Implementation of image file security using the advanced encryption standard method

Ali Ikhwan[1,2], Rafikha Aliana A. Raof[1], Phaklen Ehkan[1], Yasmin Mohd Yacob[1], Nuri Aslami[3]
[1]Embedded, Networks and Advanced Computing, School of Computer and Communication Engineering, Arau, Malaysia
[2]Faculty of Science and Technology, University Islami Negeri Sumatera Utara, Medan, Indonesia
[3]Faculty of Islamic Economics and Business, University Islam Negeri Sumatera Utara, Medan, Indonesia

Article Info

Article history:

Received Jul 9, 2022
Revised Mar 27, 2023
Accepted Apr 2, 2023

Keywords:

AES 128
Cipher block chaining
Cryptography
Electronic codebook
Mode operation

ABSTRACT

The application of technology in this era has entered digitalization and is modern. Therefore, we are already in an era of advanced and rapid technological development. It has become a human need to exchange information in every activity. Documents that contain information that is frequently sought or used. The document's use also includes essential information. Document security is undoubtedly a significant factor in prioritizing important information in a document to prevent unauthorized people from misusing the document's vital information. Cryptography is a method of overcoming document security issues so that third parties cannot read the information or messages contained within the document. The 128-bit advanced encryption standard (AES) algorithm is one of the algorithms included in the cryptography technique. Additionally, it can be combined with operation modes such as electronic codebook (ECB) and cipher block chaining (CBC) to create an application that can generate random codes to improve the security of the data contained in the document.

Corresponding Author:

Ali Ikhwan
Embedded, Networks and Advanced Computing (ENAC)
School of Computer and Communication Engineering
02600 Arau, Perlis, Malaysia
Email: ali_ikhwan@uinsu.ac.id

1. INTRODUCTION

Image files have characteristics that text data does not have, where image files can provide important information hidden from images. However, confidential image files in a storage medium (hard disks and memory cards) and image files transmitted on a network may cause eavesdropping, modification, or fabrication by certain third parties (crackers). The purpose of the cracker is to find out crucial information hidden in an image, or the cracker wants to break into confidential data behind the characteristics possessed by the image file [1]-[4].

One way to maintain the original information or data is the application of encryption with security codes that are difficult to translate. This encoding technique is called a cryptographic technique. In cryptography there are two main concepts of encryption, namely encryption and decryption by involving a secret key [5], [6]. Cryptography can be divided into symmetric key cryptography and asymmetric key cryptography. In symmetric key cryptography, the key for the encryption process is the same as the key for the decryption process [1], [7], [8]. So, in this case, the sender and recipient of the message have already shared the key before exchanging messages with each other. The advanced encryption standard (AES) method is an encryption method that uses a symmetric key with a key length of 128, 192, and 256 bits to encrypt and decrypt data in 128-bit blocks. The AES method that uses a block cipher system can perform symmetric key encoding operations with the operating mode. In addition, AES has advantages in security, speed, and characteristics of the algorithm and its implementation [3], [9]-[14].

The operating modes that will be applied to the AES method are the electronic codebook (ECB) operating mode and the cipher block chaining (CBC) operating mode which will have different levels of security. Where the ECB operating mode has an operating pattern on N blocks separately with the same K secret key and has no connection between one block and another. While the CBC mode of operation, uses the initial vector input to build the encoding linkage between one block and the next block [15], [16].

Based on the things above, a research was appointed with the title, implementation of image file security using the AES. Method with the hope of establishing security for image files with a comparison of different security levels applied from the operating mode, so that the form of security against confidential image files can be properly secured from unauthorized parties [5], [17].

2. RESEARCH METHOD

2.1. Cryptography

Cryptography was originally described as the study of how to hide messages. However, in the modern sense of confidentiality, data integrity, and entity authentication are all aspects of information security that the science of cryptography addresses. So the notion of modern cryptography is not only dealing with message hiding but more than a set of techniques that provide information security [3], [15], [18]-[22].

Meanwhile, according to Kasiran *et al.* [3] cryptography is a branch of computer science that studies how to hide information. Through cryptography, a secret message is scrambled into a message that seems to be formless, and sent to the intended party. Meanwhile, only the intended party can interpret the random message and turn it back into a secret message from the sender.

2.2. Advanced encryption standard algorithm

AES is a block encoding system that is non-Feistel because AES uses components that always have an inverse with a block length of 128 bits. AES keys can have a key length of 128, 192, and 256 bits. AES encoding uses an iterative process called a round. The number of rounds used by AES depends on the length of the key used. Each round requires a round lock and enter from the next round. The round key is generated based on the key given [13], [17], [19], [23]-[27].

2.3. Key expansion

In the process of encryption and decryption with the AES algorithm, a key (secret key) is needed. The key or secret key will be processed for the formation of key expansion by means of a round key which is carried out 10 times to produce 10 round keys. The key formation process is carried out with several functions, namely Rotword which takes the last column of the primary key matrix that has been entered by the user then performs one cyclic permutation, namely the top byte is rotated into the lowest byte, the rule of the Subword function that uses the SubBytes transformation to substitute each element in word new byte values and the use of an Rcon table as shown in Table 1. Rcon is a determination matrix measuring 10x4 and is used for the exclusive or (XOR) operations in the key generation process [28].

Table 1. Rcon tabel

Round	1	2	3	4	5	6	7	8	9	10
Rcon	01	02	04	08	10	20	40	80	1b	36
	00	00	00	00	00	00	00	00	00	00
	00	00	00	00	00	00	00	00	00	00
	00	00	00	00	00	00	00	00	00	00

S	K	R	I	P	S	I	K	R	I	P	T	O	1	1	1

Figure 1. Key arrangement in alphanumeric/string form

In the following example, an image file will be encrypted with the "SKRIPSIKRIPTO111" key (secret key). The explanation in Figure 1 is the arrangement of keys made in alphanumeric form. With the specified key, the key expansion process will be carried out in several stages, namely:

- Convert keywords that are alphanumeric or string into hexadecimal form which can be seen in Figure 2, then arrange them in state form (4x4 byte matrix) which can be seen in Figure 3. Then the key is arranged in the form of a state (4x4 byte matrix) which can be seen in Figure 3.

53	4B	52	49	50	53	49	4B	52	49	50	54	4F	31	31	31

Figure 2. Key arrangements in hexadecimal form

	1	2	3	4
1	53	50	52	4F
2	4B	53	49	31
3	52	49	50	31
4	49	4B	54	31

Figure 3. Key arrangement with 4x4 state form (secret key**)**

- From the image of the secret key or initial key in an AES algorithm, a key expansion process will be carried out to get round key 1 or round key 1. The secret key will be sorted by column as shown which can be seen in Figure 4.

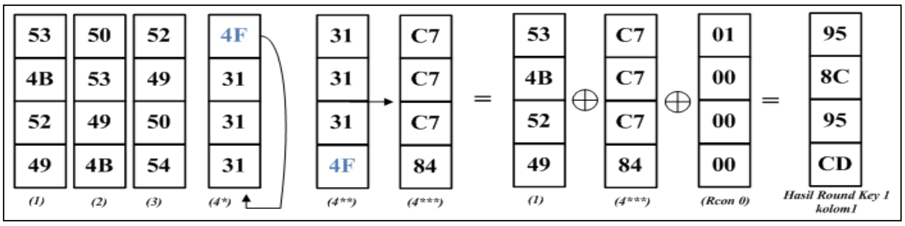


Figure 4. Key arrangement with 4x4 state form (secret key**)**

- In the next element, the 4th (fourth) column is taken to perform the Rotword function and the Subword function. The Rotword function is the transfer or shift of the top bit to the bottom bit, while the Subword function is the use of the SubBytes transformation to substitute each element into the latest byte value according to the substitution table.
- The results of the Rotword function and the Subword function are processed with the exclusive or (XOR) operation with the value in column 1 (one) secret key.
- Furthermore, the value of the operation in step 4 is also processed by the XOR operation against the value in the Rcon table. The Rcon value is processed based on the expansion operation performed. If you are looking for a value for round key 1, then the Rcon value taken is in column 1 (01,00,000.00).
- The results for round key 1 column 1 can be seen in Figure 4.
- To get the value of round key 1 for columns 2, 3 and 4, an XOR operation is performed between the values from the results of the previous column (column 1 round key 1) and the column values that are sought from the round key. For more details can be seen in Figure 5.

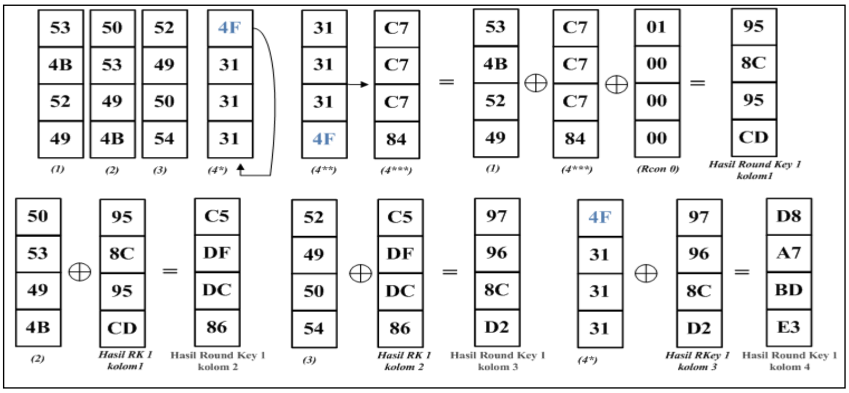


Figure 5. XOR process in columns 2, 3 and 4

2.4. Encryption process

At the encryption stage with the AES algorithm, an image file with portable network graphics (PNG) format will be encrypted based on the red green blue alpha (RGBA) value of each pixel in the file to fill in the plaintext. The entire RGBA value in the PNG file will be divided according to the rules of the AES algorithm, if during encryption the RGBA value of each pixel is less than 128 bits it will be padded until it meets the AES algorithm block size standard. The following is the encryption process for the AES algorithm with 4 types of transformations and the use of CBC and ECB operating modes [29].

2.5. Encryption process with electronic codebook operation mode

In this mode, each plaintext block will perform the encryption process individually and independently into a ciphertext block. The ECB mode of operation is the simplest mode because the encryption workflow that occurs in this operation mode operates to decipher the plaintext with the available key expansion to generate the ciphertext according to the AES algorithm transformation. The following is the process of encrypting a PNG file with the ECB operating mode which can be seen in Figure 6.

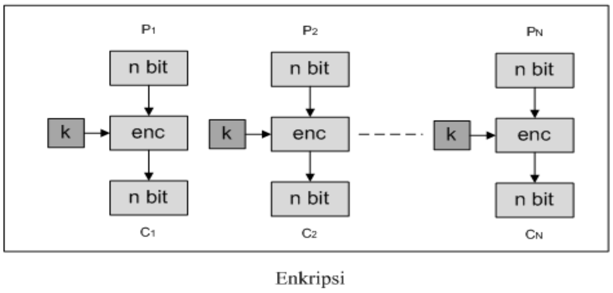


Figure 6. Encryption workflow with ECB operation mode

2.6. Encryption process with cipher block chaining operation mode

CBC operating mode is a mode that works by using an initial vector (IV) with the size of a block (n bits). The ECB operating mode will perform the XOR process between the plaintext and the initial vector so that the original plaintext pattern is not visible during the encryption process. The following is a CBC operation mode encryption workflow on the AES algorithm which can be seen in Figure 7. The encryption process using the CBC operating mode uses the same data or image files as the ECB operating mode, which will encrypt 2 blocks (pixel 1 to pixel 4 and pixel 5 to pixel 8) and use an initial vector.

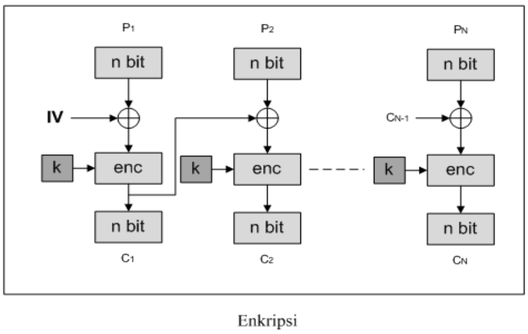


Figure 7. Encryption workflow with CBC operation mode

2.7. Decryption process

The decryption process is the process of returning the ciphertext value to the original value (plaintext). In the decryption process, an inverse transformation is carried out except for the AddRoundKey transformation process which is self-inverse with the condition that it uses the same key as the key expansion process. with InvMixColumns and still produce the same transformation. The following is the AES algorithm decryption process using the operating mode [8], [14], [30], [31].

2.8. Decryption process with electronic codebook operation mode

The decryption process in the ECB operating mode uses the same flow when encrypting. However, in the decryption process, the input that is processed is the ciphertext value. The following is the workflow and process of decrypting the AES algorithm with the ECB operating mode, which can be seen in Figure 8 [15].

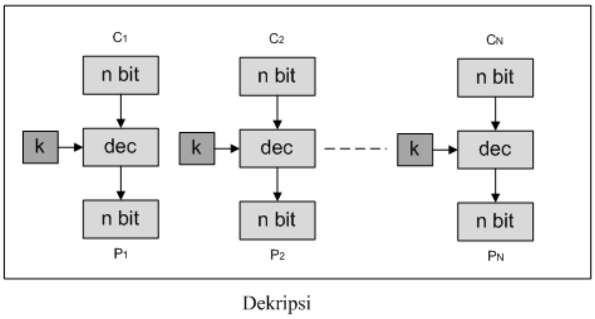


Figure 8. Decryption workflow with ECB operation mode

2.9. Decryption process with cipher block chaining operation mode

The AES algorithm decryption process with CBC encrypts every block separately. An initialization vector (IV) is added to the first block of plaintext before encryption in the CBC mode, and the ciphertext that results is added to the second block of plaintext before encryption, and so on. Decryption is the opposite operation. The receiving party must be informed about the IV and the ciphertext, which need not be kept a secret. which can be seen in Figure 9.

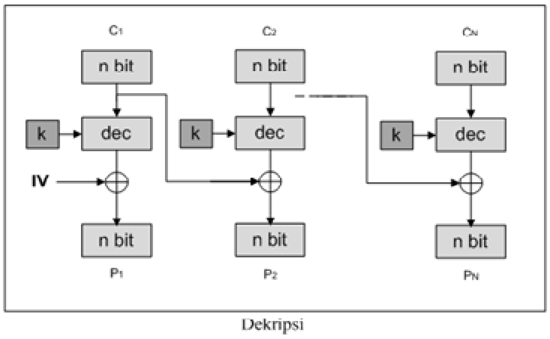


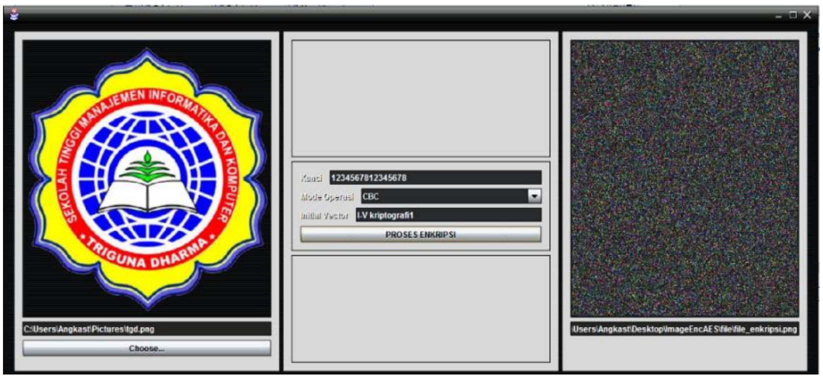
Figure 9. Decryption workflow with CBC operation mode

3. RESULTS AND DISCUSSION

At this stage, the steps in implementing the program system will be explained which will be carried out by encrypting an image. After that a decryption process will be carried out which aims to increase security in the image file. By encrypting the display of images taken by test data using the logo using the AES method, as follows:

3.1. Encryption form display

Encryption form is a form display that displays the process or processes the encryption occurs. In this form there are 3 panels divided by 3 columns. In the first column there is a panel that displays an original image file with a textfield as the image directory information and a choose button to select an image. Then in the second column there are 2 textfields, 1 combobox and a button, namely the key textfield, operation mode combobox, initial vector textfield and the encryption process button. Furthermore, in the third column there is a panel to display the encrypted image or called ciphertext and a textfield of the encrypted file placement directory. This encryption process can be processed if an image file already exists, the key has been entered and the operation mode selection. The initial vector textfield will be active if the CBC operation mode is selected, which can be seen in Figure 10.



C:\Users\Angkast\Pictures\tgd.png

Kunci 1234567812345678

Mode Operasi CBC

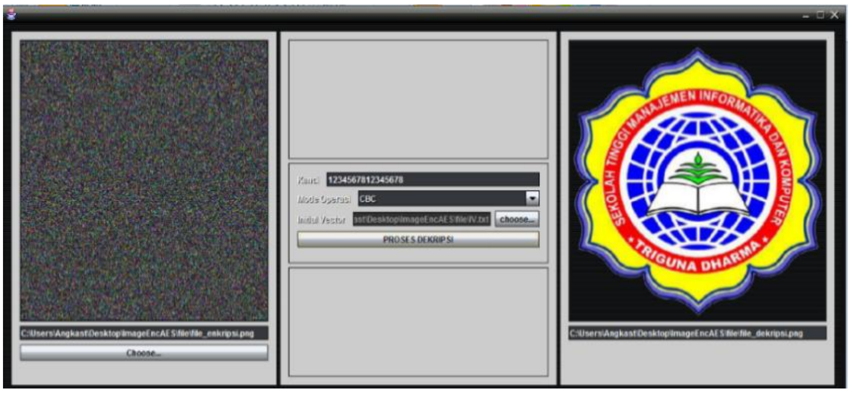
Initial Vector I.V kriptografi1

\Users\Angkast\Desktop\ImageEncAES\file\file_enkripsi.png

Figure 10. Encryption form

3.3. Decryption form display

The decryption form is a form display that displays the process or processes the decryption occurs. In this form there are 3 panels divided by 3 columns. In the first column there is a panel that displays an encrypted image file with a textfield as image directory information and a choose button to select an image. Then in the second column there are 2 textfields, 1 combobox and 2 buttons, namely the key textfield, the operation mode combobox, the initial vector textfield, the button to select the initial vector that was there during the encryption process and the decryption button. Furthermore, in the third column there is a panel to display the decrypted image or called plaintext and a textfield for the decryption file placement directory, which can be seen in Figure 11.



C:\Users\Angkast\Desktop\ImageEncAES\file\file_enkripsi.png

Kunci 1234567812345678

Mode Operasi CBC

Initial Vector ast\Desktop\ImageEncAES\file\IV.txt

C:\Users\Angkast\Desktop\ImageEncAES\file\file_dekripsi.png

Figure 11. Decryption form

4. CONCLUSION

Based on the results of the analysis, design, implementation and testing of the program. The process of securing data in an image file using the AES method is to perform the encryption and decryption process with an RGBA value on a PNG pixel for 128-bit plaintext and a 128-bit key. The security of image files that perform the encryption and decryption process is packaged with one of the operating modes, namely the electronic codebook operation mode and cipher block chaining. Elements of RGBA values are generated from each pixel in the image file with PNG format. The use of the cipher block chaining operation mode is more accurate than the electronic codebook operating mode. The standard advance encryption algorithm is a non-Feistel block encoding system because it uses components that always have an inverse with a block length of 128 bits and processes the encoding with 10 rounds.

ACKNOWLEDGEMENTS

The authors would like to acknowledge Embedded, Networks and Advanced Computing (ENAC) research cluster, school of computer and communication engineering. University Malaysia Perlis (Unimap) Arau, Perlis, Malaysia for their support in guiding the author in producing this journal and providing financial support for this manuscript.

REFERENCES

[1] M. Kumar, D. Dinesh, and D. Naveen, “Improvisation of security aspect of steganographic system by applying RSA algorithm,” *International Journal of Advanced Computer Science and Applications (IJACSA.),* vol. 7, no. 7, pp. 245-249, 2016, doi: 10.14569/ijacsa.2016.070733.

[2] F. Al-Shaarani and A. Gutub, “Securing matrix counting-based secret-sharing involving crypto steganography,” *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 9, pp. 6909-6924. 2021, doi: 10.1016/j.jksuci.2021.09.009.

[3] Z. Kasiran, H. F. Ali, and N. M. Noor, “Time performance analysis of advanced encryption standard and data encryption standard in data security transaction,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 16, no. 2, pp. 988-994, 2019, doi: 10.11591/ijeecs.v16.i2.pp988-994.

[4] M. A. Ahmad *et al.*, “Hiding patients medical reports using an enhanced wavelet steganography algorithm in DICOM images,” *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 10577-10592, 2022, doi: 10.1016/j.aej.2022.03.056.

[5] M. F. U. Farooq, “Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA,” *Journal of King Saud University-Computer and Information Sciences*, vol. 29, no. 3, pp. 295-302, 2007, doi: 10.1016/j.jksuci.2016.01.004.

[6] D. Arraziqi and E. S. Haq, “Optimization of video steganography with additional compression and encryption,” *TELKOMNIKA (Telecommunication, Computing, Electronics and Contro)l*, vol. 17, no. 3, pp. 1417-1424, 2019, doi: 10.12928/TELKOMNIKA.v17i3.9513.

[7] R. Rahim and A. Ikhwan, “Study of three pass protocol on data security,” *International Journal of Science and Research (IJSR)*, vol. 5, no. 11, pp. 102-104, 2016, doi: 10.21275/art20162670.

[8] H. J. Ali, T. M. Jawad, and H. Zuhair, “Data security using random dynamic salting and AES based on master-slave keys for Iraqi dam management system,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 23, no. 2, pp. 1018-1029, 2021, doi: 10.11591/ijeecs.v23.i2.pp1018-1029.

[9] V. Tasril and A. P. U. Siahaan, “Data security using 128-bit advanced encryption standard algorithm,” *International Journal of Scientific Research in Science, Engineering and Technology,* vol. 4, no. 10, pp. 198-205, 2018, doi: 10.31227/osf.io/24yrw.

[10] P. Sethi and V. Kapoor, “A proposed novel architecture for information hiding in image steganography by using genetic algorithm and cryptography,” *Procedia Computer Science*, vol. 87, pp. 61-66, 2016, doi: 10.1016/j.procs.2016.05.127.

[11] V. Tasril and A. P. U. Siahaan, “Data security using 128-bit advanced encryption standard algorithm,” *International Journal of Scientific Research in Science and Technology (IJSRST)*, vol. 4, no. 10, pp. 198–205, 2018, doi: 10.31227/osf.io/24yrw.

[12] C. A. Sari, G. Ardiansyah, D. R. Ignatius, and M. Setiadi, “An improved security and message capacity using AES and huffman coding on image steganography,” TELKOMNIKA *(Telecommunication Computing Electronics and Control)*, vol. 17, no. 5, pp. 2400-2409, 2019, doi: 10.12928/telkomnika.v17i5.9570.

[13] H. V. Gamido, A. M. Sison, and R. P. Medina, “Implementation of modified AES as image encryption scheme,” *Indonesian Journal of Electrical Engineering and Informatics (IJEEI),* vol. 6, no. 3, pp. 301-308, Sep. 2018, doi: 10.52549/ijeei.v6i3.490.

[14] E. M. de L. Reyes, A. M. Sison, and R. P. Medina, “File encryption based on reduced-round AES with revised round keys and key schedule,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 16, no. 2, pp. 897-905, 2019, doi: 10.11591/ijeecs.v16.i2.pp897-905.

[15] S. Fahd, M. Afzal, H. Abbas, W. Iqbal, and S. Waheed, “Correlation power analysis of modes of encryption in AES and its countermeasures,” *Future Generation Computer Systems,* vol. 83, pp. 496-509, 2018, doi: 10.1016/j.future.2017.06.004.

[16] J. Machicao, J. M. Baetens, A. G. Marco, B. De Baets, and O. M. Bruno, “A dynamical systems approach to the discrimination of the modes of operation of cryptographic systems,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 29, no. 1–3, pp. 102–115, 2015, doi: 10.1016/j.cnsns.2015.01.022.

[17] K. S. Dhanalakshmi and R. A. Padmavathi, “A survey on VLSI implementation of AES algorithm with dynamic S-Box,” *Journal of Applied Security Research,* vol. 17, no. 2, pp. 241-256, Apr. 2022, doi: 10.1080/19361610.2020.1870403.

[18] A. Ikhwan, R. A. A. Raof, P. Ehkan, Y. Yacob, and M. Syaifuddin, “Data security implementation using data encryption standard method for student values at the faculty of medicine, University of North Sumatra,” *In Journal of Physics: Conference Series*, vol. 1755, no. 1, p. 012022, 2021, doi: 10.1088/1742-6596/1755/1/012022.

[19] S. M. Hassan and G. G. Hamza, “Real-time FPGA implementation of concatenated AES and IDEA cryptography system,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS),* vol. 22, no. 1, pp. 71-82, 2021, doi: 10.11591/ijeecs.v22.i1.pp71-82.

[20] A. Ali, A. Alabaichi, and A. S. Abbas, “Dual method cryptography image by two force secure and steganography secret message in IoT,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 6, pp. 2928-2938, 2020, doi: 10.12928/telkomnika.v18i6.15847.

[21] A. M. N. G. Molk, M. R. Aref, and R. R. Khorshiddoust, “Analysis of design goals of cryptography algorithms based on different components,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS),* vol. 23, no. 1, pp. 540-548, 2021, doi: 10.11591/ijeecs.v23.i1.pp540-548.

[22] M. Khalifa, F. Algarni, M. Ayoub, and A. Ullah, “A lightweight cryptography (LWC) framework to secure memory heap in internet of things,” *Alexandria Engineering Journal*, vol. 60, no. 1, pp. 1489-1497, 2021, doi: 10.1016/j.aej.2020.11.003.

[23] S. S. Gonge and A. Ghatol, “Aggregation of discrete cosine transform digital image watermarking with advanced encryption standard technique,” *Procedia Computer Science*, vol. 89, pp. 732-742, 2016, doi: 10.1016/j.procs.2016.06.046.

[24] K. Kumar, K. R. Ramkumar, and A. Kaur, “A lightweight AES algorithm implementation for encrypting voice messages using field programmable gate arrays,” *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 6, pp. 3878-3885, 2022, doi: 10.1016/j.jksuci.2020.08.005.

[25] E. M. D. L. Reyes, A. M. Sison, R. P. Medina, and A. Info, “File encryption based on reduced-round AES with revised round keys and key schedule,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS),* vol. 16, no. 2, pp. 897-905, 2020, doi: 10.11591/ijeecs.v16.i2.pp897-905.

[26] C. H. Baek, J. H. Cheon, and H. Hong, “White-box AES implementation revisited,” *Journal of Communications and Networks,* vol. 18, no. 3, pp. 273-287, Jun. 2016, doi: 10.1109/JCN.2016.000043.

[27] K. Shahbazi, M. Eshghi, and R. F. Mirzaee, “Design and implementation of an ASIP-based cryptography processor for AES, IDEA, and MD5,” *International Journal Engineering Science and Technology,* vol. 20, no. 4, pp. 1308-1317, 2017, doi: 10.1016/j.jestch.2017.07.002.

[28] F. Ikorasaki and M. B. Akbar, “Detecting corn plant disease with expert system using bayes theorem method,” *In 2018 6th International Conference on Cyber and IT Service Management (CITSM),* 2019, doi: 10.1109/CITSM.2018.8674303.

[29] H. Cheng, C. Rong, M. Qian, and W. Wang, “Accountable privacy-preserving mechanism for cloud computing based on identity-based encryption,” *IEEE Access,* vol. 6, 2018, doi: 10.1109/ACCESS.2018.2851599.

[30] H. S. I. Harba, T. Abbs, and E. S. I. Harba, "Randomly encryption-decryption using genetic algorithm and ASCII code," *Al-Kut Collage Journal*, vol. 2, no. 4, pp. 1-10, 2017.

[31] D. Nofriansyah, A. Syaref, W. R Maya, G. Ganefri, and R. Ridwan, "Efficiency of 128-bit encryption and decryption process on elgamal method using elliptic curve cryptography (ECC)," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 16, no. 1, pp. 352-360, 2018, doi: 10.12928/telkomnika.v16i1.6953.

BIOGRAPHIES OF AUTHORS

Ali Ikhwan earned his first degree in information systems from STMIK Triguna Dharma, Medan, Indonesia, with a very satisfactory predicate, majoring in Information Systems and graduated in 2013. He received his master's degree in computers in 2015 from Putra Indonesia University YPTK, Padang, Indonesia. He currently taking a doctoral program at University Malaysia Perlis (UniMAP), Perlis, with research in data mining and cryptography. He currently works as a young lecturer at the Faculty of Science and Technology North Sumatra State Islamic University. His research interests include data analysis, data mining, cryptography. He can be contacted at email: ali_ikhwan@uinsu.ac.id.

Dr. Rafikha Aliana A. Raof obtained her first degree in electronics engineering from Multimedia University (MMU), Cyberjaya, Malaysia, with honors, majoring in computer engineering and graduating in 2002. She received the masters of science in intelligent knowledge-based system (IKBS) in 2003 from University Utara Malaysia (UUM), Sintok, Malaysia. Her Ph.D. was obtained in 2014 from University Malaysia Perlis (UniMAP), Perlis, with research in microbiological image diagnosis and artificial intelligence. He is currently working as a senior lecturer at Faculty of Electronic Engineering Technology (FTKEN), University Malaysia Perlis. Her research interests include medical diagnosis system, intelligent system, fuzzy logic and embedded system. She can be contacted at email: rafikha@unimap.edu.my.

Dr. Phaklen Ehkan received a bachelor of electrical engineering (electronic) (UTM), M.Sc. in information technology (UUM) and Ph.D. in computer engineering (UniMAP-University of Birmingham, UK). He worked as an Engineer/Sr. Engineer in Multinational Companies-Electronic Industries for six years before joined the University Malaysia Perlis (UniMAP) as a lecturer in January 2003. His research interests include reconfigurable computing and FPGA, digital design and embedded system, digital and image processing, system on chip (SoC), smart system and IoT. He has published over 110 articles in International Journals and Proceedings Scopus indexed. Currently, he is a head of high-performance computing group under CoE Advanced Computing, UniMAP. He is currently a chartered engineer (UK), professional technologist (MBOT), graduate member of BEM, member of IEEE, BCS and IACSIT. He can be contacted at email: phaklen@unimap.edu.my.

Yasmin Mohd Yacob is a senior lecturer at Faculty of Electronic Engineering Technology, University Malaysia Perlis and research fellow at advanced computing, Centre of Excellence at the same institution. She received her Ph.D. in Computational Intelligence from University Sains Malaysia. Back then, she received her B.Sc. and M.Sc. in computer science from University of Michigan, USA and University Putra Malaysia respectively. Her research interest is in machine learning, data mining and data analytics especially related to medical imaging and agriculture. She can be contacted at email: yasmin@unimap.edu.my.

Nuri Aslami had a bachelor's degree, for three and a half years at IAIN North Sumatra which has now changed to UIN North Sumatera, majoring in Islamic Economics, Faculty of Economics and Islamic Business (FEBI). It did not stop there, the author continued his education to master (S2) level at the University of North Sumatra in 2015 by majoring in management science, Faculty of Economics and Business. Currently the author is continuing his doctoral studies at the State Islamic University of North Sumatra. She can be contacted at email: Nuriaslami@uinsu.ac.id.