Journal of Soft Computing Exploration

Security improvement of aes algorithm using s-box modification based on strict avalanche criterion on image encryption

David Topanto[1], Alamsyah[2]
[1,2]Department of Computer Science, Faculty of Mathematics and Natural Sciences,
Universitas Negeri Semarang, Indonesia

Article Info

Article history:

Received Mar 11, 2022
Revised Mar 20, 2022
Accepted Mar 25, 2022

Keywords:

Security improvement
Strict avalanche criterion
Image encryption

ABSTRACT

Communication is something that cannot be separated from humans as social creatures. Images are the most commonly used visual communication in today's era. On the other hand, sending images via wireless networks is very vulnerable to piracy. AES, as one of the best cryptographic algorithms, can be applied as a solution. Even so, the AES algorithm still has weaknesses, which are weak against linear attacks and differential cryptanalysis. One solution to overcome the weaknesses of the AES algorithm is to use a stronger S-box. One of the methods to measure the strength of an S-box is the Strict Avalanche Criterion (SAC). The dataset is divided into four categories based on the image type and size of the pixels. Data that has been encrypted using the proposed algorithm will be compared with data that has been encrypted using the standard AES algorithm. Cipherimages (encrypted data) are tested using histogram analysis, information entropy, and sensitivity analysis. The results obtained from cipher image testing are differences in histogram analysis testing in grayscale and color images. The information entropy value is 0.000131583% better than the AES standard, the NPCR is 0.17613% better than the AES standard, and the UACI value. 0.211148% better than AES standard in sensitivity analysis testing. Based on these data, the proposed algorithm has a higher level of security than the standard AES algorithm on image encryption.

Corresponding Author:

David Topanto,
Department of Computer Science,
Faculty of Mathematics and Natural Sciences,
Universitas Negeri Semarang.
Email: david.topanto@students.unnes.ac.id

1. INTRODUCTION

Not only in the form of text, humans now can communicate with audio, visual, and even audio-visual. Images are the most commonly used visual communication in today's era. Pictures complement spoken and written language in explaining the existence of an object so that images have a very big role in the modern world [1]. The user of image media in visual communication via the internet has increased every year, and this is evidenced by data from the 2020 APJII Internet Survey Report in Indonesia, which has increased by 8.9% from the previous year. While on the other hand, sending images via wireless networks is threatened with being hacked [2]. One solution that can be applied is to use encryption or cryptography. In a broader meaning, cryptography is defined as a tool to maintain message security [3], [4].

Advanced Encryption Standard (AES) belongs to the category of modern cryptography using symmetric keys. AES implements encryption in the block cipher format. AES replaced the Data Encryption Standard (DES) as the Federal Information Processing Standard (FIPS) since 2001. In image encryption, AES will replace the value of each pixel block with a new value from the encryption results. The plaintext is obtained

from the process of reading the color intensity information of each pixel in the image [4, 5] so that the output value will be represented in the form of pixel color values [7].

With its various advantages, AES still has weaknesses. In 2007, by analyzing ciphertext to get the plaintext, Warren D Smith showed that the AES algorithm was still vulnerable to linear cryptoanalysis attacks [8]. Then in 2011, Lacko-Bartošová succeeded in obtaining 8-bit subkeys by performing linear attack and differential analysis on the two-round AES algorithm [9]. The use of a more powerful S-box can be one solution to overcome this problem.

One method to measure the S-box strength is to calculate the value of its Strict Avalanche Criterion (SAC)[10]. SAC calculates the power of the S-box by changing 1-bit input, and it is expected that half of the output bits will change, so the ideal value of SAC is 0.5. If the SAC value of an S-box gets closer to 0.5, the stronger the S-box will be [11].

The data in this study were obtained from www.imageprocessingplace.com with 2 additional images. The data used are 10 images which are then divided into 4 categories based on the type and size of the pixels. The objectives of this research are to increase the security of the AES algorithm by replacing the S-box based on the SAC value[12].

2. METHOD

2.1. Dataset

The data in this study were obtained from www.imageprocessingplace.com with 2 additional images. The data used are 10 images which are then divided into 4 categories based on the type of images and size of the pixels, grayscale images measuring 256 x 256 pixels, color images measuring 256 x 256 pixels, grayscale images measuring 512 x 512 pixels, color images measuring 512 x 512 pixels. The data used are shown in Figure 1 to Figure 10.

Figure 1. *Black_256*

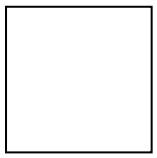

Figure 2. *white_256*

Figure 3. *lena_gray_256*

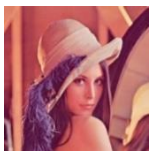

Figure 4. *lena_color_256*

Figure 5. *lena_gray_512*

Figure 6. *mandril_gray*

Figure 7. *peppers_color*

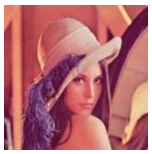

Figure 8. *lena_color_512*

Figure 9. *mandril_color*

Figure 10. *peppers_color*

2.2. Experimental Stage

In this study, images will be encrypted with the standard AES algorithm and the proposed AES algorithm. In each algorithm, the image will be encrypted in 3 types AES, AES-128, AES-192, and AES-256, and for each kind of AES, the image will be encrypted in 5 cipher block modes ECB, CBC, OFB, CFB, and CTR, so that from 1 plaintext image will produce 15 ciphertext images (cipher image) in each algorithm. Cipherkey used for AES-128 is "1234567890123456", for AES-192 is "123456789012345678901234", and for AES-256 is "12345678901234567890123456789012". Initialization Vector (IV) used in each block mode cipher is obtained from the Key Derivation Function (KDF) that cipher key entered [13]. Each encrypted image was tested using the methods histogram analysis, entropy information, and sensitivity analysis. Then the results of these tests are averaged and compared so that conclusions can be drawn. The flow of the proposed AES algorithm design is shown in Figure 11.

Data is read and written in line from the initial pixel or the top-left pixel (0,0) to the right to the end of the image width in the first line, then to the second line, and so on until the last pixel or the bottom right corner pixel (width, length) in one color channel down to the last color channel [14]. The pixel value that is read or written is in the processed channel level range 0 - 255. The value is read as a decimal value so that it can be converted into a binary or hexadecimal value to be processed in the AES algorithm [15]. PKCS#7 [16] padding is used when there is an image that is not in size.

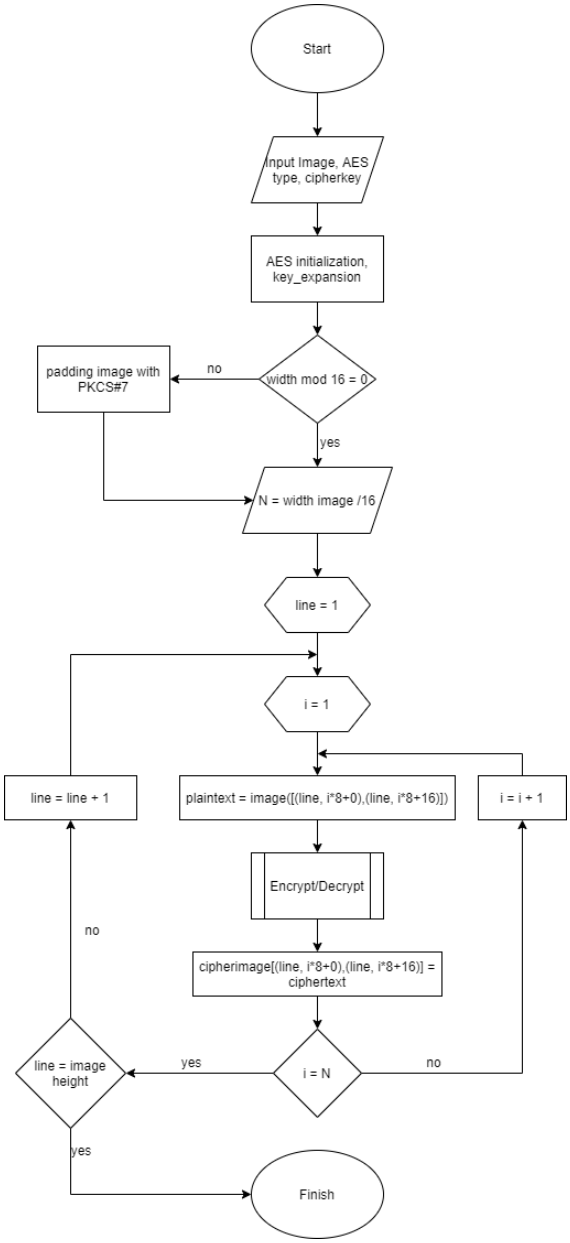

Figure 11. The flowchart of the proposed AES algorithm

2.2.1. *S-box based on SAC value*

In the standard AES algorithm, the irreducible polynomial used to build the S-box is $m(x) = x^8 + x^4 + x^3 + x + 1$ [17]. This S-box has a SAC value of 0,50488. The standard AES algorithm s-box is shown in Figure 12.

	0	1	2	3	4	5	6	7	8	9	0A	0B	0C	0D	0E	0F
0	63	7C	77	7B	F2	6B	6F	C5	30	1	67	2B	FE	D7	AB	76
10	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
20	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
30	4	C7	23	C3	18	96	5	9A	7	12	80	E2	EB	27	B2	75
40	9	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
50	53	D1	0	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
60	D0	EF	AA	FB	43	4D	33	85	45	F9	2	7F	50	3C	9F	A8
70	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
80	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
90	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A0	E0	32	3A	0A	49	6	24	5C	C2	D3	AC	62	91	95	E4	79
B0	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	8
C0	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D0	70	3E	B5	66	48	3	F6	0E	61	35	57	B9	86	C1	1D	9E
E0	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F0	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure 12. S-box AES algorithm standard

Based on the research of Alamsyah et al. [11], the S-box that has an excellent SAC value is constructed with an irreducible polynomial $m(x) = x^8 + x^5 + x^3 + x^2 + 1$ and has a SAC value of 0.49927. The S-box is shown in Figure 13.

	0	1	2	3	4	5	6	7	8	9	0A	0B	0C	0D	0E	0F
0	63	7C	5F	B4	7D	D1	88	48	DF	85	3A	A2	96	F5	45	D
10	8E	64	A3	4F	CF	2F	30	EE	2A	C2	28	1C	70	FE	54	3
20	26	43	53	9E	B0	38	75	35	86	83	F6	DE	CA	94	A5	BD
30	C7	D7	B3	BC	C6	5A	DC	10	EA	E7	AD	8F	F8	89	E0	7A
40	72	49	C0	84	C8	71	2E	18	39	9F	CE	1F	DB	E5	FB	D6
50	22	CC	13	F0	A9	B	E	2D	B7	90	2B	5	0	62	C	74
60	82	ED	8A	5E	B8	15	8C	34	2	51	4C	A1	F	33	69	77
70	14	29	21	57	4	8B	A6	EC	1D	A0	16	E1	11	8	EF	6B
80	EB	B9	C5	7F	B2	A8	23	98	B6	36	6A	DD	76	E2	6D	BB
90	4E	BF	AE	87	6	52	5D	AB	3F	C4	20	FA	9C	78	A	3B
A0	C3	2C	7	E6	E8	AA	19	7E	B5	73	E4	1	D5	1B	F7	6C
B0	9	6F	9A	9B	47	F2	50	AC	61	4D	E3	AF	D4	FF	5B	44
C0	93	1A	24	A7	97	3E	FD	68	3D	4A	58	9D	27	FC	7B	92
D0	60	D2	C9	1E	F4	F3	B1	3C	55	D3	4B	37	66	95	DA	CD
E0	D8	6E	46	C1	42	40	79	41	D0	F1	17	32	81	BE	A4	56
F0	5C	80	31	F9	D9	12	91	8D	E9	59	65	CB	25	BA	67	99

Figure 13. Proposed S-box

The S-box in Figure 13 is used in the proposed algorithm. The S-box has a distance of 0.00073 with the ideal SAC value. In other words, the difference is smaller than the standard AES algorithm S-box which has 0.00488.

2.3. Research Methods

2.3.1. *Histogram Analysis*

The histogram of the original image or photo with the cipher image must have a different value of distribution so that the cipher image is not easily carried out by statistical attacks [18]. To see the difference in the histogram, the number of pixels in the *i-th* size pixel is calculated and then compared with the number of pixels of the *i-th* size of the ciphertext. The value of *i* is an intensity value of 0 – 255, so there is a maximum of 256 differences.

2.3.2. *Information Entropy*

In image encryption, entropy is defined as a measure of the randomness of information that can interpret the source or form of the information on average [7], [18]. The entropy calculation is stated in equation 1.

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

$P(x_i)$ represents the number of possible x_i. Because the maximum pixel value in the possible image is 256 or 2^8, the maximum entropy value that can be generated is 8.

2.3.3. *Sensitivity Analysis*

Sensitivity analysis is used to calculate significant differences in ciphertext by changing to a minimum the cipher key or plaintext. Sensitivity analysis is divided into 2, namely key sensitivity and plaintext sensitivity. Key sensitivity compares the two ciphertexts that are generated from the cipher key and the cipher key, which is changed by one bit. Meanwhile, plaintext sensitivity compares two ciphertexts that are generated from plaintext and plaintext, which is changed by one bit. The sensitivity analysis value is obtained by calculating the NPCR (number pixel change rate) value and the UACI (unified average changing intensity) value. NPCR is shown in equation 2, and UACI is shown in equation 3 [7]. The ideal value that can be generated from the NPCR and UACI is 100%.

$$NPCR = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left| \text{Sign}\big(C_1(i,j) - C_2(i,j)\big) \right| \times 100\% \quad (2)$$

$$UACI = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left| \frac{\text{Sign}(C_1(i,j) - C_2(i,j))}{255-0} \right| \times 100\% \quad (3)$$

Where:
C_1 and C_2 are the images to be tested. The $sign(x)$ function will return the value 1 if $x > 0$, value 0 if $x = 0$, and value -1 if < 0.

3. RESULTS AND DISCUSSIONS

This section presents the results that have been obtained from the research that has been carried out. The results displayed are divided based on the research methods, histogram analysis, information entropy, and sensitivity analysis.

The results of the histogram analysis are shown in Table 1.

Table 1. Histogram analysis results

Algorithm	Grayscale	Red	Green	Blue
AES	239.9555556	255.9333333	255.8333333	255.9833333
Proposed	239.9777778	255.9666667	255.9000000	255.9166667

The result of the information entropy analysis is shown in Table 2. The proposed method has higher value than the algorithm AES standard with a value of 7.837736233.

Table 2. Information entropy results

Algorithm	Information Entropy
AES	7.837725707
Proposed	7.837736233

The results of sensitivity analysis are shown in Table 3. The results of NPCR and UACI were obtained from the average NPCR and UACI key sensitivity and plaintext sensitivity. The proposed method has higher value than algorithm AES standard with an NPCR value of 69.6934% and a UACI value of 23.4140%.

Table 3. Sensitivity analysis results

Algorithm	Key Sensitivity (%)		Plaintext Sensitivity (%)		Average (%)	
	NPCR	UACI	NPCR	UACI	NPCR	UACI
AES	99.6242	33.0171	39.4104	13.3886	69.5173	23.2028
Proposed	99.5430	33.4475	39.8439	13.3804	69.6934	23.4140

To get more detailed results, the results of each method in algorithm AES and proposed algorithm are compared with one another. The results comparison of the cipher image each algorithm in Table 4, and the results comparison of the ideal distance each algorithm's cipher image test are shown in Table 5.

Table 4. The results comparison of the cipher image each algorithm

Alg.	Histogram Analysis		Information Entropy	Sensitivity Analysis (%)	
	Grayscale	Color		NPCR	UACI
AES	239.955556	255.916667	7.837725707	69.5173	23.2028
Proposed	239.977778	255.927778	**7.837736233**	**69.6934**	**23.4140**

Note: The **bold** fonts style shows the best value compared to the other algorithm.

Table 5. The results comparison of the ideal distance each algorithm's cipher image test

Alg.	Information Entropy	Sensitivity Analysis (%)		Average
		NPCR	UACI	
AES	0.162274293	30.4827	76.7972	35.814058542
Proposed	**0.162263767**	**30.3066**	**76.5860**	**35.684960144**

Note: The **bold** fonts style sign shows the best value compared to the other algorithm.

Based on Table 4 and Table 5, the distance between the ideal value of the proposed algorithm is smaller with a value of 35.684960144 than the standard AES algorithm with a value of 35.814058542.

4. CONCLUSION

In this study, the cipher image generated by the proposed AES algorithm was tested using histogram analysis, information entropy, and sensitivity analysis, then the test results were compared with the test results of the standard AES algorithm. As a result, the proposed algorithm is safer than the standard AES algorithm. This is evidenced by the proposed algorithm's ideal value distance smaller than the standard AES algorithm. For future research, the results can be better if the variety of data used is more diverse.

REFERENCES

[1] F. H. Istanto, "Gambar sebagai alat komunikasi visual," *Nirmana*, vol. 2, pp. 23–35, 2000.
[2] H. Cheng, "Partial encryption of compressed images and videos," *IEEE Trans. Signal Process.*, vol. 48, no. 8, pp. 2439–2451, 2000, doi: 10.1109/78.852023.
[3] R. Munir, "Pengantar kriptografi IF5054 kriptografi," *Dep. Tek. Inform. Inst. Teknol. Bandung*, vol. 1, p. 320, 2004.
[4] D. A. A. Pertiwi and D. Djuniadi, "Simulations of text encryption and decryption by applying vertical bit rotation algorithm," *J. Soft Comput. Explor.*, vol. 2, no. 2, pp. 61–66, 2021.
[5] P. Singhai and A. Shrivastava, "An efficient Image security mechanism based on advanced encryption standard," *Int. J. Adv. Technol. Eng. Explor.*, vol. 2, no. 13, pp. 175–182, 2015.
[6] E. Setyaningsih, "Optimasi algoritma super enkripsi untuk meningkatkan pengamanan data citra digitaldalam pengiriman mms pada piranti cerdas," *J. Teknol. Technoscientia*, vol. 5, no. 2, pp. 142–151, 2013.
[7] Y. Zhang, "Test and verification of AES used for image encryption," *3D Res.*, vol. 9, no. 1, pp. 1–27, 2018, doi: 10.1007/s13319-017-0154-7.

[8] W. D. Smith, "AES seems weak linear time secure cryptography," *Work*, vol. 2007, pp. 1–24, 2007.
[9] L. Lacko-Bartošová, "Linear and differential cryptanalysis of reduced-round AES," *Tatra Mt. Math. Publ.*, vol. 50, no. 1, pp. 51–61, 2011, doi: 10.2478/v10127-011-0036-y.
[10] A. Alamsyah, "A novel construction of perfect strict avalanche criterion s-box using simple irreducible polynomials," *Sci. J. Informatics*, vol. 7, no. 1, pp. 10–22, 2020, doi: 10.15294/sji.v7i1.24006.
[11] Alamsyah, A. Bejo, and T. B. Adji, "S-box construction of highly strict avalanche criterion using algebraic technique," *Proc. 3rd Int. Conf. Informatics Comput. ICIC 2018*, pp. 1–4, 2018, doi: 10.1109/IAC.2018.8780454.
[12] A. S. Mabruri, "Data security system of text messaging based on android mobile devices using advanced encrytion standard dynamic," *J. Soft Comput. Explor.*, no. October 2000, pp. 39–46, 2020.
[13] L. Janczewski, H. B. Wolfe, and S. Shenoi, "Security and privacy protection in information processing systems: 28th ifip tc 11 international conference, SEC 2013 Auckland, New Zealand, July 8-10, 2013 Proceedings," *IFIP Adv. Inf. Commun. Technol.*, vol. 405, no. July, 2013, doi: 10.1007/978-3-642-39218-4.
[14] M. N. Ardian, "Improved security of AES algorithm using modified shiftrows transformation with dynamic s-box in image encryption," vol. 6, no. 1, pp. 1–10, 2019.
[15] A. Yosanny, "Perancangan enkripsi pada citra bitmap dengan algoritma des, triple des, dan idea," *ComTech Comput. Math. Eng. Appl.*, vol. 1, no. 2, p. 853, 2010, doi: 10.21512/comtech.v1i2.2618.
[16] B. Kaliski, "PKCS #7: cryptographic message syntax," *Netw. Work. Gr.*, 1998.
[17] J. Daemen and V. Rijmen, "The block cipher rijndael," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 1820, pp. 277–284, 2000, doi: 10.1007/10721064_26.
[18] S. M. Wadi and N. Zainal, "High definition image encryption algorithm based on AES modification," *Wirel. Pers. Commun.*, vol. 79, no. 2, pp. 811–829, 2014, doi: 10.1007/s11277-014-1888-7.