Base64 encode.

Index	63	61	35	63

Counted until 6x6 pixels so in get results from encoding

Index	63	61	35	63
Index	63	48	1	2
Index	0	0	0	0
Index	2	0	0	1
Index	0	1	40	0
Index	0	0	0	0
Index	29	7	9	47
Index	27	54	52	32
Index	28	38	61	41
Index	25	2	36	0
Index	11	54	57	51
Index	11	38	5	36

3.3. Analysis Calculation Algorithmic Image Encryption Elgamal

From the results of image encryption with the base64 algorithm, the calculation is again carried out with the Elgamal algorithm using:
Key Generation Algorithm

1. Choose any prime number p (p can be *shared* among group members)
2. Choose two random numbers, g and x, provided that g < p and 1<_ x <_ p – 2
3. Calculate $y = g^k \bmod p$

   The result of this algorithm:

Public key: triple (y, g, p)
Private key: pair (x, p)
The Pubic Key is a triple : P = 229 G = 7 Y = 29
Private keys are pairs : X = 191p = 229
To find the value of Y:
$Y = g^{x} \bmod p$
$Y = 7^{191} \bmod 229$
Y = 29
Child : K is a prime random number
K = 174

Elgamal Algorithm Encryption

1. Choose a random number k, which in this case 1 <_ k <_ p – 2
2. Each m block is encrypted with a formula
   $a = g^{k} \bmod p$
   $b = y^{k} . m \bmod p$

Pairs a and b are ciphertexts for message block m. So, the size of the ciphertext is twice the size of the plaintext.
Then the image encryption process with the Elgamal algorithm is as follows:
Plaintext = 63
a = (7^174) mod 229 = 168
b = (29^174) x 63 mod 229 = 50
So, the resulting ciphertext is (168.50)
Plaintext = 61
a = (7^174) mod 229 = 168
b = (29^174) x 61 mod 229 = 172
So, the resulting ciphertext is (168,172)
Plaintext = 35
a = (7^174) mod 229 = 168
b = (29^174) x 35 mod 229 = 155

So, the resulting ciphertext is (168,155)
El Gamal Algorithm Ciphertext

63,61,35,63, = (168,50),(168,172),(168, 155), (168, 50)

continued count until to the final plaintext:
(168,50),(168,172),(168, 155), (168, 50), (168, 50), (168,49), (168,168), (168, 107), (168, 0), (168, 0), (168,0), (168, 0), (168,107), (168, 0), (168, 0), (168,168), (168,0), (168, 168), (168,79), (168, 0), (168, 0), (168,0), (168, 0), (168,0), (168,63), (168, 31), (168,138), (168, 110), (168, 185), (168,141), (168,34), (168, 109), (168,124), (168, 201), (168,172), (168,18), (168, 78), (168, 107), (168,94), (168, 0), (168, 16), (168,141), (168, 187), (168,95), (168, 16), (168, 201), (168, 153), (168,94)

3.4. Analysis Calculation Algorithmic Image Decryption Elgamal

Then describe it with the elgamal algorithm by calculating with the following formula:

1. Use private key x to calculate
   $(a^{x})^{-1} = a^{p-1-x} \bmod p$
2. Calculate the plaintext m with the equation
   $m = b/a^{x} \bmod p = b\ (a^{x})^{-1} \bmod p$

Then the image decryption process with the Elgamal algorithm is as follows:
Plaintext = 63
$l/a^{x} = (a^{x})^{-1} = a^{p-1-x} \bmod p$ = 168^37 mod 229 = 15
$m = b/a^{x} \bmod p$ = 50 x 15 mod 229 = 63
Plaintext = 61
a. (168^37) mod 229 = 15
m. (172 x 15) mod 229 = 61
Plaintext = 35
a. (168^37) mod 229 = 15
m. (155 x 15) mod 229 =35
Plaintext = 63
a. (168^37) mod 229 = 15
m. (50 x 15) mod 229 = 63
Plaintext = 63
a. (168^37) mod 229 = 15
m. (50 x 15) mod 229 = 63

continued until calculation end :

3.5. Base 64 Decryption Process

1. Change the ASCII character encoding results to a decimal value to the Index table.

Base64 Encoded	?	=	#	?
Index	63	61	35	63

2. Change Index code to binary code (*Bit Pattern*) 6 bits:

Base64 Encoded	?						=						#						?					
Index	63						61						35						63					
Bit Pattern (6 bits)	1	1	1	1	1	1	1	1	1	1	0	1	1	0	0	0	1	1	1	1	1	1	1	1

3. Make the bits of each block contain 8 data bits instead of the 6 bits again:

Base64 Encoded	?						=						#						?					
Index	63						61						35						63					
Bit Pattern (6 bits)	1	1	1	1	1	1	1	1	1	1	0	1	1	0	0	0	1	1	1	1	1	1	1	1
Bit Pattern (8 bits)	1	1	1	1	1	1	1	1	1	1	0	1	1	0	0	0	1	1	1	1	1	1	1	1

4. Convert 8 bit binary code to decimal.

Base64 Encoded	?						=						#						?					
Index	63						61						35						63					
Bit Pattern (6 bits)	1	1	1	1	1	1	1	1	1	1	0	1	1	0	0	0	1	1	1	1	1	1	1	1
Bit Pattern (8 bits)	1	1	1	1	1	1	1	1	1	1	0	1	1	0	0	0	1	1	1	1	1	1	1	1
Decimal	255						216						255											

Counted carry on count until to plaintext end

4. Conclusion

This research shows that the super encryption model proposed through a combination of Base64 and Elgamal algorithms is able to provide a better level of security compared to using only one algorithm. The combination of the two algorithms is able to provide a ciphertext that is stronger and more difficult to crack, so that images with the extension PNG and JPG are very safe when encrypted and decrypted using the Base64 and Elgamal algorithms.

References

[1] IP Sinaga, “Implementation of Elgamal Algorithm Hybrid Cryptography and Double Playfair Cipher in Desktop-Based Jpeg File Security,” vol. 1, no. 2, pp. 67–74, 2021.

[2] F. Al Isfahani and F. Nugraha, "Implementation of LSB Steganography with Base64 Encryption in Images with CMYK Color Space," *Sci. Comput. sci. Informatics J.* , pp. 1–8, 2019.

[3] A M H. Pardede, BS Ginting, and K. Lumbanbatu, "Image File Security Application Using the Elgamal Algorithm," vol. 3, no. 2, 2018.

[4] DA Prabowo and D. Abdullah, "Detection and Calculation of Objects Based on Color Using Color Object Tracking," *Pseudocode* , vol. 5, no. 2, pp. 85–91, 2018, doi: 10.33369/pseudocode.5.2.85-91.