Indonesian Journal of Electrical Engineering and Computer Science
Vol. 19, No. 3, September 2020, pp. 1596~1601
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v19.i3.pp1596-1601

Implementation of a bit permutation-based advanced encryption standard for securing text and image files

Heidilyn V. Gamido
College of Computer Studies, Tarlac State University, Tarlac City, Philippines

Article Info

Article history:

Received Jan 10, 2020
Revised Mar 13, 2020
Accepted Apr 8, 2020

Keywords:

Avalanche effect
Encryption
Image encryption
Mixcolumns
Security

ABSTRACT

The paper proposes a modification of the Advanced Encryption Standard (AES) to address its high computational requirement steaming from the complex mathematical operations in the MixColumns Transformation which makes the encryption process slow. Bit Permutation was used instead of the MixColumns Transformation since the use of bit permutation in an encryption algorithm achieves efficiency by providing minimum encryption time and memory requirement. Results of the study showed that the modified AES algorithm exhibited faster encryption by 18.47% and faster decryption by 18.77% for text files. The modified AES algorithm also resulted to 16.53% higher avalanche effect compared with the standard AES thus improving the security performance. Application of the modified AES in encrypting images in Cipher Block Chaining mode showed that the modified algorithm also exhibited 16.88% faster encryption and 11.96% decryption compared with the standard AES. Likewise, modifying the algorithm achieved the ideal result in the histogram analysis, information entropy, the correlation coefficient of adjacent pixels to resist statistical attack. The ideal value in number of pixels change rate and unified average change intensity were also achieved making the modified algorithm resistant to differential attack. These results show that modifying AES by using bit permutation to replace MixColumns Transformation was able to address the high computational requirement of the algorithm resulting in a faster and more secure encryption algorithm for text files and images.

Corresponding Author:

Heidilyn V. Gamido,
College of Computer Studies, Tarlac State University,
Tarlac City, Philippines.
Email: htvgamido@tsu.edu.ph

1. INTRODUCTION

The exponential growth in the use of computers coupled with the need to protect confidential and essential information from unauthorized and illegal users makes the security of digital data a great challenge in the worldwide communication network [1]. Encryption is used to secure data and protect the confidentiality of data during transmission over the network [2-3]. Encryption algorithms can be categorized as symmetric or asymmetric. Common symmetric encryption algorithms, like Data Encryption Standard (DES), Triple DES (3DES), and AES, are used for encrypting binary data or text.

DES and 3DES are encryption algorithms that were once considered secure but have been proven to be inadequate and unsecured due to vulnerability to differential and linear attack [3-4]. Advanced Encryption Standard (AES) was established by the National Institute of Standards and Technology (NIST) of the United State of America to replace DES and 3DES [5-7]. Since then, AES is considered as the standard for encryption because of its combination of security, performance both in hardware and software, and flexibility [8-10].

Despite the fact that AES is one of the most commonly-used encryption techniques, there is a problem in its higher computational requirement [11-14] due to the complex mathematical operations in the MixColumns Transformation [14] causing a slow encryption process [15].

Bit permutation technique offers a solution to the slow encryption process in AES since the use of bit permutation in an encryption algorithm achieves efficiency by providing minimum encryption time and memory requirement. Bit permutation is also easy to implement since it does not require a complex mathematical computation [16-17]. Bit Permutation, like the MixColumns, provides diffusion in cryptographic algorithms [18].

2. RESEARCH METHOD

The standard and modified AES algorithm were developed in. NET Framework using the Microsoft Visual C# 2015 version 14.0.2543.01. The developed program was used to encrypt text and images. Matlab R2017a was used to test the performance of the modified algorithm in image encryption in terms of histogram analysis, entropy, correlation coefficient, NPCR, and UACI. The study was developed and tested using a laptop computer with Intel ® Core ™ i5-7th Gen processor, 3.10GHz CPU speed, 8GB DDR3 RAM with 1TB HDD storage and running in a 64-bit Windows 10 OS. The encryption and decryption processes of the modified AES algorithm are shown in Figure 1.

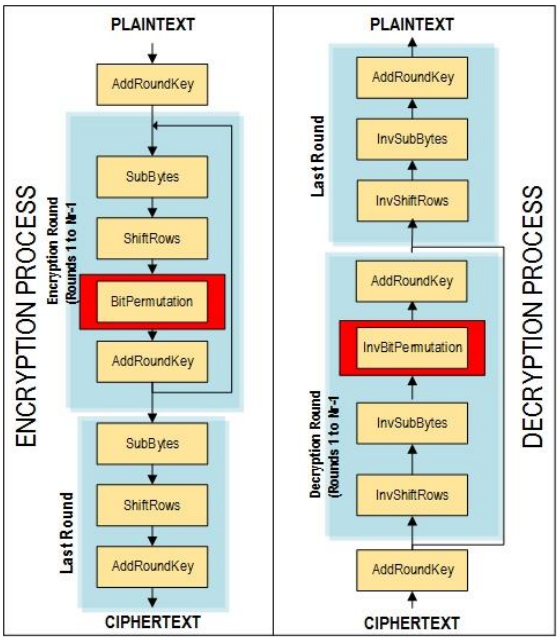

Figure 1. The modified AES process

The modified algorithm consists of the ten rounds following the number of rounds of 128-bit AES. Consequently, the modified algorithm follows the same sequence of transformations of AES. The modification of the algorithm is in the MixColumns Transformation. The Bit Permutation Transformation replaces the MixColumns Transformation of the standard AES during the encryption process. An inverse Bit Permutation transformation is needed for the decryption process [19-20]

3. RESULTS AND ANALYSIS

3.1. Execution time

The modified algorithm was compared to the modifications presented by [13] and [21]. The figure below shows that the modification using multiple S-boxes has the fastest performance among the algorithms while the standard AES has the slowest performance in encrypting text files. The modified AES using bit permutation technique shows that the algorithm has reduced the encryption time of the standard AES by 18.47%.

Figures 2 and 3 show that the modification using multiple S-boxes is the fastest performance among the algorithms while the standard AES has the slowest performance in decrypting text files. The modified AES using bit permutation technique shows that the algorithm has reduced the decryption time of standard AES by 18.77%.

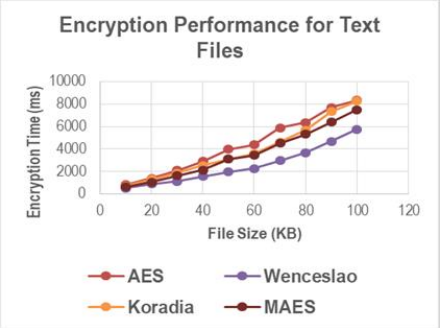

Figure 2. Encryption for text files

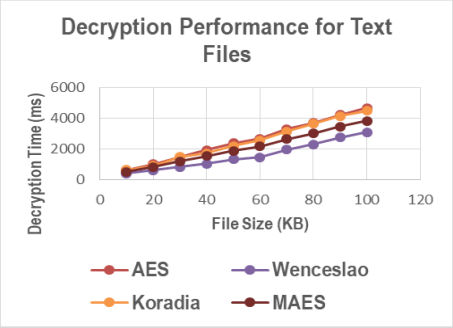

Figure 3. Decryption for text files

Figure 4 shows that the modified algorithm using bit permutation has reduced the encryption of the standard AES 16.88% and reduced the decryption of the standard AES by 11.96% for encrypting images. A faster encryption algorithm for images is needed to provide better security of digital images [22-23].

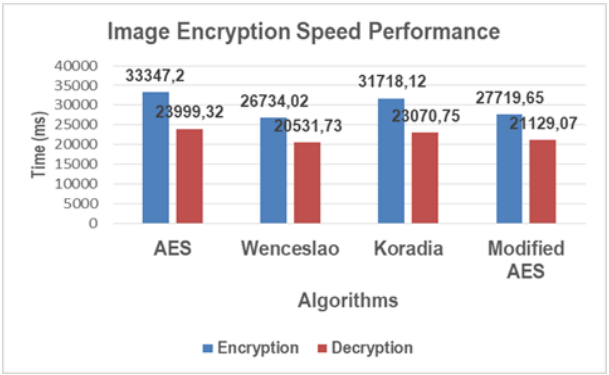

Figure 4. Execution performance for image

3.2. Avalanche effect

Figure 5 shows that the modified algorithm has the highest avalanche effect among the algorithms. The modification using multiple S-boxes indicated that it is the fastest among the algorithms, but suffered greatly in the avalanche effect test where it did not meet the mean value of 50% for all the plaintexts used. A very low value for the avalanche effect compromises the security of the encryption algorithm [24].

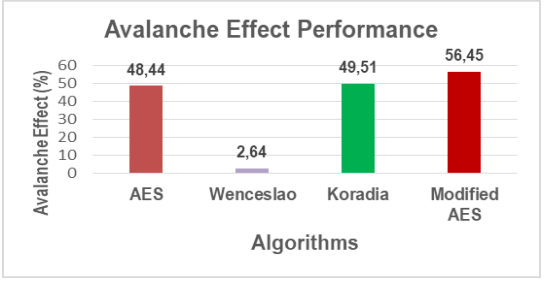

Figure 5. Avalanche effect performance

Figure 6 shows that only the modified AES algorithm has met the 50% mean value of the avalanche effect for the set of plaintexts used and has also improved the security level of the standard AES.

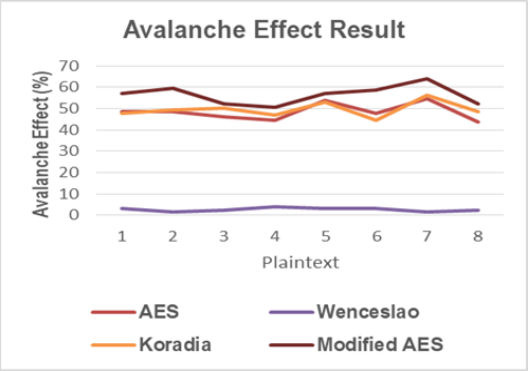

Figure 6. Avalanche effect result

3.3. Statistical attack

In histogram analysis, Figure 7 shows that two histograms are completely different, and the encrypted image has a uniformly distributed histogram which means that a little information about the data is known. The result of the analysis of the histogram shows that the modified algorithm is resistant to statistical attack. For an encryption algorithm to be resistant to statistical attack, it must have a histogram that is entirely different from the plain image and has a uniform distribution of values [25-27].

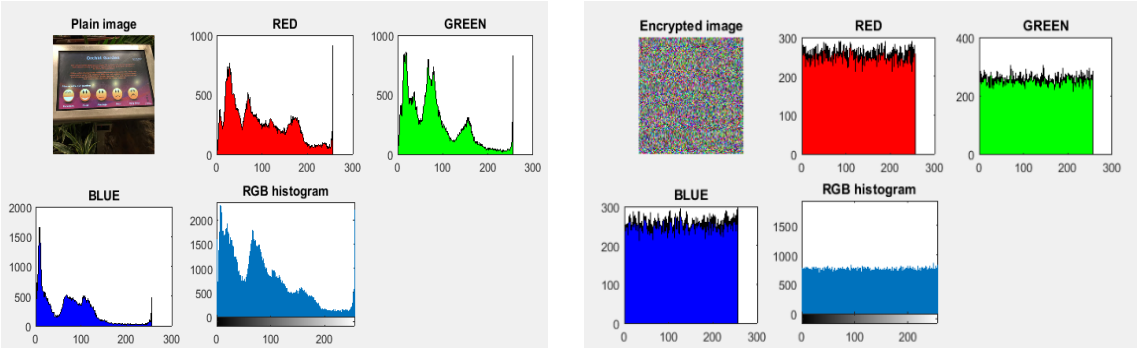

Figure 7. Histogram analysis of plain and encrypted images

The result in Table 1 shows that the correlation coefficient of the plaintext image is close to one which has a very strong correlation. The correlation coefficient of the encrypted image using the modified algorithm is very close to zero which means that there is a weak correlation among adjacent pixels. A correlation coefficient equal to one means that both images are identical and are in perfect correlation and that the encryption process fails because the encrypted image is the same as the plaintext image. A value that is very low or very close to zero means that the plain and encrypted images are completely different [28].

Table 1. Correlation coefficient of MAES

Image	Plaintext image		Encrypted image using the MAES	
	H	V	H	V
Mandril	0.8216	0.8475	-0.0054	-0.0056
Pepper	0.9189	0.9368	-0.0055	-0.0017
Cameraman	0.9300	0.9651	-0.0185	0.0208
Lena	0.9603	0.9809	0.0300	0.0078
Smiley	0.9717	0.9407	-0.0130	-0.0267
Butterfly	0.9875	0.9896	-0.0221	-0.0152

The information entropy result in Table 2 shows that the modified AES has achieved an entropy value approximated to eight (8), which implies that the modified AES has a negligible value of predictability and introduces randomness to the encrypted image.

Table 2. Entropy of MAES

Image	Modified AES
Mandril	7.996
Pepper	7.996
Cameraman	7.999
Lena	7.999
Smiley	7.999
Flower	7.999

3.4. Differential attack

NPCR and UACI are factors to demonstrate that the modified encryption algorithm can strongly resist differential attack [28, 29]. The ideal value of NPCR and UACI is 99.56% and 33.46% respectively [29-31]. However, a higher value than 99.56% for NPCR is better since NPCR focuses on the precise number of pixels that change the value in differential attack. A lower value than 33.46% is better for UACI since UACI concentrates on the average difference between two paired cipher images [30]. NPCR and UACI performance as shown in Table 3.

Table 3. NPCR and UACI performance

File	AES		Modified AES	
	NPCR (%)	UACI (%)	NPCR (%)	UACI(%)
Mandril	99.65	33.53	99.62	33.41
Pepper	99.64	33.46	99.61	33.53
Cameraman	99.63	33.51	99.62	33.38
Lena	99.62	33.5	99.61	33.48
Smiley	99.46	33.43	99.44	33.46
Butterfly	99.47	33.44	99.48	33.47
Average	99.58	33.48	99.56	33.46

4. CONCLUSION

Based on the results of the study, the bit-permutation based AES has improved the standard AES algorithm in terms of encrypting and decrypting text and image files. The modified AES has also improved the avalanche effect of the standard algorithm by 16.53%. The experiments also showed that the modified algorithm is resistant to statistical and differential attacks. The results clearly show that modifying the Advanced Encryption Standards by using bit-permutation to replace the MixColumns Transformation was able to address the high computational requirement of the algorithm resulting in a faster and more secure encryption algorithm for text and image files.

ACKNOWLEDGMENTS

The researcher would want to acknowledge the Tarlac State University for funding the research.

REFERENCES

[1] A. E. Omolara and A. Jantan, "Modified honey encryption scheme for encoding natural language message," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 3, p. 1871, 2019.
[2] S. Dadhich, "Performance Analysis of AES and DES Cryptographic Algorithms on Windows & Ubuntu using Java," vol. 35, no. 4, pp. 179–183, 2016.
[3] A. Verma, S. Kaur, and B. Chhabra, "Design and Development of Robust Algorithm for Cryptography using Improved AES Technique," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. April, pp. 66–82, 2017.
[4] N. Aleisa, "A Comparison of the 3DES and AES Encryption Standards," *Int. J. Secur. Its Appl.*, vol. 9, no. 7, pp. 241–246, 2015.
[5] A. Bulus and E. Bulus, "Cipher with AES," in 2018 3rd International Conference on Computer Science and Engineering (UBMK), pp. 27–30, 2018.
[6] O. C. Abikoye, A. D. Haruna, A. Abubakar, N. O. Akande, and E. O. Asani, "Modified Advanced Encryption Standard Algorithm for Information Security," *Symmetry (Basel).*, vol. 11, no. 12, p. 1484, 2019.

[7] E. M. De Los Reyes, A. M. Sison, and R. P. Medina, "File encryption based on reduced-round AES with revised round keys and key schedule," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 16, no. 2, pp. 897–905, 2019.
[8] P. Kumar and S. B. Rana, "Development of modified AES algorithm for data security," *Optik (Stuttg).*, vol. 127, no. 4, pp. 2341–2345, 2016.
[9] H. Talirongan, A. M. Sison, and R. P. Medina, "Modified Advanced Encryption Standard using Butterfly Effect," *2018 IEEE 10th Int. Conf. Humanoid, Nanotechnology, Inf. Technol. Control. Environ. Manag.*, no. 1998, pp. 0–6, 2018.
[10] E. M. De Los Reyes, A. M. Sison, and R. Medina, "Modified AES Cipher Round and Key Schedule," *Indones. J. Electr. Eng. Informatics*, vol. 7, no. 1, pp. 29–36, 2019.
[11] R. Riyaldhi, Rojali, and A. Kurniawan, "Improvement of Advanced Encryption Standard Algorithm With Shift Row and S.Box Modification Mapping in Mix Column," *Procedia Comput. Sci.*, vol. 116, pp. 401–407, 2017.
[12] B. Bhat, A. W. Ali, and A. Gupta, "DES and AES performance evaluation," *in International Conference on Computing, Communication & Automation*, pp. 887–890, 2015.
[13] F. V Wenceslao, B. D. Gerardo, and B. I. T. Tanguilig, "Modified AES Algorithm Using Multiple S-Boxes," in Second International Conference on Electrical, Electronics, Computer Engineering and their Applications (EECEA2015), vol. 5, no. 1, pp. 1–9, 2015.
[14] R. Rejani and D. V Krishnan, "Study of Symmetric key Cryptography Algorithms," *Int. J. Comput. Tech.*, vol. 2, no. 2, pp. 45–50, 2015.
[15] S. Rehman, S. Q. Hussain, W. Gul, and Israr, "Characterization of Advanced Encryption Standard (AES) for Textual and Image data," *Int. J. Eng. Comput. Sci.*, vol. 5, pp. 18346–18349, 2016.
[16] A. Jolfaei, X.-W. Wu, and V. Muthukkumarasamy, "On the Security of Permutation-Only Image Encryption Schemes," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 2, pp. 235–246, 2016.
[17] H. Ali-Pacha, N. Hadj-Said, A. Ali-Pacha, M. Mamat, and M. A. Mohamed, "An Efficient Schema of a Special Permutation Inside of Each Pixel of an Image for its Encryption," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 11, no. 2, 2018.
[18] N. Tyagi and Priyanka, "A Survey on Ensemble of Modifications on AES Algorithm," *J. Basic Appl. Eng. Res.*, vol. 1, no. 7, pp. 19–24, 2014.
[19] H. V. Gamido, A. M. Sison, and R. P. Medina, "Modified AES for Text and Image Encryption," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 11, no. 3, pp. 942–948, 2018.
[20] H. V Gamido, A. M. Sison, and R. P. Medina, "Implementation of Modified AES as Image Encryption Scheme," *Indones. J. Electr. Eng. Informatics*, vol. 6, no. 3, pp. 301–308, 2018.
[21] V. C. Koradia, "Modification in Advanced Encryption," *J. Information, Knowl. Res. Comput. Eng.*, vol. 2, no. 2, pp. 356–358, 2013.
[22] W. Yao *et al.*, "A Fast Color Image Encryption Algorithm Using 4-Pixel Feistel Structure," *PLoS One*, vol. 11, no. 11, p. e0165937, Nov. 2016.
[23] A. Houas, Z. Mokhtari, K. E. Melkemi, and A. Boussaad, "A novel binary image encryption algorithm based on diffuse representation," *Eng. Sci. Technol. an Int. J.*, vol. 19, no. 4, pp. 1887–1894, 2016.
[24] T. F. G. Quilala, A. M. Sison, and R. P. Medina, "Modified blowfish algorithm," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 11, no. 3, pp. 1027–1034, 2018.
[25] Shivaputra, H. Sheshadri, and V. Lokesha, "A Naïve Visual Cryptographic Algorithm for the Transfer of Compressed Medical Images," *Bull. Electr. Eng. Informatics*, vol. 5, no. 3, pp. 347–365, 2016.
[26] Y. Jain, R. Bansal, G. Sharma, B. Kumar, and S. Gupta, "Image Encryption Schemes : A Complete Survey," *Int. J. Signal Process. Image Process. Pattern Recognit.*, vol. 9, no. 7, pp. 157–192, 2016.
[27] O. Omoruyi, C. Okereke, K. Okokpujie, E. Noma-Osaghae, O. Okoyeigbo, and S. John, "Evaluation of the quality of an image encrytion scheme," *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 17, no. 6, p. 2968, 2019.
[28] C. B. B. Aguila, A. M. Sison, and R. P. Medina, "Enhanced RC6 permutation-diffusion operation for image encryption," in Proceedings of the 2018 International Conference on Data Science and Information Technology - DSIT '18, pp. 64–68, 2018.
[29] V. Shadangi, S. K. Choudhary, and K. A. K. Patro, "Novel Arnold Scrambling Based CBC-AES Image Encryption Novel Arnold Scrambling Based CBC- AES Image Encryption Novel Arnold Scrambling Based CBC-AES Image Encryption," *Int. J. Control Theory Appl.*, no. January, 2017.
[30] S. Toughi, M. H. Fathi, and Y. A. Sekhavat, "An image encryption scheme based on elliptic curve pseudo random and Advanced Encryption System," *Signal Processing*, vol. 141, pp. 217–227, 2017.
[31] X. Tong, Y. Liu, M. Zhang, H. Xu, and Z. Wang, "An image encryption scheme based on hyperchaotic Rabinovich and exponential chaos maps," *Entropy*, vol. 17, no. 1, pp. 181–196, 2015.

BIOGRAPHY OF AUTHOR

Heidilyn V. Gamido is a graduate of Doctor in Information Technology at Technological Institute of the Philippines, Quezon City under the CHED K-12 Transition Program Scholarship. She obtained her Masters of Engineering major in Information and Communications in 2006 at Pai Chai University, Daejeon South Korea on a scholarship. She finished her BS Information Technology at Saint Louis University, Baguio City Philippines in 2002. She is an Associate Professor at Tarlac State University - College of Computer Studies and is designated as the Director of the Management of Information Systems Office. Her research interests include data security, image processing, and information system.