Image Cryptographic Application Design using Advanced Encryption Standard (AES) Method

Nur Afifah[1], Aris Fanani[1], Yuniar Farida[1] and Putroue Keumala Intan[1]
[1] *Department of Mathematics, Science and Technology Faculty*
Sunan Ampel Islamic State University, Street Ahmad Yani 117, Surabaya, East Java

Keywords: Cryptography, Image, Advanced Encryption Standard, Attack, Encryption

Abstract: Development of technology gives significant impact on progress of all field of life, both in positive and negative way. Among the negative impacts is crime, such as theft, burglary and others. In communication security, information is very important. Data confidentiality is a priority so that maintaining the information security needs an application that can encrypt the data. One of the sciences used to design a data security application is cryptography, in which there are many methods can be used to encrypt a data. However, the best method is Advanced Encryption Standard method (AES). There are many types of AES that can be used but the most effective is AES-128. So, the aim of this study is to design image cryptographic application using the AES-128 method. Process of design applications with this method is through several stages, such as process of encryption, decryption, key generation and testing of the methods used. The attacks test is given by cropping, blurring, and enhancing the ciphertext image. In previous studies, there has never been an attack on the results of ciphertext, so this study will be accompanied by testing of attacks on ciphertext to determine the resistance of the method used. From the result of encryption and decryption, it is known that this AES-128 method was successfully applied to the image. While on the attack test, it was found that this method is resistant to cropping attacks, but not resistant to blurring and enhancement attacks.

1 INTRODUCTION

Technology development, including computer technology, is one of the most important aspects of human life. Anything as complex as any problems can be solved quickly and easily by a computer. Technology development is closely linked to the development of mathematics because every creation of a new technology is always calculated mathematically. However, by the sophistication of technology, now almost every secret can be found easily just by computer encoding. To obtain the data or information, people will do anything they can, such as breaking, stealing, or even tapping. This is very unfortunate. Some examples of data theft cases are even experienced by large companies, such as linkedIn, whose password was stolen (Rahmad, 2016), Gmail data theft (Darmawan, 2010) etc.

In the field of communication, information security is very important (Soleh, 2010) because that theft of data or information also includes violations of copyright. This has been regulated in Law No.28 of 2014 because the information obtained does not get the permission from the owner or the manufacturer. In addition, Indonesia also regulates the theft of data in the ITE Law in article 3 of 2008.

In order to anticipate the theft of such data, encryption is necessary to keep the confidential data to stay safe. Cryptography is a mathematical computation study that has relationships with information security, such as data integrity, entity authenticity, and data authenticity (Rahmatullah, 2016). Cryptography uses various techniques to secure data, one of which is the Advanced Encryption Standard (AES) method.

AES is the best choice method in encoding (Munir, 2006). This method has been used in several researches, such as Designing Application Encryption and Digital Image Description Using Rijndael Algorithms based on Java SE which produce encrypting and shortcut technique with 100% accuracy value (Yoga, 2014), Image Encryption and Decryption using AES Algorithm which can encrypt and decrypt an image (Desmukh, 2016).

Afifah, N., Fanani, A., Farida, Y. and Intan, P.
Image Cryptographic Application Design using Advanced Encryption Standard (AES) Method.
DOI: 10.5220/0008905500002481
In *Proceedings of the Built Environment, Science and Technology International Conference (BEST ICON 2018)*, pages 247-254
ISBN: 978-989-758-414-5

AES method has three types according to the key length that are AES- 128, AES -192, and AES 256. Previous studies mentioned that the most excellent AES algorithm is AES 128 (Arya, 2016). Therefore, in this study the method used is AES 128.

2 THEORITICAL FRAMEWORK

2.1 Cryptography

The term “cryptography” is derived from two Greek words, *crypto* and *graphia*. *Crypto* means secret and *graphia* means writing (Munir, 2006). Terminologically, cryptography is encryption techniques where randomized data uses an encryption key so that it will be difficult to read by someone who does not have a decryption key (Kromodimoeldjo, 2009).

According to historical records, cryptography has been used in Egypt since 4000 years ago by Egyptian kings during the war to send secret messages to their warlords through their couriers. The person who does this encoding is called a cryptographer, while the person who studies science and art in opening or deciphering a cryptographic algorithm without having to know the key is called cryptanalyst (Munir, 2006).

A good cryptographic algorithm is determined by the complexity of processing data or messages to be delivered and by fulfilling the following 4 requirements (Munir, 2006):

- Confidentiality. Message *(plaintext)* can only be read by authorized party.
- Authentication. The sender of the message must be identified with certainty, the intruder must be ensured that he cannot pretend to be someone else.
- Integrity. The recipient of the message must be able to ensure that the message received is not modified during data transmission process.
- *Non-repudiation*. The sender of the message must not be able to deny the message he sent.

Cryptograph basically consists of two processes, namely the process of encryption and the decryption process. The encryption process is the process of encoding common messages into secret messages called ciphertext. Ciphertext is something to be delivered through open communication channels. When ciphertext is received by the recipient of the message, then the secret message is changed again into an open message through the decryption process so that the message can be read again by the recipient of the message. This plaintext can be writing, photos, or videos in the form of binary data.

Generally, based on the key similarities, the encryption algorithm is divided into 2 types:

1. Symmetric key algorithm
   In this algorithm, the key used in encryption and decryption is the same. The AES method is included in this algorithm.
2. Asymmetric key algorithm
   This algorithm uses different keys in the encryption and decryption process. For example, the RSA method.

2.2 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a cryptographic algorithm that can be used rightly to secure data. This AES algorithm works on data blocks in the form of 4 x 4 matrix. Symmetrical ciphertext blocks can encrypt (encipher) and decrypt (decipher) information. AES algorithm uses clicking the cryptographic keys 128, 192, and 256 bits to encrypt and decrypt the data. Therefore, this algorithm is known as AES-128, AES-192, and AES-256. This algorithm also has another name that is Rijndael algorithm. It is because this algorithm was made by Rijndael, which is combined from Vincent Rijmen dan John Daemen.

AES (Advanced Encryption Standard) is the development of the standard DES (Data Encryption Standard) encryption algorithm of which validity period deemed to be over due to security. The rapid computer speed was considered very dangerous to the DES, so that on March 2, 2001 the new Rijndael algorithm was established as AES (Publication, 2001).

In the process stages of this algorithm, there are 3 main processes, namely encryption, decryption, and key expansion.

2.2.1 Key Expansion

The key expansion function takes the user supplied 16 bytes long key and utilizes the previously created round constant matrix rcon and the substitution table s_box to generate a 176 byte long key schedule w, which will be used during the end and decryption processes (Buchholz, 2001).

In this key generation. we initialize the initial key as a 16 byte cipher key and then expand to generate another key In this process, there are 3 stages, namely RotWord, SubWord, and XOR.

On RotWord shifting, every one byte is up cyclically in the fourth column. Results from RotWord are then substituted with the S-Box table. Then, to get the first sub key of the first column, XOR operation is performed with the first column of the cipher key and the R-con. The results of the operation then are used to get the next column by doing XOR to the column with the corresponding cipherkey and so on.

2.2.2 Encryption

Encryption is process of encoding the plaintext into ciphertext. On an 8-bit processor, encryption with Rijndael or AES can be programmed by simply implementing the different steps. The implementation of ShiftRows and AddRoundKey is straight forward from the description. The implementation of SubBytes requires a table of 256 bytes (Joan Daemen, Vicent Rijmen, 2002).

In encryption, there are several processes, they are:

- SubBytes
  In this process, substitution is carried out for each byte in the state with the S-box table set by Vincent. The following is the S-Box table used:

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 1: S-box table

Substitution for each byte in the state array, for example S [r,c] = xy, is a hexadecimal digit of the value S [r,c]. Then, the substitution value expressed by S [r,c] is an element in the S-Box which is the intersection of row x and column y. The following is transformation of SubBytes.

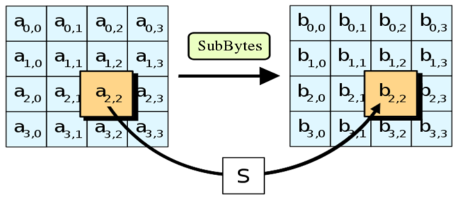


Figure 2: Subtituion of byte with s-box table

- ShiftRows
  In this process, shifting each byte is carried out in the state as the following figure:

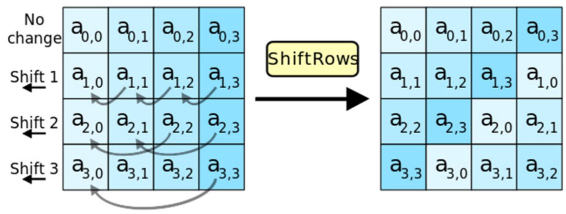


Figure 3: ShiftRows process

- MixColumns
  In the MixColumns stage, it operates every element in one column at the state. The elements in the column are multiplied by a fixed polynomial

$$a(x) = (03)x^3 + (01)x^2 + (01)x^3 + (02) \quad (1)$$

More details for the MixColumns transformation can be seen in the following multiplication matrix:

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \quad (2)$$

- AddRoundKey
  This round key process is added to the state with a simple bitwise XOR operations. Each round key consists of Nb words in which each word is then summed up with the corresponding word or column from state. The state of addroundkey is of the same size and obtain the next state an XOR operation for every element. So, it becomes:

$$b(i,j) = a(i,j) \oplus k(i,j) \quad (3)$$

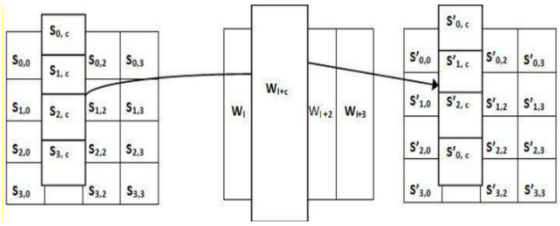


Figure 4: AddRoundKey Operation

with w_i is word of the corresponding key where $i = round * Nb + c$.

The AddRoundKey transfromation is implemented first in round = 0, where the key used is the initial key or key entered by the cryptographer and has not experienced key expansion process.

2.2.3 Decryption

Decryption is similar in structure to encryption, but uses the invers (Joan Daemen, Vicent Rijmen, 2002). At this decryption stage, the process is the same as encryption, but it uses inverse in each process. So, it consists of:

- InvSubBytes
  This Inverse SubBytes process is almost the same as process on encryption, but the subtitution is with the Invers S-Box table

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Figure 5: Inv S-box table

- InvShiftRows
  Inv ShiftRows is a transformation of a byte that is the opposite of the ShiftRows transformation. If ShiftRows transform the bit shift to the left, then InvShiftRows transform the bit shift to the right.

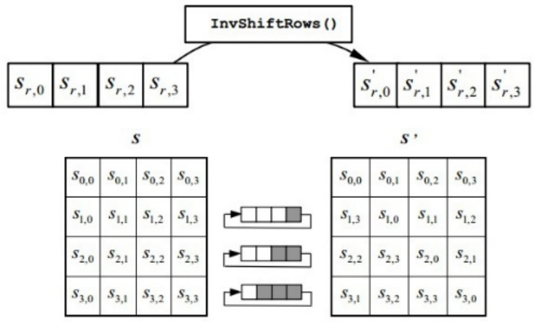


Figure 6: InvShiftRows process

- InvMixColumn
  In the InvMixColumns process, the columns in each state or word will be seen as polynomials for GF (2^8) and multiplying the modulo $x^4 + 1$ with fixed polynomials $a^{-1}(x)$ obtained from:

$$a^{-1}(x) = (0b)x^3 + (0d)x^2 + (09)x + (0e) \quad (4)$$

or in a matrix:

$$S'(x) = a(x) * S(x) \quad (5)$$

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \quad (6)$$

- InvAddRoundKey
  In the transformation of Inverse AddRoundKey, it does not have a difference with the AddRoundKey transformation because in this transformation, only simple addition operations are performed using XOR bitwise operations.

2.2.4 Digitial image

Image is a multimedia component that has an important role as a form of visual information (Hanifah, 2012). Image has different characteristics from data of text. Image has more information than data of text. In other words, image data can provide more information than text because the information of them is presented in text form (Hanifah, 2012).

In general, Image is a two dimensional plane. Image is a continuous function of light intensity in a two dimensional plane symbolized by $f(x, y)$. In this case, $(x, y)$is a coordinate in two dimensional fields and $f(x, y)$ is the light intensity at the point (x, y) (Munir, 2006).

Digital images are generally rectangular in size, expressed by dimensions of length (m) x width (n).

Dimensional size is the representation of an image in the form of a matrix of size m x n pixels, as presented in the following functions:

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,m-1) \\ f(1,0) & f(1,2) & \dots & f(1,m-1) \\ \vdots & \vdots & \vdots & \vdots \\ f(n-1,0) & f(n-1,1) & \cdots & f(n-1,m-1) \end{bmatrix}$$

3 RESEARCH METHOD

To collect data required in this study, researcher searched data and information as appropriate reference to support the truth of the description of the material, theory, and discussion. Meanwhile, the data used in this research is an image file of greyscale with the size 32 x 32.

Design on this system uses AES 128 so that the pixel value matrix of the image is entered in the partition into blocks 4 x 4 and represented in hexadecimal numbers.

The attacks tested in this study were cropping, blurring, and enhancing. This testing attacks is used to determine the resistance of an AES or Rijndael method.

The following is a flowchart of the encryption process:

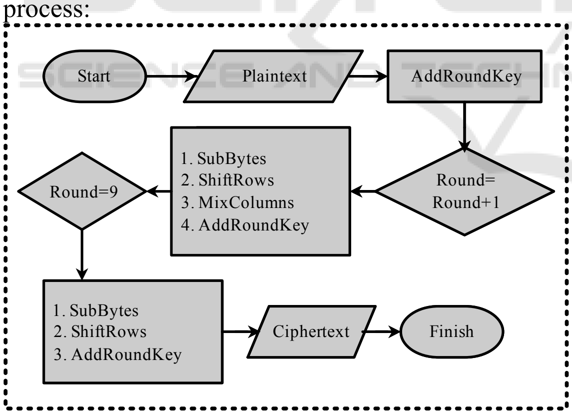


Figure 7: Flowchart of Encryption Process

Ciphertext that has been attacked then is decrypted for testing. The following is the flowchart of decryption process:

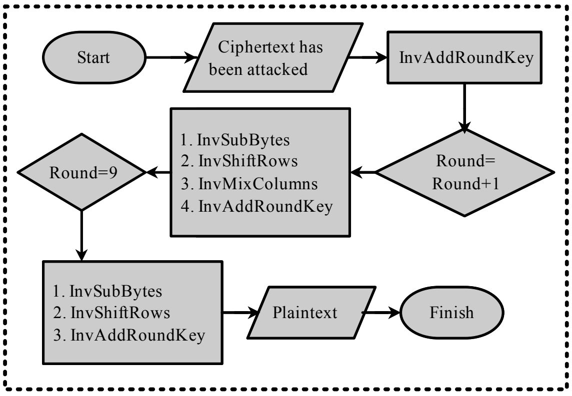


Figure 8: Flowchart of Decryption Process

4 RESULT AND DISCUSSION

The previous discussion has been briefly described the process of encryption and encryption using AES method. This chapter will explain about the design and each stage. The first stage in the design of the application is to generate the first key and then to do the encryption and decryption stages. For more details, it will be described in each of the following stages:

4.1 Key Schedule

Key schedule is a process to generate keys that will be used in the process of encryption and decryption. As explained in the previous chapter, this key formation consists of several stages, namely RotWord, SubWord, XOR with R-con values, and XOR with the previous word. In designing this system, the cipher key is inputted by the application maker. The cipher key entered is then converted to an ASCII number. If the cipher is inputted more than 16 bytes, then the first 16 bytes are used, but if the cipher entered is less than 16 bytes then the cipher will be computed to 16 bytes with the addition of the number 0. The ASCII number of the cipher key is then converted to hexadecimal number and represented in matrix which size 4 x 4.

Input cipher key: "prodi matematika"

Each input entered will be converted to ASCII number. So, the ASCII number of inputted cipher key is:

110 172 73 99 62 176 85 60 90 145 103 115 82 168 96 79

ASCII numbers are converted into hexadecimal and represented in the matrix of 4 x 4 so as to produce the cipher key as follows:

Cipher key:

$$\begin{bmatrix} 6e & 3e & 5a & 52 \\ ac & b0 & 91 & a8 \\ 49 & 55 & 67 & 60 \\ 63 & 3c & 73 & 4f \end{bmatrix}$$

The next stage is RotWord. This stage is used to generate the first column in the first sub key (Wi), then to shift each byte in the last column of the cipher key cyclically up one time.

$$\text{RotWord: } \begin{bmatrix} 52 \\ a8 \\ 60 \\ 4f \end{bmatrix} \rightarrow \begin{bmatrix} a8 \\ 60 \\ 4f \\ 52 \end{bmatrix}$$

The results of RotWord at this stage are then substituted with the S-Box table that has been set.

$$\text{Subword: } \begin{bmatrix} a8 \\ 60 \\ 4f \\ 52 \end{bmatrix} \rightarrow (\text{S} - \text{Box}) \rightarrow \begin{bmatrix} c2 \\ d0 \\ 84 \\ 00 \end{bmatrix}$$

The last stage to get the column key into (W_i) is the XOR process to the sub word result with the corresponding R-con value. XOR process is then done again with the column (W_{i-4}). At this stage, hexadecimal numbers are changed first to binary numbers to be able to do XOR operations. The process is as follows:

$$\begin{bmatrix} c2 \\ d0 \\ 84 \\ 00 \end{bmatrix} \oplus \begin{bmatrix} 01 \\ 00 \\ 00 \\ 00 \end{bmatrix} \oplus \begin{bmatrix} 6e \\ ac \\ 49 \\ 63 \end{bmatrix}$$

The following is XOR operation using binary number:

$$\begin{bmatrix} 11000010 \\ 11010000 \\ 10000100 \\ 00000000 \end{bmatrix} \oplus \begin{bmatrix} 00000001 \\ 00000000 \\ 00000000 \\ 00000000 \end{bmatrix}$$

$$\oplus \begin{bmatrix} 01101110 \\ 10101100 \\ 01001001 \\ 01100011 \end{bmatrix} = \begin{bmatrix} 10101101 \\ 01111100 \\ 11001101 \\ 01100011 \end{bmatrix}$$

Result from binary XOR operations is $\begin{bmatrix} 10101101 \\ 01111100 \\ 11001101 \\ 01100011 \end{bmatrix}$

if it changes in hexadecimal, it is $\begin{bmatrix} ad \\ 7c \\ cd \\ 63 \end{bmatrix}$.

So the result for the first sub key of the first column is $= \begin{bmatrix} ad \\ 7c \\ cd \\ 63 \end{bmatrix}$

Furthermore, to get the first sub key to the second to fourth column, XOR operations are carried out between W_i and column W_{i-3} . Similar step is carried out to get the third and fourth columns in the first key sub.

The second column of the first sub key

$$(W_{i+1}) = \begin{bmatrix} ad \\ 7c \\ cd \\ 63 \end{bmatrix} \oplus \begin{bmatrix} 3e \\ b0 \\ 55 \\ 3c \end{bmatrix} = \begin{bmatrix} 93 \\ cc \\ 98 \\ 5f \end{bmatrix}$$

The third column of the first sub key

$$(W_{i+2}) = \begin{bmatrix} 93 \\ cc \\ 98 \\ 5f \end{bmatrix} \oplus \begin{bmatrix} 5a \\ 91 \\ 67 \\ 73 \end{bmatrix} = \begin{bmatrix} c9 \\ 5d \\ fb \\ 6c \end{bmatrix}$$

The fourth column of the first sub key

$$(W_{i+3}) = \begin{bmatrix} c9 \\ 5d \\ fb \\ 6c \end{bmatrix} \oplus \begin{bmatrix} 52 \\ a8 \\ 60 \\ 4f \end{bmatrix} = \begin{bmatrix} 9b \\ f5 \\ 9b \\ 23 \end{bmatrix}$$

So the first sub key is $\begin{bmatrix} ad & 93 & c9 & 9b \\ 7c & cc & 5d & f5 \\ cd & 98 & fb & 9b \\ 63 & 5f & 6c & 23 \end{bmatrix}$

The above processes are repeated as many as 10 iterations to produce 10 sub keys used for the encryption and decryption process.

4.2 Encryption and Decryption

The input is in the form of a greyscale image, then represented in matrix according to the pixel size of the image. The AES algorithm operates using blocks cipher so that the matrix of the image will be partitioned into blocks of size corresponding to the type of AES used.

Design on this system uses AES 128 so that the pixel value matrix of the image is entered in the partition into blocks 4 x 4 and represented in hexadecimal numbers. If the last partition of the element does not reach 16 bytes, it will add dummy of element 0 to 16 bytes.

The first is to put the digital image that will be used with the size of 32 x 32. The image that this inputted can be any image as long as it is at the same size with the limits set. The following is the result of encryption and decryption of the image.

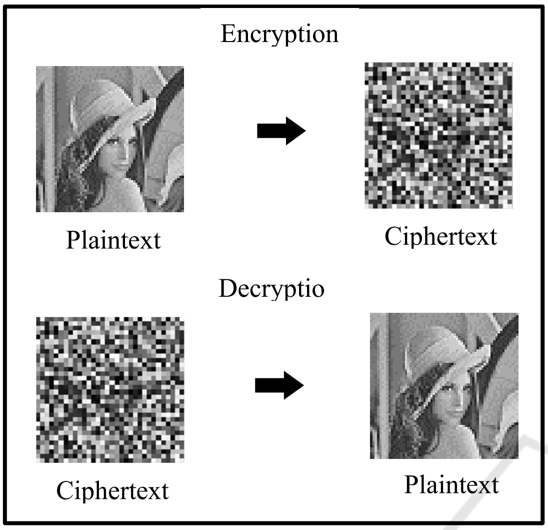


Figure 9: Flowchart of Decryption Process

From the encryption and decryption process, it has been found that the AES method can be used to encrypt images. The images that become ciphertext can be returned or decrypted to the original plaintext.

4.3 Testing

Testing in this study is a test carried out on encryption results. The encrypted image will be attacked in the form of crop, blur, and enhancement. This attack can do inside or outside the process using supporting applications. Testing on the decryption process of the ciphertext that has been attacked aims to determine the resistance of the AES method against the attack. The result of tests are as shown ini Figure 10:

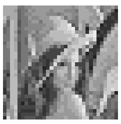
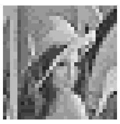
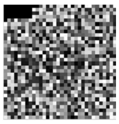
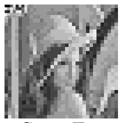
Encryption & Decryption	 Original Image	 Image of Encryption Results	 Image of Decryption Result
Cropping	 Ciphertext Encryption Result	 Cropping of Encryption Image	 Crop Test Result of Image Decryption
Blurring	 Ciphertext Encryption Result	 Blurring of Encryption Image	 Blur Test Result of Image Decryption
Enhanceme nt	 Ciphertext Encryption Result	 Enhancing of Encryption Image	 Enhancement Test Result of Image Decryption

Figure 10: Results of Attack Tests

From the result of attacks test on the ciphertext, it can be seen that:

- Test of cropping attacks on ciphertext can still recognize the original plaintext. Although the cropping area is different, the original plaintext can still be detected clearly. This is because the process at the decryption stage on each block has no effect on other blocks. This cropping is only partial so the decryption changes only on the block affected by the cropping. For other blocks, it is still able to properly prune the initial plaintext. So, in this test, the Advanced Encryption Standard (AES) method is resistant to cropping attacks.
- Test of blurring attack performed on ciphertext affects the decryption process so the result of this testing attack can not return the original plaintext. This is because the blurring process changes the existing pixel values in the ciphertext image matrix and it affects the decryption process as well. Therefore, decryption of the ciphertext image that has been blurred can not restore to the original plaintext. So, the Advanced Encryption Standard (AES) method is not resistant to blur attacks.
- Testing the ciphertext with enhancement attack produces a different plaintext, or in other words, plaintext can not return to the original image because the enhancement process changes the

pixel value of the image matrix, which is very influential on the decryption process. In the process of ciphertext decryption that has been done, enhancement is not able to restore the original plaintext. So, the Advanced Encryption Standard (AES) method is also not resistant to Enhancement attacks.

This research of encryption and decryption was carried out on an image by adding attack testing. From several attack tests that have been carried out on ciphertext to determine the resistance of the AES method, it was found that the determinant of the success or failure of the decryption process of the image file depends on the pixel value. When the pixel value of the encrypted image is changed, the decryption process have been successful, but it cannot restore the plaintext image. So, the key for the success of endurance testing is that the attack cannot change the pixel value. Whereas the cropping process changed only the pixel value, which is partial of the image, so that the other pixel values remain. It makes the encrypted image that has been cropped still recognizable, but if the cropping of the image is very large, then there is possibility that the decrypted image will not be able to be recognized. Because the blurring and enhancing process can change the pixel value of the image, the decryption process cannot restore the original image. It can be concluded that the AES method is resistant to cropping attacks, but is not resistant to blurring and enhancement attacks.

The result of the research is that advanced encryption standard (AES) method still have weakness. Although the attacker cannot solve or find the key, but if they attack the ciphertext using blurring or enhancement, it can prevent the recipient from opening the plaintext. Result of this research is expected to be an input to improve Advanced Encryption Standard (AES) method.

5 CONCLUSIONS

The Advanced Encryption Standard (AES) algorithm was successfully applied to encrypt an image. In the decryption process, this method can restore plaintext as clear as before.

Attack test is given on the ciphertext by cropping, blurring, and enhancing. It is found that this method can recognize plaintext clearly for cropping attacks only. However, for the other two attacks, it cannot recognize the original plaintext. It can be concluded that the Advanced Encryption Standard (AES) method is a method that is resistant to cropping attacks and is not resistant to blurring attacks and enhancements. So, this method still has weakness that when the attacker performs attacks, such as blurring and enhancement of the ciphertext image, the recipient cannot open the original plaintext.

REFERENCES

Arya, A. (2016). *Effective AES Implementation* . IJECET

Buchholz, J. J., 2001. *Advanced Encryption Standard.* s.l.:s.n.

Darmawan, I. (2011). *Gmail Hacked, US-China on the verge of Cyber War.* Jakarta: VIVA.

Deshmukh, P. (2016). *An Image Encryption And Decryption Using AES Algorithm* . *IJSER* , 7.

Hanifah, F. (2012). Aplikasi Algoritma Rijndael Dalam Pengamanan Citra Digital. Skripsi

Joan Daemen, Vicent Rijmen, 2002. *The Design of Rijndael.* New York: Springer-Verlag Berlin Heidelberg.

Kromodimoeljo, S. (2009). Teori Dan Aplikasi Kriptografi. Jakarta: Spk It Consulting

Munir, R. (2006). *Cryptography.* Bandung: Informatika Bandung.

Publications, F. I. (2001). *Announcing the Advanced Encrytion Standard.* New York: National Institute of Standarts and Technologys

Rahmat, A. (2016). *Thief 117 LinkedIn passwords arrested in Czech.* Czech: PT. Net Mediatama Indonesia.

Rahmatullah. *Design of File Cryptography Applications Using the Advanced Encryption Standard (AES) Method* . 2016 . Surabaya. Journal of ITS

Soleh, M. (2010). *Analysis and Implementation of Watermarking with AES Algorithm for Giving Data on Copyright on Audio Files* . *UIN Syarif Hidayatullah* , Jakarta.

Yoga Palilianto. *Design of Encryption Applications And Digital Image Descriptions Using Java-based Rijndael Algorithms SE* .2014.