Journal of Applied Intelligent System (e-ISSN : 2502-9401 | p-ISSN : 2503-0493)
Vol. 6 No. 2, 2021, pp. 54 – 61

A File Encoding Using A Combination of Advanced Encryption Standard, Cipher Block Chaining and Stream Cipher In Telkom Region 4 Semarang

Lekso Budi Handono*[1], **Andi Danang Krismawan**[2]
Universitas Dian Nuswantoro, Jl. Imam Bonjol 207 Semarang, 50131
Email: [1]handoko@dsn.dinus.ac.id, [2]andidanang@dsn.dinus.ac.id
**Corresponding author*

Abstract - The increase in significant advances in information technology greatly provides comfort and convenience in managing data. This convenience is what makes people who are not responsible for using it as a crime such as hacking, cracking, phishing, and so on. In Telkom Region 4 Semarang, there is a container where there are important company data such as customer data. Customer data is very important and the contents of the data must be kept confidential. The company has experienced significant losses due to information leakage due to negligence in the last 5 years. For this reason, data security is necessary so that data is safe and is not misused. This study applies the Advance Encryption Standard algorithm - Cipher Block Chaining (AES-CBC) and Stream cipher in order to secure data so as to reduce the risk of data theft by telecom subscribers. Based on the average avalanche effect value of AES-CBC and a stream cipher of 49.34%, this shows that the AES-CBC and Stream Cipher encrypted files are difficult to crack so that data confidentiality is well maintained.

Keywords - Security, cryptography, AES-CBC, Stream Cipher, Avalanche Effect

1. INTRODUCTION

The increase in significant advances in information technology greatly provides comfort and convenience in managing data. Along with this convenience, negative impacts also occur, such as threats to the security of confidential personal data. This convenience is what makes people who are not responsible for using it as a crime such as hacking, cracking, phishing and so on. Of course this will harm certain parties such as state secrecy or the confidentiality of important company data. In August 2013 ago, one of the biggest websites, Yahoo, was hacked by hackers, approximately 3 billion accounts were stolen. The hacker managed to get user account information such as name, email, telephone number, date of birth, password that was received by MD5, to security questions and answers [1].

The impact of the hack made Verizon's acquisition value of Yahoo drop by approximately USD 1 billion. In Telkom Region 4 Semarang there is a website dashboard where there are important company data such as customer data and so on. Customer data is very important and the contents of the data must be kept confidential. The dashboard of the website can only be accessed by Telkom employees who have obtained access permits only. However, it does not rule out the possibility of data theft, such as a third party who managed to get an account to access the dashboard, if this customer data falls into the hands of an irresponsible third party and is misused for personal gain, of course this is very detrimental to

the Telkom and its customers. For this reason, data security is necessary so that the data is safe and is not misused.

There are many ways to secure data, including changing data using cryptographic techniques [2]. With data cryptography techniques are encoded or encrypted into confidential data so that the data will not mean anything to unauthorized parties who successfully access the data [3]. Confidential data that has been encrypted and received by the recipient can be changed back or described to the original data so that it can be understood. There are several algorithms that can be used to encrypt data, two of which are the Advance Encryption Standard - Cipher Block Chaining (AES-CBC) and Stream ciphers [4]. The AES algorithm is a block cipher algorithm that uses a permutation and substitution system (P-Box and S-Box) instead of the Feistel network like block ciphers in general. AES or often called Rijndael has been established by the National Institute of Standards and Technology (NIST) as a replacement for DES in current cryptographic standards [5]. As with block cipher algorithms in general, the Rijndael algorithm can be run in several modes of operation, namely Electronic Code Block (ECB) [6], Cipher Block Chaining (CBC) [4], Cipher Feedback (CFB) , and Output Feedback (OFB).

According to research [5] the level of security using the Cipher Block Chaining (CBC) operation mode is safer than the AES / AES Electronic Code Block (ECB) operation mode. In CBC, the feedback technique applies to a block of bits where the encryption results from the previous block are feedback for the encryption and decryption of the next block. In other words, each block of ciphertext is used to modify the encryption and decryption process in the next block. CBC mode requires IV (Initialization Vector) to be used as the initial encryption process [4]. Stream Cipher is a type of symmetric key cipher algorithm. Where the key for encryption is the same as the key for decryption. This algorithm encrypts the plaintext into ciphertext by substituting bits per bit. Stream ciphers use the XOR function, where the plaintext is XORED with a key stream generator or keystream generator [7]. The level of security of the stream cipher lies in the key stream generator. The more random the output generated by the key stream generator, the more difficult the cryptanalyst will solve the ciphertext. To prevent attacks on the AES-CBC algorithm, a stream cipher algorithm is added to strengthen the encryption process and be more secure against cryptanalysis.

2. RESEARCH METHOD

2.1. Encryption Decription

Encryption is the process of securing data or encrypting data before the original data is sent to the recipient [8]. The encryption process converts the original data or plaintext into ciphertext, while the decryption process is the process of returning the ciphertext to its original plaintext. It takes a cryptographic cipher or algorithm and a key in the encryption and decryption process [9]. The purpose of encryption is to hide messages or information from unauthorized parties. In general, the encryption anda decryption process can be formulated as shown in (1) and (2).

$E_k (P) = C$ (1)
$D_k (C) = P$ (2)

Where E is Encryption Process, D is Decryption Process,K is Key, P is Original or Plaintext message and C is Ciphertext. To perform the encryption process, input in the form of plaintext and key is needed so that it can produce ciphertext [10]. Meanwhile, the decryption process requires input in the form of ciphertext and keys to be able to produce plaintext.

2.2. Advanced Encryption Standard

AES is the Rijndael algorithm invented by Dr. Vincent Rijmen and Dr. Joan Daemen. AES is a symmetry algorithm and block cipher [11]. Thus this algorithm uses the same key at the time of encryption and description and the input and output are blocks with a certain number of bits. The Rijndael algorithm was established by NIST (National Institute of Standards and Technology) as AES (Advanced Encryption Standard) 2000 in October. Rijndael has a key length of 128 to 256 bits in 32 bit steps [12]. Because AES has a fixed key length of 128, 192, and 256 and full support of the flexible Rijndael algorithm, AES is currently known as AES-128, AES-192, AES-286. Here are the differences between the three versions of AES as shown in Table 1.

Table 1. AES Varian

Key Size	AES-128	AES-192	AES-256
	4 word (16 byte)	6 word (24 byte)	8 word (32 byte)
Plaintext block size	4 word (16 byte)	4 word (16 byte)	4 word (16 byte)
Number of round	10	12	14
Round key size	4 word (16 byte)	4 word (16 byte)	4 word (16 byte)
Expanded key size	44 word (176 byte)	52 word (208 byte)	60 word (240 byte)

Using the key Nk = 4 words or words which each word consists of 32 bits, the total key is 128 bits. Since the total key is 128 bits, there are $2^{128} = 3{,}4 \times 10^{38}$ possible keywords. This process would take up to 5,4x1024 years to complete even with a computer capable of processing one million keys per second. The encryption and decryption process in the AES algorithm consists of 4 types of bytes transformations, namely SubBytes, ShiftRows, Mixcolumns, and AddRoundKey. At the beginning of the encryption process, plaintext will undergo an AddRoundKey byte transformation. After that, the resulting state will undergo transformation of SubBytes, ShiftRows, MixColumns, and AddRoundKey repeatedly for Nr rounds. For the last round it is different from the previous rounds where in the last round, the state does not undergo a MixColumns transformation.

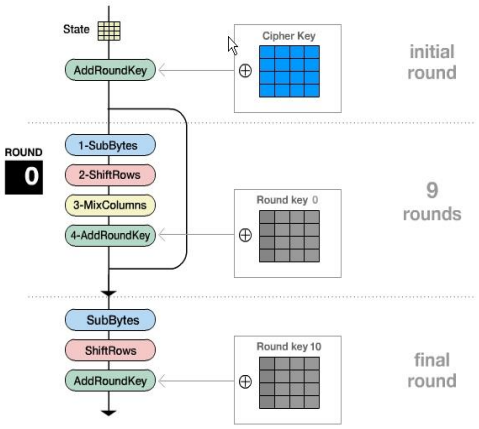

Figure 1. AES Encryption

Meanwhile, the decryption process is the opposite of the encryption because AES is a symmetric key, the key used for the sender and receiver is the same.

2.2. *Cipher Block Chaining (CBC)*

CBC mode uses feedback operations, also known as chaining. The encryption result of the previous block is feedback for encryption and decryption of the next block. In other words,

each ciphertext block is used to modify the encryption and decryption process in the next block. In CBC mode [6], random data is required as the first block for encryption. This random block of data is often called an initialization vector or IV. The IV can be given by the user or generated randomly by the program. To produce the first block cipher, IV is used to replace the previous block ciphertext. In contrast to the decryption, the first plaintext block is obtained by XOR-XORing the results of the decryption of the first ciphertext block [13].

2.3. Stream Cipher

Stream Cipher is a type of symmetric key cipher algorithm, where the key for encryption is the same as the key for decryption [14]. This algorithm encrypts the plaintext into ciphertext by substituting bits per bit [7]. Stream ciphers use the XOR function, where the plaintext is XOR as in (3).

$Ci = Pi \oplus Ki$ (3)
$Pi = Ci \oplus Ki$ (4)

Where C is Ciphertext, P is Plaintext and K is Key. The level of security of the stream cipher lies in the key stream generator. The more random the output generated by the key stream generator, the more difficult the cryptanalyst will solve the ciphertext [15].

2.3. Proposed Method

In this research, the original plaintext or message will be encrypted first using the Advance Encryption Standard algorithm - Cipher Block Chaining (AES-CBC) first to produce temporary ciphertext and then the temporary ciphertext will be re-encrypted using the Stream Cipher algorithm so as to get the final ciphertext result. Meanwhile, in the decryption process, the final ciphertext will be returned again like the original plaintext or message. The decryption process also uses the same algorithm as used in the previous encryption process. In the flowchart as shown in Figure 2, it can be explained how the encryption process is carried out, as follows:

1) For the first step, input a .xlsx file, key for AES-CBC and key for Stream Cipher.
2) After that, it will be XORed between the binary value of the file and the specified IV.
3) Then the XOR result will be XORed once again with the AES-CBC key binary.
4) Then the calculation results will enter the SubBytes process, which is to substitute each byte using the substitution table (SBox).
5) The next process is to do ShiftRows, which experiences a shift on each line, other than the first line. The 2nd row will be shifted to the left 1 time (1 byte), the 3rd row 2 times (2 bytes), and finally the 4th row 3 times (3bytes).
6) Next, the MixColumns process is to multiply each column of the state array by the predefined polynomial a (x). The multiplication process is the same as a matrix multiplication.
7) The result of MixColumns will then undergo the AddRoundKey process, which is to XOR with a round key. The round key is obtained from the calculation of the cipher key entered.
8) The process will be repeated Nr (N round), except for the last round (10th round) which did not undergo the MixColumns transformation
9) The final result of AES-CBC encryption will be re-encrypted using a stream cipher algorithm, namely XORing with a key stream. This final result will be the final ciphertext.

While the flowchart of the encryption and decryption process can be seen in Figure 2, in this figure it will be explained that the decryption process is the reverse direction of the encryption process where the ciphertext file will be encrypted first with a stream cipher then

the results of this encryption will be re-encrypted with AES-CBC to get plaintext end or original file.

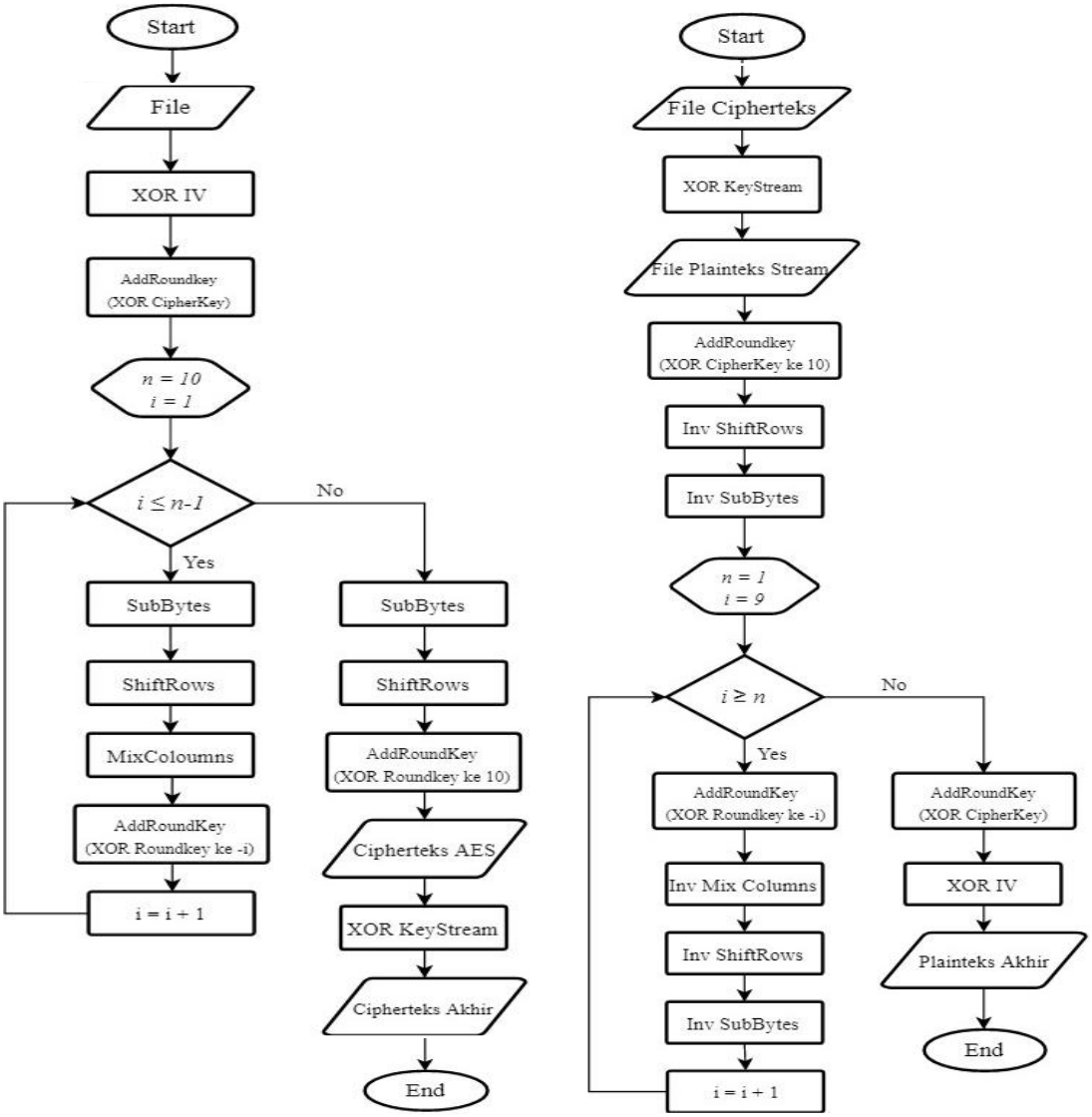

Figure 2. Proposed Method : the left is encryption process and the right is decryption process

3. RESULTS AND DISCUSSION

In this research, using files with the extension *.xls and *.xlsx as encrypted media. The application is made with the Visual Basic programming language. NET. The encryption algorithm used in this application is the AES-CBC algorithm and Stream Cipher. By entering the correct key or the same as the previous encryption process, Figure 17 shows the AES-CBC decryption process was successfully carried out.

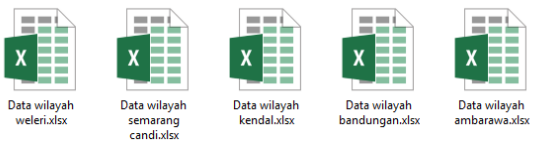

Figure 3. Dataset

Here, we used Black-box testing as tool to evaluate our experiment. Black-box testing is a test that is carried out only from the outside (interface) and without knowing what is actually happening in the detailed process. Black Box Testing is intended to train the entire functional unit of the application so that the application can work properly without experiencing system failure.

Table 2. Results of Black-box Testing

Test Case	Scenario	Expected Result	Information
Input File	The sender / receiver enters files to be encrypted	The application can accept file input	Valid
Input Key	The sender / receiver enters the key for the encryption and decryption process	Keys can be used for encryption and decryption	Valid
Encryption	Encrypt the file with the input key	Applications can encrypt well	Valid
Decryption	Decrypt files with the same key during the encryption process	The application can restore encrypted files to original files	Valid

From the Black Box test in Table 2, it can be concluded that the implementation of the Advance Encryption Standard Algorithm - Cipher Block Chaining (AES-CBC) and Stream ciphers can run well. In order to evaluate further, in this study we used the Avallache Effect calculation as shown in Table 3. This test is conducted to analyze the performance and security of a cryptographic encryption algorithm. Here, the avalanche effect value is obtained through the value of the number of different bits from the comparison of plaintext and ciphertext, divided by the total number of bits overall in this study taking one hex value block from each sample data as shown in (5). An avalanche effect is said to be good if the resulting bit change is between 45-60% [16][17]. The more bit changes that occur, the more difficult the cryptographic algorithm will be to solve.

$$\text{Avalanche Effects} = \frac{\text{Different bits}}{\text{Total bits}} \text{ x } 100\% \qquad (5)$$

Table 3. Results of Avalanche Effect

Original File	Original File (HEX)	Ecrypted File (HEX)	Avalanche (%)
Data wilayah weleri	5c7c7abf288e8bf450faba3615685f2d	66cfa00f4dd0207ea106ac82859a0994	51,5%
Data wilayah kendal	68b26e6db68288c6bb520c8b81c8c055	f95b7b78fe59432f4eb6234e0f9e8024	50%
Data wilayah semarang candi	89fb1042a1156a37b112cfdc7b32f1cd	ebf47150cb2cf279faed8a4ec0980cd9	50%
Data wilayah ambarawa	45f748fc43e42d4adcb2400835ed82c7	03552830b222fd0586edffdfb92cc23	48.4%
Data wilayah bandungan	122a513ec0c493c6aa635b9e6969ff9e	232f685281dbe58a16ac2a896998b8fb	46,8%

Avalance Effect Average Value = (51.5 + 50 + 50 + 48.4 + 46.8) / 5 = 49.34%. From the test results above, the avalanche effect average value of the AES-CBC algorithm and Stream Cipher is 49.34%. This shows that using the AES-CBC algorithm and Stream Cipher proves to be difficult to solve. Another test by size difference has been done as shown in Table 4. The size difference test is carried out in order to know the size of the size change that occurs after the application performs the encryption and decryption process. From the data from the size change test results above, it can be concluded that the encryption process AES-CBC and

Stream Cipher, the encryption size does not change the bit size or is still the same as the original size. So that the algorithm used is proven to secure data without any change in size.

Table 4. Results of Size Difference

File	Original Size	Ecrypted Size
Data wilayah weleri	167.936 bytes	167.936 bytes
Data wilayah kendal	368.640 bytes	368.640 bytes
Data wilayah semarang candi	917.504 bytes	917.504 bytes
Data wilayah ambarawa	290.816 bytes	290.816 bytes
Data wilayah bandungan	110.592 bytes	110.592 bytes

The last testing, has been done by running time. The process running time stage is carried out in order to know the processing time required by the application to perform the encryption and decryption process as shown in Table 5 and Figure 4.

Table 5. Results of Running Time

File	Size file	Encryption Time	Decryption Time
Data wilayah weleri	167kb	125 ms	140 ms
Data wilayah kendal	368kb	122 ms	162 ms
Data wilayah semarang candi	917kb	278 ms	295 ms
Data wilayah ambarawa	290kb	213 ms	162 ms
Data wilayah bandungan	110kb	144 ms	148 ms

Based on the results of the tests carried out in Table 5, the difference in encryption and decryption time needed to process is not much different from the maximum value of the difference of 51 ms. And the file size affects the length of the encryption and decryption process, the larger the file size the longer the encryption and decryption process takes.

4. CONCLUSION

From the research conducted by researchers covering the design stages to the implementation of the Adnvance Encryption Standard-Cipher Block Chaining and Stream Cipher cryptographic applications, the following conclusions were obtained:

1. From the results of block box testing, the application can run well in encrypting and re-decrypting excel files (.xlsx) using the Visual Basic programming language.
2. From the results of the avalanche effect calculation, the average value of the Adnvance Encryption Standard-Cipher Block Chaining and Stream Cipher algorithm is 49.34%. This shows that using the AES-CBC algorithm and the Stream Cipher file encryption proved difficult to crack so that it can secure files properly.
3. Data after going through the encryption and decryption process does not change and is not damaged (the same as the original file), in other words the Advance Encryption Standard-Cipher Block Chaining and Stream Cipher methods run smoothly and successfully.
4. The encryption process is AES-CBC and Stream Cipher, the encryption file size has not changed or is still the same as the original size. So that the algorithm used is proven to secure data without any change in size.
5. The time required for the encryption and decryption process is not much different and the file size affects the length of time the encryption and decryption process takes.

From the research conducted, suggestions that are useful in the development of this study uses 128-bit AES-CBC, therefore for further research it can be tried with 192-bit or 256-

bit AES-CBC. The key used for the Stream Cipher would be better if it could be longer. Future research is expected to have a variety of different combinations to choose from.

REFERENCES

[1] D. P. Joseph and M. Krishna, "Cognitive Analytics and Comparison of Symmetric and Asymmetric Cryptography Algorithms," *Int. J. Adv. Res. Comput. Sci.*, vol. 6, no. 3, pp. 51–56, 2015.

[2] G. Ardiansyah, C. A. Sari, D. Setiadi, and E. H. Rachmawanto, "Hybrid Method using 3-DES , DWT and LSB for Secure Image Steganography Algorithm," in *International Conference on Information Technology, Information Systems, and Electrical Engineering*, 2017, pp. 248–253.

[3] A. I. Ali, "Comparison and Evaluation of Digital Signature Schemes Employed in NDN Network," *Int. J. Embed. Syst. Appl.*, vol. 5, no. 2, pp. 15–29, Jun. 2015.

[4] M. A. Alomari, K. Samsudin, and A. R. Ramli, "A study on encryption algorithms and modes for disk encryption," *2009 Int. Conf. Signal Process. Syst. ICSPS 2009*, pp. 793–797, 2009.

[5] Sangeeta and E. A. Kaur, "A Review on Symmetric Key Cryptography Algorithms," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 4, pp. 358–362, 2017.

[6] K. R. Ilaga and C. A. Sari, "Analysis of Secure Image Crypto-Stegano Based on Electronic Code Book and Least Significant Bit," *J. Appl. Intell. Syst.*, vol. 3, no. 1, pp. 28–38, 2018.

[7] A. Kulsoom, D. Xiao, Aqeel-ur-Rehman, and S. A. Abbas, "An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules," *Multimed. Tools Appl.*, vol. 75, no. 1, pp. 1–23, 2016.

[8] W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, "A Good Performance OTP Encryption Image based on DCT-DWT Steganography," *TELKOMNIKA*, vol. 15, no. 4, pp. 1987–1995, 2017.

[9] H. Rahmalan, M. A. Faizal, Z. Kosnin, C. A. Sari, and E. H. Rachmawanto, "Analysis of Optimization Medical Image Watermarking Using Particle Swarm Optimization Based on SLT," in *4th International Conference of Soft Computing and Pattern Recognition*, 2012, vol. 17, pp. 19–24.

[10] M. Ubaidullah and Q. Makki, "A Review on Symmetric Key Encryption Techniques in Cryptography," *Int. J. Comput. Appl.*, vol. 147, no. 10, pp. 43–48, 2016.

[11] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Comput. Sci.*, vol. 78, no. December 2015, pp. 617–624, 2016.

[12] F. Anwar, E. H. Rachmawanto, C. A. Sari, and de Rosal Ignatius Moses Setiadi, "StegoCrypt Scheme using LSB-AES Base64," in *2019 International Conference on Information and Communications Technology, ICOIACT 2019*, 2019.

[13] Y. A. Alsultanny, "Image encryption by Cipher feedback mode," *Int. J. Innov. Comput. Inf. Control*, vol. 3, no. 3, pp. 589–596, 2007.

[14] S. Garg, S. Khera, and A. Aggarwal, "Extended Vigenere Cipher with Stream Cipher," *Int. J. Eng. Sci. Comput.*, vol. 6, no. 5, pp. 5176–5180, 2016.

[15] R. Naoum, A. Shihab, and S. Alhamouz, "Enhanced Image Steganography System based on Discrete Wavelet Transformation and Resilient Back-Propagation," *Int. J. Comput. Sci. Netw. Secur.*, vol. 16, no. 1, pp. 114–122, 2016.

[16] A. Kumar and N. Tiwari, "Effective Implementation and Avalanche Effect of AES," *Int. J. Secur. Priv. Trust Manag.*, vol. 1, no. 3, pp. 31–35, 2012.

[17] P. Witoolkollachit, "The avalanche effect of various hash functions between encrypted raw images versus non-encrypted images : A comparison study," *J. Thai Med. Informatics Assoc.*, vol. 1, pp. 69–82, 2016.