**Advance Sustainable Science, Engineering and Technology (ASSET)**
**Vol. 5, No.3, October 2023, pp. 0230305-01 ~ 0230305-08**
**ISSN: 2715-4211 DOI:** https://doi.org/10.26877/asset.v5i3.17150

# A Combination of Vigenere Cipher and Advanced Encryption Standard for Image Security

**Ivan Stepheng[1*], Christy Atika Sari[1], Eko Hari Rachmawanto[1], Folasade Olubusola Isinkaye[2]**

[1]Faculty of Computer Science, University of Dian Nuswatoro, Imam Bonjol 207 Semarang, 50131, Central Java, Indonesia

[2]Faculty of Computer Science, Ekiti State University, Ado Ekiti, Ekiti State, 360101, Nigeria.

ivanstepheng2003@gmail.com

**Abstract**. In an era where digital information security is paramount, this research addresses the pressing need for robust encryption methods. We propose a novel approach that combines the Vigenere Cipher and the Advanced Encryption Standard (AES) for secure digital image transmission. Our study recognizes the research gap in secure image transmission methods and aims to bridge it with a powerful encryption solution. We implement this hybrid encryption approach using the Vigenere Cipher in C++ and the AES algorithm in MATLAB. Our experiments validate the effectiveness of our program in concealing and restoring digital images during transmission. This hybrid encryption technique has promising applications in healthcare, military, and confidential business operations, bolstering image security in real-life scenarios. By enhancing image security, our research can contributed to safeguarding sensitive information in the digital age.

**Keywords**: *Vigenere Cipher, Advanced Encryption Standard, Encryption, Decryption*

***(Received 2023-10-06, Accepted 2023-10-13, Available Online by 2023-10-24)***

## 1. Introduction

Along with the development of today's technology, it is now commonplace for people in the digital era to send messages/data. With the activity of sending messages/data between people via the internet, it is necessary to have a level of data security so that the data sent is not opened by unauthorized parties and privacy is maintained [1]. Computer technology made it easier for society to communicate. However, with the development of this technology, it is also necessary to pay attention to the level of security of the information. The internet is one of the infrastructures to facilitate communication so it is widely used by the public. Therefore, there is a high possibility of wiretapping and data manipulation, therefore the security of data/information sent and received is very important [2]. Data cannot be separated from issues of data confidentiality and security. Big data analysis can be carried out with third parties so that

it can be processed in a manner that avoids problems properly to protect sensitive data and ensure its security, because they of course entrust experts or other tools to analyze data, which can increase the potential for security hazards. Security and privacy are sensitive issues that are often compromised by technological advances. Personal data requires protection. For example, the banking and telecommunications sectors receive personal data directly from customers, which can be misused by other parties [3]. One of the randomization techniques with a key so that the information is unknown is usually called a cryptographic technique. In cryptography, it is further classified into symmetric and asymmetric cryptography. Symmetric methods such as AES are relatively fast in carrying out the encryption and decryption process. [5] Advance Encryption Standard (AES) is a cryptographic technique that has the ability to encrypt and decrypt keys with lengths of 128 bits, 192 bits, and also 256 bits. The use of this key will later affect the round calculations carried out in the Advance Encryption Standard (AES) algorithm [6].

Based on the problems in this research, we will try to combine the Advance Encryption Standard (AES) algorithm and the Vigenere Cipher algorithm. It is hoped that using a combination of these two algorithms can increase the security of the encrypted data. The purpose of using the Vigenere Cipher algorithm is to encrypt the key used in AES. The Vigenere Cipher algorithm is an encryption technique in cryptography that is often used to encrypt data in the form of text. Encoding this algorithm requires a key. One of the advantages of using the Vigenere Cipher algorithm is that this algorithm is one of the algorithms that is not easily vulnerable to password cracking methods [7].

Implementation of the AES-128 algorithm for file security at Imelda Medan Public Hospital, the implementation is carried out using a website with a login page before carrying out the encryption and decryption process, the advantage of the implementation is that it improves radiological test results at the RSU, but the disadvantage is that it can only process files with .jpg and .png format extensions, outside these formats it will automatically be rejected by the system [8]. The AES-128 algorithm for Document Encryption at Gunung Geulis Elok Abadi company, the implementation is carried out using a website with a login page before carrying out the encryption and decryption process. The implementation of the AES algorithm is aimed at text document files, the implementation of this algorithm is only carried out using one algorithm, namely the AES Algorithm. The author's statement says that using just 1 algorithm is considered less secure in the file encryption and decryption process, so the author suggests using 2 algorithms to make it safer [9]. Application of the AES-128 Algorithm in Securing Population Data at the Pematangsiantar City office of demographic affairs, implemented by Java programming language to carry out encryption and decryption on files with the extension .doc, .xls, .ppt, .pdf, .jpg, and .png whose encryption results in the form of text for all file types, both images and text. The decryption process will display the same results as before encryption if the same key is used [10]. Implementation of the AES Algorithm for Securing Login and Customer Data in Web-Based E-Commerce, this implementation uses a website to encrypt the text, namely the password used by users when logging in to the website they own. So the use of the AES – 128 algorithm aims to encrypt data in the form of text which will later be stored in the existing database. By implementing the AES algorithm on an e-commerce website, the author states that it can provide security when logging in and guarantee the security of customer data [11]. Implementation of the AES Algorithm on the QR CODE for Ticket Verification Security, the implementation of the AES algorithm on the QR Code uses a smartphone device, so that the encryption and decryption process is carried out when the user orders a ticket so that the identity of the user/ticket order cannot be accessed by anyone. To check the tickets ordered, the counter staff only scans the existing barcode and then automatically checks the database using an API which is used in real time using the internet. This implementation aims to ensure that the system can secure ticket identities from ticket resale and manipulation of ticket data from unauthorized parties [12].

In this research, the author aims to address the challenge of securing digital image data during transmission. Specifically, it proposes a solution that combines the Vigenere Cipher and the Advanced Encryption Standard (AES) to enhance the security of digital image communication. The study intends to demonstrate that this hybrid encryption approach effectively conceals and restores digital images,

ensuring their confidentiality and integrity during transmission. To achieve this, the research will employ the Vigenere Cipher implemented in C++ for one layer of encryption and the AES algorithm implemented in MATLAB for another layer. The combination of these two encryption methods aims to provide a robust and layered approach to image security, mitigating potential threats in digital image communication.

## 2. Methods

For this research, the author used Code::blocks V20.03 software for the Vigenere Cipher algorithm with C++ and the MATLAB R2021A application to run the AES algorithm. For hardware, the author uses an AMD Ryzen 5 5600G processor, 16GB 3200 Mhz Dual Channel RAM and 1TB SSD. Algorithms are the steps to do a job, in choosing the algorithm used it must be correct. In selecting an algorithm there are considerations that must be assessed, including: how good the results provided by the algorithm are, the efficiency provided by the algorithm both in terms of time and memory [13]. Cryptography is the science of maintaining the security of messages sent so that they can be safely received by the recipient of the message. This word encoding technique is carried out by hiding the original data so that the information is not known by unauthorized / unrelated parties [14]. According to Bruce Schneider, cryptography is the art or science of maintaining the confidentiality of data so that it is not known by unauthorized parties. Experts in cryptography are cryptographers, and cryptanalysis is the opposite of the cryptographic process [15]. Meanwhile, according to Sadikin, cryptography is not a science that studies message hiding techniques alone, but cryptography also includes data security techniques such as data integrity, confidentiality, authentication, and so on [16]. According to Sentot Kromodimoeljo, cryptography is a science that discusses encryption techniques using keys so that the data is difficult to read by people who do not have the key to the data [17].

The Vigenere cipher algorithm is a cryptographic algorithm which is a development of the polyalphabetic substitution cipher [18]. This algorithm can be done in 2 ways [19], namely using the manual method using the Tabula Recta table in Figure 1 or using a formula (1) and (2).

| KEYWORD LETTERS \ PLAINTEXT LETTERS | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

Figure 1. Vigenere Tabula Recta

$$Ci = (Pi + Ki)\ mod\ 26 \qquad (1)$$

$$Pi = (Ci - Ki)\ mod\ 26 \qquad (2)$$

Where, *Ci* is decimal value of the i-th ciphertext character, *Pi* is decimal value of the $i^{th}$ plaintext character and *Ki* is decimal value of $i^{th}$ the key character. The Rijndael Algorithm / AES Algorithm is a safe cryptographic algorithm to protect confidential data / information. In the AES algorithm there are several key lengths consisting of 128 bits, 192 bits and 256 bits. The difference in key lengths affects the rounds carried out by the AES algorithm in carrying out the encryption process. The longer the key,

the more rounds it takes [20], as shown in Figure 2. There are three different types of rounds in the AES algorithm as shown in Table 1. Based on Table 1, this research uses a 128 bit key with 10 rounds of encryption. The key used is a random letter, this is an example of the key used in this research key = "Halokamudisana" with a calculation of 8 bits per letter so that there are 16 characters which, if multiplied by 8 bits, = 128 bits.

Table 1. AES Key Type [20]

| Type | Key Length | Block Length | Rounds Number |
|---|---|---|---|
| AES – 128 | 128 bit | 128 bit | 10 |
| AES – 192 | 192 bit | 128 bit | 12 |
| AES – 256 | 256 bit | 128 bit | 14 |

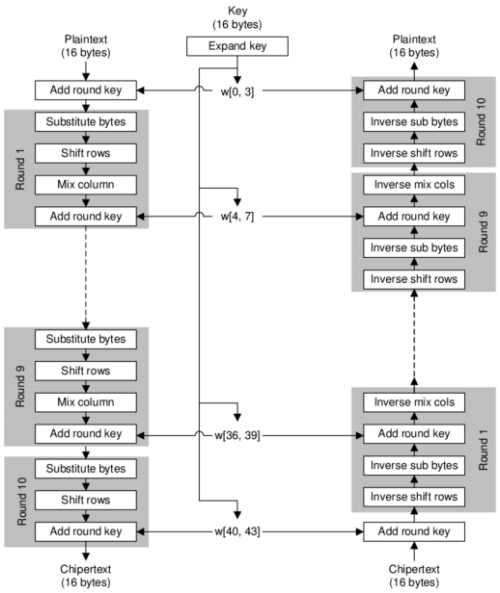



Figure 2. AES General Process

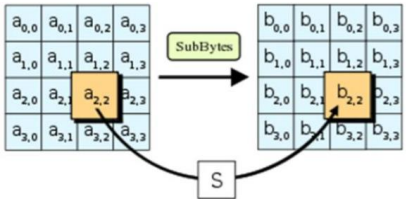
Generaly [21], AES algorithm has 4 main processes for encryption and decryption as in the Figure 3, include:

1) AddRoundKey, to combine state array and round key for illustration.
2) Sub – Bytes, it is a process to exchange the contents of Bytes in each state with an existing substitution table (S-Box),
3) ShiftRows, this is the process of shifting the leftmost bit to the right on each row in the state array, for illustration.
4) MixColumn as in figure 6, it is a multiplication process between a block cipher and a predetermined matrix, to randomize each state array using (3).

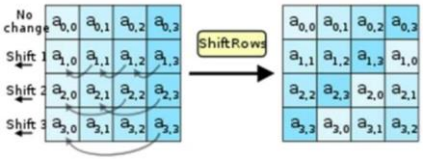
Meanwhile, for decryption process include :

1) AddRoundKey, to combine state array and round key for illustration.
2) InvShiftRows, this is the opposite process to ShiftRows in the encryption process, in this process the bits of each row are shifted from right to left.
3) InvSubBytes, this is the opposite process to SubBytes, in this process the elements in the state are mapped to the existing inverse S-Box table, for inverse S-BOX.
4) InvMixColumn, this is the process of multiplying the state column with the AES matrix.

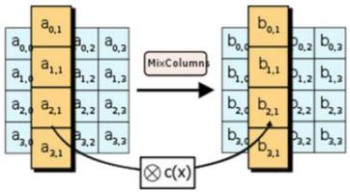
$$A(x) = \{03\}x^2 + \{01\}x^2 + \{01\}x + \{02\} \qquad (3)$$



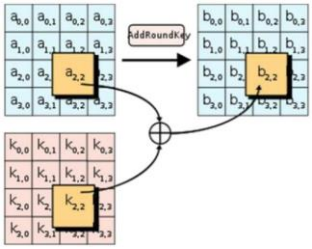

(a) Sub byte




(b) Shift Row




(c) Mix Column




(d) Add Round Key

Figure 3. AES Common Stages

## 3. Results and Discussion

Here, program testing is carried out in several stages, including:

1) Use a normal / unencrypted key, namely= Halokamudisanasa as the main key;
2) Carry out the encryption and decryption process using the AES algorithm, to get the test results;
3) Encrypt the key = Halokamudisanasa using the Vigenere Cipher algorithm;
4) Use a key that has been encrypted using the Vigenere Cipher algorithm, namely = Pplbspmhlxsnvpsn as the main key;
5) Carry out the encryption and decryption process using the AES algorithm, to get the test results;
6) Test and compare the results between keys that have been encrypted using the Vigenere Cipher algorithm and keys that have not been encrypted using any algorithm.

In this test, 10 image samples were used, consisting of 5 color images and 5 grayscale images with .jpeg and .jpg file formats. using key = "Halokamudisanasa" which will be detailed in Table 2.

Table 2. Data Collection for Encryption

| Number | Height (px) | Width (px) | Size (kb) | Type |
|---|---|---|---|---|
| **1** | 210 | 240 | 6 | Grayscale |
| **2** | 285 | 177 | 9 | Colored |
| **3** | 667 | 1000 | 118 | Colored |
| **4** | 167 | 301 | 4 | Colored |
| **5** | 350 | 300 | 21 | Colored |
| **6** | 540 | 360 | 25 | Colored |
| **7** | 408 | 612 | 16 | Grayscale |
| **8** | 375 | 500 | 20 | Grayscale |
| **9** | 395 | 600 | 38 | Grayscale |
| **10** | 300 | 332 | 14 | Grayscale |

The encryption results will produce a file called encrypt and the decryption results will produce a file called decrypt. Where in this experiment the encryption and decryption process will be carried out directly in the existing program, table 3 will display the results of the tests carried out. In this second test, 10 image samples has been used, consisting of 5 color images and 5 grayscale images with .jpeg and .jpg file formats. using key = "Pplbspmhlxsnvpsn" which detailed in Table 2, Key calculations has been done using manual calculations or using programs such as those in Figure 4 and Figure 5.

Table 1. AES Encryption Test Results

| No. | Size Original (kb) | Size Decrypted (kb) | Time (sec) | Bit Error Rate (BER) | UACI | NPCR | Entropy Original | Entropy Decrypt |
|---|---|---|---|---|---|---|---|---|
| **1** | 6 | 43 | 10.54 | 0 | 33.00% | 100.00% | 7.6445 | 7.6445 |
| **2** | 9 | 89 | 6.73 | 0.000010738 | 33.19% | 99.28% | 7.7374 | 7.7372 |
| **3** | 118 | 929 | 764.35 | 0.00000049975 | 33.01% | 98.06% | 7.8269 | 7.8269 |
| **4** | 4 | 85 | 4.94 | 0.000009118 | 32.44% | 99.30% | 7.5878 | 7.5879 |
| **5** | 21 | 100 | 26.72 | 0.0000031746 | 38.98% | 97.94% | 7.2345 | 7.2345 |
| **6** | 25 | 103 | 69.07 | 0 | 34.18% | 99.56% | 6.8013 | 6.8013 |
| **7** | 16 | 83 | 113.90 | 0 | 48.26% | 99.01% | 6.1985 | 6.198 |
| **8** | 20 | 154 | 65.02 | 0.0000026667 | 44.27% | 98.95% | 7.6389 | 7.6390 |
| **9** | 38 | 205 | 101.15 | 0.0000014065 | 36.88% | 99.36% | 7.6396 | 7.6397 |
| **10** | 14 | 84 | 20.60 | 0 | 38.67% | 98.44% | 7.4534 | 7.4534 |

```
Masukkan teks yang akan dienkripsi: Halokamudisanasa
Masukkan kunci enkripsi: ipan
Teks terenkripsi: Pplbspmhlxsnvpsn

Process returned 0 (0x0)   execution time : 7.145 s
Press any key to continue.
```

Figure 4. Key Encryption using Program

The encryption results will produce a file called encrypt and the decryption results will produce a file called decrypt. Where in this second experiment the encryption and decryption process will be carried out directly in the existing program, table 4 will display the results of the tests carried out. The UACI and NPCR graphic display of the experimental results shown in Figure 7.

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Teks = | H | a | l | o | k | a | m | u | d | i | s | a | n | a | s | a |
| Key = | i | p | a | n | i | p | a | n | i | p | a | n | i | p | a | n |
| Urutan Abjad pada Teks = | 7 | 0 | 11 | 14 | 10 | 0 | 12 | 20 | 3 | 8 | 18 | 0 | 13 | 0 | 18 | 0 |
| Urutan Abjad pada key = | 8 | 15 | 0 | 13 | 8 | 15 | 0 | 13 | 8 | 15 | 0 | 13 | 8 | 15 | 0 | 13 |
| Total Teks + Key = | 15 | 15 | 11 | 27 | 18 | 15 | 12 | 33 | 11 | 23 | 18 | 13 | 21 | 15 | 18 | 13 |
| Mod 26 | 15 | 15 | 11 | 1 | 18 | 15 | 12 | 7 | 11 | 23 | 18 | 13 | 21 | 15 | 18 | 13 |
| Konversi Ke Abjad | P | p | l | b | s | p | m | h | l | x | s | n | v | p | s | n |

Figure 6. Key Encryption using manual calculation

Table 2. AES Key Encrypted Encryption

| No. | Size Original (kb) | Size Decrypted (kb) | Time (sec) | Bit Error Rate (BER) | UACI | NPCR | Entropy Original | Entropy Decrypt |
|---|---|---|---|---|---|---|---|---|
| **1** | 6 | 43 | 11.54 | 0 | 33.00% | 100.00% | 7.6445 | 7.6445 |
| **2** | 9 | 89 | 65.73 | 0.000010738 | 33.19% | 99.28% | 7.7374 | 7.7372 |
| **3** | 118 | 929 | 760.35 | 0.00000049975 | 33.01% | 98.06% | 7.8269 | 7.8269 |
| **4** | 4 | 85 | 7.94 | 0.000009118 | 32.44% | 99.30% | 7.5878 | 7.5879 |
| **5** | 21 | 100 | 23.72 | 0.0000031746 | 38.98% | 97.94% | 7.2345 | 7.2345 |
| **6** | 25 | 103 | 67.07 | 0 | 34.18% | 99.56% | 6.8013 | 6.8013 |
| **7** | 16 | 83 | 108.90 | 0 | 48.26% | 99.01% | 6.1985 | 6.198 |
| **8** | 20 | 154 | 61.02 | 0.0000026667 | 44.27% | 98.95% | 7.6389 | 7.6390 |
| **9** | 38 | 205 | 98.15 | 0.0000014065 | 36.88% | 99.36% | 7.6396 | 7.6397 |
| **10** | 14 | 84 | 25.60 | 0 | 38.67% | 98.44% | 7.4534 | 7.4534 |

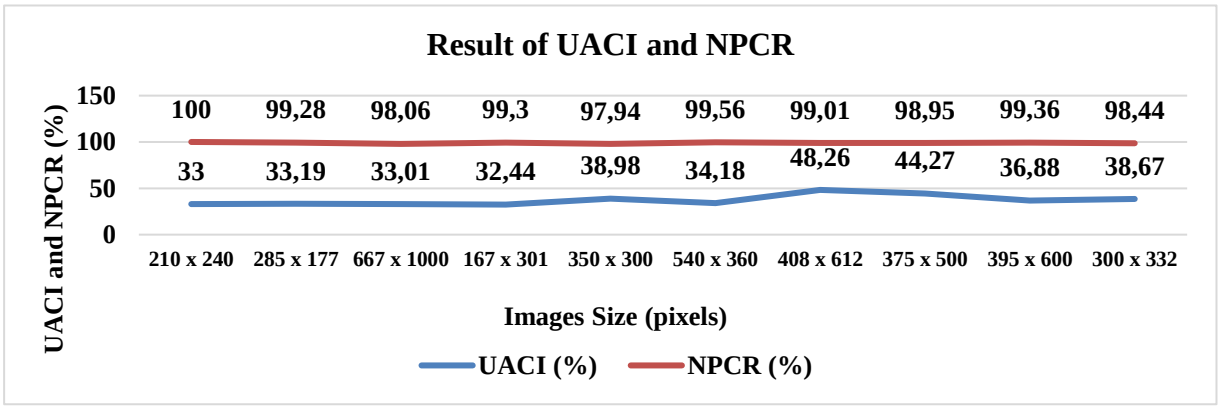



Figure 7. Result of UACI and NPCR

From the experimental results above, it can be concluded that, encrypted and unencrypted keys actually give the same results because they have the same 128 bits and the AES algorithm only runs 10x rounds. AES – 128 algorithm has been used as an alternative for securing data in the form of digital images. The size of the digital image/image affects the time of the encryption and decryption process carried out by the system. In accordance with the research objective, namely to make digital images safe so that they can be used in various institutions and aspects of research results: based on the UACI and NPCR graphs above, it can be seen that the average NPCR value is close to 100%, which means the original image is identical to the decrypted image, the same Likewise, the UACI is getting closer to 50%, indicating an inconspicuous change between the original image and the encrypted image, thus indicating that the resulting encryption has a fairly balanced level of security. The entropy result shown to be close to 10 means that the resulting encrypted image is random enough so it is considered safe in securing data. From the research results, it is proven that the initial image that has undergone the encryption and decryption process will return to the original image and remain unchanged.

## 4. Conclusion

This research still has many shortcomings and limitations, including being quite complex, it cannot be said to be perfect in carrying out encryption, it takes quite a long time if the image size is large. This research can be used to secure digital images so that they are not easily identified by other people as long as the key is not given. For further development, this research will continue to develop encryption and decryption of digital images using a combination of AES and k-order based on Fibonacci due to enhance key security and get the best results of imperceptibility.

## References

[1] N. 'Dian and S. 'Yohanes, "Aplikasi Pengamanan Informasi Menggunakan Metode Least Significant Bit(Lsb) dan Algoritma Kriptografi Advanced Encryption Standard (AES)," *Jurnal Informatika Global*, vol. 09, pp. 84–84, Dec. 2018.

[2] Heru Satria Tambunan, Indra Gunawan, Raja Sari Novica Aswita, Zulaini Masruro Nasution, and Sumarno, "IMPLEMENTASI ALGORITMA AES DAN RC4 TERHADAPKEAMANANDATAPRODUKBENIHSAYURANDIPT.EWINDO," *Journal Sosial dan Sains*, vol. 1, Jun. 2021.

[3] N. Salsabila Nainggolan and P. Nasution, "Pentingnya Keamanan Big Data Dalam Lembaga Pemerintahan Di Era Digital," *Jurnal Jurnal Sains Dan Teknologi (JSIT)*, vol. 3, no. 2, p. 253, 2023, [Online]. Available: http://jurnal.minartis.com/index.php/jsit

[4] F. Prasetyo Nugroho, R. Wariyanto Abdullah, and S. Wulandari, “KEAMANAN BIG DATA DI ERA DIGITAL DI INDONESIA,” 2019.
[5] C. Kirana, E. Sugianto, and P. Studi Teknik Informatika STMIK Atma Luhur Pangkalpinang, “Penerapan Algoritma AES dan Konversi SMS ke dalam Bahasa Khek pada Aplikasi Enkripsi Berbasis Mobile Application,” *Journal Ilmu Komputer dan Informatika*, vol. 5, no. 1, 2019.
[6] M. ’Azhari, F. ’Ali, D. ’Iskandar, and F. ’Joko, “Implementasi Pengamanan Data pada Dokumen MenggunakanAlgoritma Kriptografi AdvancedEncryption Standard(AES),” *Jurnal Pendidikan Sains dan Komputer*, vol. 1, pp. 164–164, Feb. 2022.
[7] V. Saputra Ginting, “PENERAPAN ALGORITMA VIGENERE CIPHER DAN HILL CIPHER MENGGUNAKAN SATUAN MASSA,” *Jurnal Teknologi Informasi*, vol. 4, no. 2, 2020.
[8] D. Hulu, B. Nadeak, and S. Aripin, “Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan,” *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, vol. 4, no. 1, 2020, doi: 10.30865/komik.v4i1.2590.
[9] A. I. Suranta, D. Virgian, and S. Y. Sakti, “Penerapan Algoritma AES (Advance Encryption Standart) 128 untuk Enkripsi Dokumen di PT. Gunung Geulis Elok Abadi,” *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 5, no. 1, pp. 1–10, 2022.
[10] I. Asih, R. Simbolon, I. Gunawan, I. O. Kirana, R. Dewi, and S. Solikhun, “Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar,” *Journal of Computer System and Informatics (JoSYC)*, vol. 1, no. 2, 2020.
[11] L. Mustika, “Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada E-Commerce Berbasis Web,” *JURIKOM (Jurnal Riset Komputer)*, vol. 7, no. 1, p. 148, Feb. 2020, doi: 10.30865/jurikom.v7i1.1943.
[12] A. Pariddudin and F. Syauqi, “Penerapan Algoritma AES pada QR CODE untuk Keamanan Verifikasi Tiket,” *Jurnal Ilmiah Teknologi - Informasi & Sains*, vol. 10, pp. 43–52, 2020, doi: 10.36350/jbs.v10i2.
[13] M. Iqbal Afandi, “Implementasi Algoritma Vigenere Cipher Dan Atbash Cipher Untuk Keamanan Teks Pada Aplikasi Catatan Berbasis Android,” 2020.
[14] S. U. Lubis, “IMPLEMENTASI METODE MD5 UNTUK MENDETEKSI ORISINALITAS FILE AUDIO,” *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, vol. 3, no. 1, Nov. 2019, doi: 10.30865/komik.v3i1.1620.
[15] L. H. Sijabat, N. I. Syahputri, and M. Khairani, “Kriptografi dan Steganografi Penyembunyian Pesan Pada Media Audio Menggunakan Algoritma AES,” *ALGORITMA: Jurnal Ilmu Komputer dan Informatika*, p. 1, 2021.
[16] L. A. Indrayani and I. M. Suartana, “Implementasi Kriptografi dengan Modifikasi Algoritma Advanced Encryption Standard (AES) untuk Pengamanan File Document,” 2019.
[17] R. Laia, “Implementasi Algoritma Aes 256 Bit Dan Lsb Untik Pengamanan Dan Penyisipan Pesan Teks Pada File Audio,” 2020.
[18] R. Imam and F. Abdul, “Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher,” *Journal Informatika Sunan Kalijaga*, vol. 7, pp. 33–45, Jan. 2022.
[19] T. S. Alasi, A. T. Al, and A. Siahaan, “Algoritma Vigenere Cipher Untuk Penyandian Record Informasi Pada Database,” *Jurnal Informasi Komputer Logika*, vol. 1, no. 4, 2020, [Online]. Available: http://ojs.logika.ac.id/index.php/jikl
[20] A. Puji Nugroho, H. Bayu Suseno, and U. Islam Negeri Syarif Hidaytullah Jakarta, “Keamanan Data Transaksi Nasabah Pada Aplikasi Bank Sampah Berbasis Web Menggunakan Algoritma AES,” *Query : Journal Sistem Informasi*, vol. 4, Apr. 2020.
[21] A. Prameshwari and N. P. Sastra, “Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen,” *Eksplora Informatika*, vol. 8, no. 1, p. 52, Sep. 2018, doi: 10.30864/eksplora.v8i1.139.