Implementation of advanced encryption standard for file security in stego-object

S Y Yuliani2,3,*, A R Atmadja1, Y S Nurjanah1, D Fauzy3, R G Utomo4 and D R Nur4

1 Department of Informatics, UIN Sunan Gunung Djati Bandung, Bandung, Indonesia
2 Faculty of Information and Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia
3 Department of Informatics, Universitas Widyatama, Bandung, Indonesia
4 Universitas Widya Gama Mahakam Samarinda, Samarinda, Indonesia

*sy.yuliani@widyatama.ac.id

Abstract. Security issues and data confidentiality are very important in the digital and internet era today. Important files circulating on the internet, both in the form of documents, images, and videos need to be supported with good security. This article aims to secure files by utilizing steganography technology, both in encryption and decryption of the file. The method used was the Advanced Encryption Standard (AES) which was applied to Stego-Object. Experiments were done on document files with extensions .doc, .xlsx, .pdf, and .txt, also on image files with extensions .jpeg, .png, and .bitmap. The experimental results showed that AES can encrypt and decrypt quite effectively without changing the quality of files both images and documents. This research could develop for video files.

1. Introduction

Along with the development of technology, it increasingly changes the way people communicate. Reviewing the rapid development of various multimedia technologies, more and more multimedia data is generated and transmitted, the internet also allows a broad distribution of digital media data. Now, it is much easier to edit, modify and duplicate digital information. However, as technology develops, crime also increases in the system. With various techniques for illegally extracting information, many are trying to access information that is not their right. The existence of technology not only has a positive impact, one of the negative impacts is data tapping, which is one of the most feared problems by users of communication networks. Security and confidentiality of data are one of the important aspects of an information system [1]. Implementing the need for security may be more expensive than the value of the data to be secured. Protecting data from attacks is difficult, so that using cryptographic techniques can solve to protect the data [2]. Cryptography is an art and science to protect unwanted information from individuals by turning it into a form that is not recognized by attackers as long as the data is stored and transmitted. Cryptographic data mainly changes the contents of data, such as text, images, audio, video and so on to be used as unreadable, invisible or incomprehensible data during transmission or storage called encryption [3]. Besides cryptographic techniques, there are also other techniques namely the steganography technique. Steganography is a science of hiding information so that the existence of messages is not detected by the unintended recipients [4]. This technique is often used to avoid people's
suspicion and avoid the desire of people to know the contents of the secret message [5]. The way is by hiding confidential information/data in a container because steganography requires two properties, namely container and confidential data that will be hidden. The main purpose of the cryptographic and steganography method is to maintain the security of the form of data from invalid attackers. With regard to data file security, steganography is only one of many ways that can be done to hide secret messages. Steganography is more suitable to be used in conjunction with other methods, one of which is encryption. Using an encryption method that is applied simultaneously with the steganography technique can make the technology used look simple but the tracking is quite difficult.

Many research has been done in file encryption. First, the research presents the knowledge about the Least Significant Bit (LSB) based image steganography and its applications to various file formats. LSB is a method for embedding data into cover image. The least significant bit of each pixel of an image is altered to a bit of a message that is to be hidden. The paper also analyse the available image based steganography along with cryptography technique to achieve security [6]. Second, the study proposed a system on android platform to encrypt the file. The encrypt process are done before it is transmitted over the network. The research is used for all file type such as text, docx, pdf and image encryption. AES algorithm is used for encryption and decryption [7]. Last, the research focused on designing a web-based information security system to secure image and text using the Advanced Encryption Standard algorithm. The system has implemented encrypt and decrypt to hide text and image information. The conclusion of this study proves that the AES Algorithm method is a very good algorithm in securing text and image files. In this research, Advanced Encryption Standard (AES) have done for encrypt file [8]. The reason for using this algorithm is because the actual level of security is compared to existing algorithms both in terms of calculation of processing time, pixel size, key security, and has a simple design.

2. Methods

2.1. Steganography

Steganography is the science and art of hiding secret messages such that the existence of messages is not detected by the human senses [4,9]. The media used is generally a different medium with confidential information carriers, which is where the function of the steganography technique is as a disguise technique using different media so that confidential information in the initial media is not clearly visible. Steganography is usually often misrepresented with cryptography so both of them aim to protect valuable information. The word steganography comes from Greek, namely from the words Steganos (covered) and Graptos (writing). Steganography in the modern world usually refers to information or an archive that has been hidden into a digital image file, audio, or video. In World War II, the steganography technique was commonly used by German soldiers in sending secret messages from or to Germany.

Steganography also can be used for a variety of reasons, some for good reasons, but also for bad reasons. For the purposes of legitimacy, security can be used such as images with watermarking, for reasons of copyright protection. Digital watermarks (also known as fingerprinting, which are specifically for copyright matters) are very similar to steganography because they use a hidden method in archives, which appears as an original part of the archive and is not easily detected by most people [10]. Steganography can also be used as a way to substitute for a one-way hash value. In addition, steganography can be used as tags for online imagery. Finally, steganography can also be used to maintain the confidentiality of valuable information, to safeguard the data from the possibility of sabotage, theft, or from unauthorized parties.

2.2. AES (Advanced Encryption Algorithm)

The Advanced Encryption Standard is a symmetric cryptographic algorithm that can be used to secure data. This algorithm is a key-symmetric encryption standard. The AES algorithm is obtained through a competition conducted in 1997 by NIST (National Institute of Standard and Technology) to look for
standard encryption algorithms that can be used in various applications. This selection process is very strict and requires a long time. In the end, on October 2, 2000 the Rijndael algorithm was created by Rijmen and Daemen from Belgium as a standard encryption algorithm commonly called AES. Although still new, this algorithm has been used in various applications, one of which is for password encryption. The use of this algorithm has often been seen in software for data compression. In the software, one of the methods used to encrypt passwords is the AES algorithm. The AES algorithm has symmetric ciphertext blocks can encrypt (encipher) and decrypt (decipher) on information. This type of algorithm is divided into 3, namely AES-128, AES-192 and AES-256. Each type of AES algorithm can encrypt and decrypt data in 128 bit blocks. 128-bit block is a fixed size cipher block used in the AES algorithm. Rijndael supports 128-bit to 256-bit keys[7]. The key length and block size can be chosen independently, and each block is encrypted by a certain number of rounds. The number of rounds used by the AES algorithm can be seen in table 1.

| Type     | Key Length | Block Size | Number of Round |
|----------|------------|------------|-----------------|
| AES-128  | 128 bit    | 128 bit    | 10              |
| AES-192  | 192 bit    | 128 bit    | 12              |
| AES-256  | 256 bit    | 128 bit    | 14              |

2.3. System architecture
System architecture is needed for describe the encryption process starting from original file, covering process and output file which become stego-object file. Figure 1 showed the architecture of created system.

Figure 1. System architecture in file encryption.

Inside the system architecture, there were several stages, namely:
- At the first stage, the stego-file (original file) would be inputted. Stego-file was a file that would be hidden. Input cover that would be proceed using AES as the algorithm for processed security file.
- Cover process is used to hiding stego-files. Whereas AES was an algorithm that was used to insert messages and extract it from stego-file.
- File that had been processed would become a stego-object. Stego-object was a message that contained combination of stego-files and cover.
3. Results and discussion
In this study, performance test was carried out in several scenarios. First, the scenario was started with document files. Then, the second performance test continue with encrypting image files include jpeg, png, and bitmap formats. Last, the testing also done in different character length.

3.1. Performance test for document files
Performance test for document files consisting of doc, xlsx, pdf, and txt formats. The following was the test results described in table 2.

| No | Format | Name of File   | Size (kb) | Time (milisecond) |
|----|--------|----------------|-----------|-------------------|
|    |        |                | Plain     | Encrypt | Decrypt | Encrypt | Decrypt |
| 1  | Doc    | data diri.doc  | 12.7      | 12.7    | 12.7    | 16      | 23      |
| 2  | xlsx   | data diri.xlsx | 9.85      | 9.85    | 9.85    | 10      | 20      |
| 3  | Pdf    | data diri.pdf | 3.92      | 3.93    | 3.92    | 4       | 8       |
| 4  | Txt    | data diri.txt  | 0.132     | 0.144   | 0.132   | 288     | 3       |

3.2. Performance test for image files
Performance test for image files consisting of jpeg, png, and bitmap formats. The following was the test results in table 3.

| No | Format | Name of File   | Size (kb) | Time (milisecond) |
|----|--------|----------------|-----------|-------------------|
|    |        |                | Plain     | Encrypt | Decrypt | Encrypt | Decrypt |
| 1  | jpeg   | uin_sample.jpeg| 18        | 18      | 18      | 824     | 69      |
| 2  | png    | uin_sample.png | 25.2      | 25.2    | 25.2    | 323     | 50      |
| 3  | bmp    | uin_sample.bmp | 28.8      | 28.8    | 28.8    | 25      | 28      |

Performance test for keys of different character length. The following was the test result of table 4.

| No | Key Lengths | Format | Name of File | Size (kb) | Time (milisecond) |
|----|-------------|--------|--------------|-----------|-------------------|
|    |             |        |              | Plain     | Encrypt | Decrypt | Encrypt | Decrypt |
| 1  | 3 character | Doc    | 12.7         | 12.7      | 12.7    | 11      | 11      |
|    |             | xlsx   | 9.85         | 9.85      | 9.85    | 8       | 9       |
|    |             | pdf    | 3.92         | 3.93      | 3.92    | 4       | 5       |
|    |             | txt    | 0.132        | 0.144     | 0.132   | 2       | 1       |
|    |             | jpeg   | 18           | 18        | 18      | 784     | 75      |
|    |             | png    | 25.2         | 25.2      | 25.2    | 323     | 50      |
|    |             | bitmap | 28.8         | 28.8      | 28.8    | 25      | 28      |
| 2  | 5 character | doc    | 12.7         | 12.7      | 12.7    | 16      | 23      |
|    |             | xlsx   | 9.85         | 9.85      | 9.85    | 10      | 20      |
|    |             | pdf    | 3.92         | 3.93      | 3.92    | 4       | 8       |
|    |             | txt    | 0.132        | 0.144     | 0.132   | 288     | 3       |
|    |             | jpeg   | 18           | 18        | 18      | 824     | 69      |
|    |             | png    | 25.2         | 25.2      | 25.2    | 323     | 50      |
|    |             | bitmap | 28.8         | 28.8      | 28.8    | 25      | 28      |
### Table 4. Cont.

| 3 | 10 character | doc | 12.7 | 12.7 | 12.7 | 9 | 10 |
|---|-------------|-----|------|------|------|---|---|
|   | xlsx        | 9.85 | 9.85 | 9.85 | 8 | 8 |
|   | pdf         | 3.92 | 3.93 | 3.92 | 4 | 4 |
|   | txt         | 0.132 | 0.144 | 0.132 | 1 | 1 |
|   | jpeg        | 18 | 18 | 18 | 16 | 16 |
|   | png         | 25.2 | 25.2 | 25.2 | 21 | 21 |
|   | bitmap      | 28.8 | 28.8 | 28.8 | 23 | 22 |

Changes in the stego-object file obtained based on the tests that had been done in the encryption and decryption process were illustrated in figure 2 and figure 3.

**Figure 2.** Changes after the encryption process.

**Figure 3.** Changes after the decryption process

### 4. Conclusion

Based on the research results, it can be concluded that Advanced Encryption Standard (AES) algorithm was appropriate to be implemented in securing image files and document files whose confidentiality was very guarded. In addition, the performance of this algorithm works very effectively because it did not change the size of the file during the encryption or decryption process regardless of the length of key characters inputted by the user. Finally, increasing the file size, the greater the execution time of the encryption and decryption process. As it could be seen in the performance test table that got the result of increasing execution time as the file size increases.

The study can be further developed with the addition of data that had a larger size. Furthermore, it was expected that the steganography file application system could also be connected to other systems.

### Acknowledgment

We would like to say thank you for Research and Publication Centre of UIN Sunan Gunung Djati Bandung that give the full support for this publication research.
References

[1] Duan H, Huag W and Zhu G 2019 Research on Data Encryption Technology Inf. Comput. Secur. 1(1) 1–6

[2] Kurniawan S T C, Dedih D and Supriyadi S 2018 Implementasi Kriptografi Algoritma Rivest Shamir Adleman dengan Playfair Cipher pada Pesan Teks Berbasis Android J. Online Inform. 2(2) 102

[3] Goud A and Verma V K 2018 Data Encryption and Decryption Process Using Private Key Cryptography Int. J. Sci. Technol. Manag. Res., 3(6) 39–42

[4] Din R, Bakar R, Utama S, Jasmis J and Elias S J 2019 The evaluation performance of letter-based technique on text steganography system Bull. Electr. Eng. Informatics 8(1) 291–297

[5] Beroual A and Al-Shaikhli I F 2018 A Review of Steganographic Methods and Techniques Int. J. Perceptive Cogn. Comput., 4(1) 1–6

[6] Thangadurai K and Devi G S 2014 An analysis of LSB based image steganography techniques in 2014 International Conference on Computer Communication and Informatics: Ushering in Technologies of Tomorrow, Today, ICCCI 2014

[7] Tayde S and Siledas S 2015 File Encryption, Decryption Using AES Algorithm in Android Phone Int. J. Adv. Res. Comput. Sci. Softw. Eng., 5(5) 550–554

[8] Sihotang H T, Simarmata J, Limbong T, Ginting M B R, Damanik R and Padli M I 2018 Implementation of AES Algorithm for Information Security of Web-Based Application Int. J. Eng. Technol. 7(3.4) 318–320

[9] Rahim R 2018 Combination Base64 Algorithm and EOF Technique for Steganography J. Phys. Conf. Ser., 1007(1) 1–5

[10] Supiyandi S 2018 Application of Invisible Image Watermarking Int. J. Eng. Technol., 7(2) 760–762