1

by A L

Journal of Physics: Conference Series

PAPER · OPEN ACCESS

Enhancement security AES algorithm using a modification of transformation ShiftRows and dynamic S-box

Enhancement security AES algorithm using a modification of transformation ShiftRows and dynamic S-box

Alamsyah*, B Prasetiyo, and M N Ardian

Department of Computer Science, Universitas Negeri Semarang, Indonesia

*Corresponding author: alamsyah@mail.unnes.ac.id

Abstract. AES algorithm is a popular encryption algorithm and has a strong resistance to a variety of attacks, especially linear and differential attacks. However, it is necessary to modify the algorithm to improve the performance of the AES algorithm so that the encryption produced (ciphertext) is more resistant from various types of attacks. In this paper, the increased strength of encryption in the AES algorithm uses a modified ShiftRows transformation and dynamic S-box. Modifications to the transformation of ShiftRows are used to simplify the encryption process, while dynamic S-box is used to randomize S-box. The data used in this paper are image data sets. The results of image encryption were tested using histogram analysis, correlation analysis, information entropy, and sensitivity analysis. Based on the test results obtained the ideal range value is 26.76114. This value is better than the results of previous studies.

1. Introduction

The Advanced Encryption Standard (AES) algorithm is one of the modern cryptographic algorithms that implement encryption in cipher block format [1]. The AES algorithm can be applied to image encryption by changing the value of each pixel block with the pixel block value resulting from the encryption process [2]. Plaintext in the image is obtained from the process of reading the color intensity information of each pixel in each color channel in an image, so the output value will be represented in the form of pixel color intensity values in the appropriate color channel [3].

Although the security of AES algorithm encryption has been recognized, the AES algorithm still has weaknesses. Lacko-Bartošová succeeded in carrying out linear attacks and differential cryptanalysis in the AES algorithm two rounds and obtained 8 subkey bits. Both attacks are carried out by analyzing the input, output, and complexity of the S-box [4]. In addition, Nyberg's research showed that the AES algorithm was still susceptible to attacks by linear cryptanalysis by using a ciphertext analysis to get the plaintext [5]. The use of static S-boxes is one of the causes of the vulnerability of the AES algorithm [6].

The AES algorithm has many components that can be modified, one of them is the process of shiftrows transformation and the use of dynamic S-boxes. The shiftrows transformation process works by shifting the state array to the left or right in warping [7]. In each round in the AES algorithm, the shiftrows transformation process will always be carried out in the same way. By simply modifying the shiftrows transformation process [8], there is an increase in the ciphertext entropy value from 7.9989 to 7.9992 assuming that the value 8 is the highest value. Meanwhile, the S-box table functions as a table of a search for substitute values in each SubBytes process. The S-box table is used in the encryption process, while the inverse S-box table is used in the decryption process [9]. Dynamic S-box means the

use of S-boxes with values that can change. Replacement of S-boxes in dynamic versions in Zobeiri and Maybodi studies [9] can increase the level of security of S-boxes.

The purpose of this study is to improve the security of the AES algorithm using modified shiftrows transformation with dynamic S-boxes on the implementation of image encryption. The data used in this study are "Standard" test images obtained from www.imageprocessingplace.com with an additional 2 solid images. The total data used is 10 images.

2. Method

2.1. Modified Shiftrows Transformation

Modification of shiftrows transformation is executed by an algorithm:

(1) If state [0] [0] = even, then go to step two. If state [0][0] = odd, then go to step 3.
(2) Shift according to the Shiftrows process on lines 1 and 3.
(3) Shift according to the Shiftrows process on lines 1 and 2.

With this algorithm, there is no additional process of encryption or decryption [10] which reduces the process but adds data security and encryption speed [11].

2.2. Dynamic S-box

Based on research by Alamsyah et al. [12][13][14][15], the best S-box is composed of a combination of irreducible polynomial $m(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x + 1$ and an affine matrix such as Figure 1.

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Figure 1. The proposed AES affine matrix.

Dynamic S-boxes are obtained by randomizing the value of additional bit constants from 0 to 255. So that with a combination of polynomial irreducible and affine mapping matrix 256 S-boxes are formed [12] [14]. In this study, the S-box used changes each round in one process of encryption or decryption. Replacement of S-boxes is carried out according to the additional bit constants of many rounds according to the type of AES. These additional bit constants are used as S-box indexes. The S-box index is determined by the Fibonacci sequence with the first and second values obtained from the results of XOR per byte in cipherkey. The third value until the last value is obtained from the sum of the previous 2 index values in GF (2^8).

3. Result and discussion

The data used in this study are "Standard" test images obtained from www.imageprocessingplace.com with an additional 2 solid images. The data used is divided into 4 types, i.e., grayscale images with 256 x 256 pixels resolution, color images with 256 x 256 resolution, grayscale images with 512 x 512 pixels resolution, and color images with 512 x 512 pixels resolution. All data used is shown in Figure 2 to Figure 11. The displayed image has been reduced and adjusted.

Figure 2. all_black_256

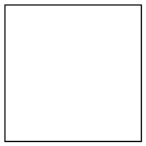

Figure 3. all_white_256

Figure 4. lena_gray_256

Figure 5. lena_color_256

Figure 6. cameraman

Figure 7. house

Figure 8. peppers_gray

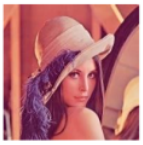

Figure 9. lena_color_512

Figure 10. mandril_color

Figure 11. peppers_color

Each image is encrypted using a standard AES algorithm hereinafter called algorithm 0, the AES algorithm with shiftrows transformation modification only hereinafter called algorithm 1, and the proposed AES algorithm hereinafter called algorithm 2. Each type of AES algorithm used is run in three types of AES namely AES -128, AES-192, and AES-256. The tested images are also run with each cipher block mode in sequence, i.e., ECB, CBC, CFB, OFB, and CTR so that each image will produce a total of 15 different images in each type of algorithm used. The initialization vector (IV) used in each mode is "1111111111111111". Cipherkey used is "1234567890123456" for type AES-128, "123456789012345678901234" for type AES-192, and "12345678901234567890123456789012" for type AES-256. Each data that has been encrypted is tested using testing methods, namely histogram analysis, correlation analysis, information entropy, and sensitivity analysis. The encryption results of each image in each type of algorithm are averaged and compared to draw conclusions. studies.

3.1. Histogram Analysis

Referring to the results of Wadi and Zainal's research [16], histograms of original images or photos with cipher images must have different distribution values so that cipher image is not easy to carry out statistical attacks. To see the difference in histograms, in this study histogram analysis, was calculated based on the number of differences in the value of the cipher image histogram with the original image histogram at the intensity value of 0 – 255, so that there are 256 maximum differences. The final results of the average number of differences in histograms on histogram analysis can be seen in Table 1.

Table 1. The final results of the average number of different histograms.

Algorithm	Grayscale	Red	Green	Blue
0	239.6222222	246.0733333	102.3133333	102.3
1	239.5666667	246.0066667	102.2666667	102.28
2	239.5888889	246.0466667	102.2866667	102.2666667

3.2. Correlation Analysis

In Figure 2 to Figure 11, each adjacent pixel usually has a high correlation [16]. In a good encryption scheme, the correlation between adjacent pixels must produce a value close to 0. To find out the correlation value between the first pixels select N pairs of pixels x and y randomly, pixels x and y are

adjacent pixels. Adjacent pairs can be selected horizontally, vertically, diagonally, and diagonally (diagonally counters). Then, calculate each pixel pair with Equations 1 - 4 [9].

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (1)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (2)$$

$$cov(x,y) = E\left[\left(x - E(x)\right)\left(y - E(y)\right)\right] \quad (3)$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (4)$$

Where:

$x = \{x_i\}, y = \{y_i\}$. x_i and y_i = pixel pairs that are processed.

The final results of the correlation analysis test can be seen in Table 2. The best algorithm obtained is algorithm 2 with an average value of 0.0177. The average value in the correlation analysis test is calculated from the absolute average horizontal, vertical, diagonal, and diagonal counter values. Absolute value is used because the value of the correlation analysis can be a negative value.

Table 2. Final results of testing correlation analysis.

Algorithm	Hor.	Ver.	Diag.	Ctr. Diag.	Avg.
0	0.0022	0.0460	0.0014	0.0026	0.0238
1	-0.0076	0.0453	-0.0077	-0.0074	0.0222
2	-0.0038	0.0459	-0.0035	-0.0049	0.0177

3.3. Information Entropy

In image encryption, entropy is defined as the level of measurement of the randomness of information that can interpret the source or shape of the information on average [17]. The entropy calculation is expressed in Equation 5.

$$H(x) = \sum_{i=0}^{2^N-1} P(x_i) \log_2 \frac{1}{P(x_1)} \quad (5)$$

$P(x_i)$ state the number of possibilities x_i. In an image, the maximum possible pixel value is 256 or 2^8. Thus, with Equation 5 the maximum entropy value produced is 8. The final results of information entropy testing can be seen in Table 3. The best algorithm obtained is algorithm 2 with an average value of 7.829647777.

Table 3. The final result is testing information entropy.

Algorithm	Information Entropy
0	7.828525996
1	7.827663534
2	7.829647777

3.4. Sensitivity Analysis

Sensitivity analysis is used to calculate the significance value of ciphertext with cipher key or plaintext with minimal differences. Sensitivity analysis is divided into two types, namely key sensitivity and plaintext sensitivity. Key sensitivity is applied by comparing the cipher image obtained from A key with the cipher image obtained from key A by changing one value of one bit. Meanwhile, plaintext sensitivity is applied by comparing the cipher image obtained from the A test image with the A test image by changing one bit with the same key. In general, sensitivity analysis will calculate the NPCR value (number pixel changes the rate) with Equation 6 and UACI (unified average changing intensity) with Equation 7[15]. The best value that can be obtained from NPCR and UACI is 100%.

$$NPCR = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|Sign\left(C_1(i,j) - C_2(i,j)\right)\right| x\ 100\% \quad (6)$$

$$UACI = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\frac{Sign\left(C_1(i,j) - C_2(i,j)\right)}{255-0}\right| x\ 100\% \quad (7)$$

Where:

C1 and C2 are images to test. The sign (x) function will result in a value of 1 if x> 0, value 0 if x = 0, and value -1 if x <0.

Table 4. Final results of sensitivity analysis testing.

Algorithm	Key Sensitivity (%)		Plaintext Sensitivity (%)		Average (%)	
	NPCR	UACI	NPCR	UACI	NPCR	UACI
0	99.6278	33.3643	39.8445	13.3809	69.7362	23.3726
1	99.5443	33.3515	39.8436	13.3858	69.6940	23.3686
2	99.6271	33.4259	39.8439	13.3902	69.7355	23.4080

3.5. Comparison of results

The final results on each test method on algorithm 0, algorithm 1, and algorithm 2 are compared to obtain detailed results of the comparison of each algorithm. The following results of the comparison of the results of cipher image testing for each algorithm can be seen in Table 5, and the distance with the ideal values from cipher image testing for each algorithm can be seen in Table 6. between one algorithm and another.

Table 5. Results of cipher image testing for each algorithm.

Alg.	Histogram Analysis		Correlation Analysis Average	Information Entropy	Sensitivity Analysis (%)	
	Grayscale	Color			NPCR	UACI
0	239.6222222	255.7611111	0.0238	7.828525996	**69.7362**	23.3726
1	239.5666667	255.6777778	0.0222	7.827663534	69.694	23.3686
2	239.5888889	255.7055556	**0.0177**	**7.829647777**	69.7355	**23.408**

Table 6. Distance with ideal values for cipher image testing for each algorithm.

Alg.	Correlation Analysis	Information Entropy	Sensitivity Analysis (%)		Average
			NPCR	UACI	
0	0.0238	0.171474	**30.2638**	76.6274	26.77162
1	0.0222	0.1723365	30.306	76.6314	26.78298
2	**0.0177**	**0.1703522**	30.2645	**76.592**	**26.76114**

The bold sign shows the best value compared to other algorithms.

Based on Table 5 to Table 6, the proposed algorithm is the safest algorithm compared to the other two algorithms. This is evidenced by the distance value of the proposed cipher image algorithm which has the least value compared to the other two algorithms.

4. Conclusion

In this study, cipher image generated through the proposed AES algorithm (algorithm 2) was tested using histogram analysis, correlation analysis, information entropy, and sensitivity analysis then the results were compared with the results of the cipher image test on the standard AES algorithm (algorithm 0) and the AES algorithm with modifications shiftrows transformation only (algorithm 1). The result, the distance to the ideal value of cipher image algorithm 0 testing has a value of 26.77162, algorithm 1 has a value of 26.78298, and algorithm 2 has a value of 26.76114. So that cipher image algorithm 2 is

safer than the other two algorithms because the distance to the ideal value of the proposed cipher image algorithm test has the least value compared to the other two algorithms.

References

[1] Stallings W 2017 *Cryptography and Network Security: Principles and Practice* Seventh Ed. (Pearson)
[2] Amani H. R. and Yaghoobi M., 2019 *Multimed. Tools Appl.* **78** 21537
[3] Li M, Lu D, Xiang Y, Zhang Y, and Ren H 2019 *Nonlinear Dyn.* **1**
[4] Lacko-Bartošová L 2011 *Tatra Mt. Math. Publ.* **50**(1) 51
[5] Nyberg K 2018 *Cryptogr. Commun.*(Springer) published online 25 Agustus 2018
[6] Xu G, Zhao G, and Min L 2009 *Proc. - 2009 IEEE Int. Conf. Intell. Comput. Intell. Syst. ICIS 2009* Vol **2** p 473
[7] Paar C and Pelzl J 2010 *Understanding Cryptography* 1st ed. (Springer-Verlag Berlin Heidelberg) vol 1
[8] Kamali S. H., 2010. *2010 Int. Conf. Electron. Inf. Eng.* Vol **1** 141
[9] Daemen J and Rijmen V 2000 *Smart Card Res. Apllication* **1820** 277
[10] Choudhury K P and Kakoty S 2017 *Int. J. Curr. Res. Rev.* **9**(22) 31
[11] Shtewi A., Hasan B E, and Hegazy A E F 2010 *Int. Conf. Electr. Eng.* **7**(7) 1
[12] Alamsyah, Bejo A and Adji T B 2018 *Nonlinear Dyn.* **93**(4)
[13] Alamsyah, Bejo A, and Adji T B 2019 *J. Phys. Conf. Ser.* **1321**(3)
[14] Alamsyah, Bejo A, and Bharata Adji T 2017 *2017 IEEE Conference on Dependable and Secure Computing* p 366
[15] Alamsyah, Bejo A, and Adji T B 2018 *Proc. 3rd Int. Conf. Informatics Comput. ICIC 2018*, doi: 10.1109/IAC.2018.8780454.
[16] Wadi S M and Zainal N 2014 *Wirel. Pers. Commun.* **79**(2) 811
[17] Zhang Y. *3D Res.* **9**(1) 2

ORIGINALITY REPORT

12%	11%	10%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	repo.uum.edu.my Internet Source	4%
2	iopscience.iop.org Internet Source	2%
3	elar.urfu.ru Internet Source	2%
4	pakar.unnes.ac.id Internet Source	1%
5	Alamsyah, A Bejo, T B Adji. "Enhancement strict avalanche criterion value in robust S-boxes construction using selected irreducible polynomial and affine matrixes", Journal of Physics: Conference Series, 2019 Publication	1%
6	Bigaud, D.. "Models of interactions between process, microstructure and mechanical properties of composite materials--a study of the interlock layer-to-layer braiding technique", Composite Structures, 200501 Publication	1%

7	Shuang Liang, Huixiang Liu, Yu Gu, Xiuhua Guo, Hongjun Li, Li Li, Zhiyuan Wu, Mengyang Liu, Lixin Tao. "Fast automated detection of COVID-19 from medical images using convolutional neural networks", Research Square, 2020 Publication	<1 %
8	P. Czapski, C. Ramon, L. L. Huntsman, G. H. Bardy, Y. Kim. "On the contribution of volume currents to the total magnetic field resulting from the heart excitation process: a simulation study", IEEE Transactions on Biomedical Engineering, 1996 Publication	<1 %
9	cache.freescale.com Internet Source	<1 %
10	filehippo.com Internet Source	<1 %
11	Ho Won Kim, Sunggu Lee. "Design and implementation of a private and public key crypto processor and its application to a security system", IEEE Transactions on Consumer Electronics, 2004 Publication	<1 %
12	e-sciencecentral.org Internet Source	<1 %

Exclude quotes	On	Exclude matches	< 10 words
Exclude bibliography	On		

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7