Data security improvements on cloud computing using cryptography and steganography

N R D P Astuti*, E Aribowo and E Saputra
Department of Informatics Engineering, Faculty of Industrial Technology, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

*Email: rochmahdyah@tif.uad.ac.id

Abstract. Cloud computing is a service that eases its users to store data on the internet. However, cloud computing has lack, which is related to stored data security specifically to image file that can be manipulated easily. To improve the data securities of JPG file type on cloud computing, the combination of advanced encryption standard (AES) cryptography and least significant bit (LSB) steganography methods is required. This study implemented AES 128 algorithm cryptography process to scramble the messages that will be inserted and LSB steganography to hide the messages that has been scrambled. The data were assessed using Stegspy. The results of this study indicated that cloud computing service of Platform as a Service (PaaS) has resulted ciphertext that was attached to JPG/JPEG images using Least Significant Bit (LSB). From 5 (five) samples, the encryption result testing on JPG/JPEG files was bigger than the original file. The bigger the number of characters of the inserted text, the bigger the size of JPG/JPEG files will be.

1. Introduction
Digital storage media is massively utilized at this time along with the development of technology. One of which is the cloud computing-based storage. Cloud computing provides easy access to store the data on the internet for the users. Various storage capacities are offered by the service providers based on the users’ requests [1]. The users do not need to prepare either software or hardware devices to store the data for the data and information will be stored in a physically unknown server. The data on cloud can be accessed by the client using internet network [2, 3]. By utilizing cloud computing as storage media, the users will be able to reduce the operational costs without providing infrastructure and software devices to use it [1, 5].

However, from the security aspect, cloud method comes up with lack that related to data security, which can be stolen [4]. This is linked to the increase of practiced hackers in the whole world that escalates the risks toward cloud computing data security [3, 4]. Image file is one of the most stored types in cloud. Image file format manipulation can convey negative impacts with the change of the original form that can harm the owners by giving them unpleasant impressions [5].

To secure image format file, cryptography technique is encouragingly suggested to be implemented. The data encoded by cryptographic techniques will convert into incomprehensible data [6]. Nevertheless, by only implementing cryptography technique will trigger suspiciousness to the cryptanalysts. To enhance or lessen the suspiciousness, hence steganography process is put into operation. The advantage of steganography technique covers the ability to hide classified data into digital media; therefore, the data are hardly recognized by other people. The Least Significant Bit (LSB) is one of steganography methods most popular [7]. With the change of bit, it will converse the value in the RGB colors equal to 1 out of the 256 available colors, therefore the conversion is scarcely detected by bare eyes [8].
To improve the security of image format file, two processes of combining cryptography technique using AES algorithm with steganography technique using LSB method [9] were implemented in this study. The image format file tested in this study was JPG file type that stored in cloud computing.

2. Research method

2.1. Cloud computing architecture system
There are four layers covered in cloud computing architecture system. The layers consist of hardware device, infrastructure, platform, and application [3] as illustrated in Figure 1.

To assemble the system, a service based on the Platform as a Service (PaaS) of the cloud computing system was utilized. PaaS is a delivery service that consists of two layers. It provides several services such as assembling, testing, and spreading any under development application [3].

2.2. Flowchart system
Flowchart is used to describe the built system flow. There are two processes that will be executed by the system. The first process takes in the cryptography method using AES algorithm, which includes encryption and decryption processes for the file that will be hidden. The second process takes in the steganography method using LSB that used to hide classified file in image file format.

2.3. Construction
Construction refers to the implementation of the system workflows that have been designed. The system will be implemented on cloud computing. The construction process uses PHP and JavaScript programming.

2.4. Testing
To make sure that all methods run well, hence the testing process applies both functionality and compatibility tests.

3. Experimental result

3.1. Finding and discussion
Cloud computing scheme is a model to give a comfortable request network access from several users to share a configured computing resource (for example a network, server, storage, application, and service) that able to quickly set and release using a minimum management or interaction service provider. The result of developing scheme can be seen in the Figure 2.

The process of cloud computing system that built to support a security process is PaaS with encryption and Decryption process run on cloud computing. With the benefits on PaaS has been provide an operating system, database, and web server. Figure 3 is an illustration of cloud computing system that has been built.
The first process is encrypting using a cryptography hidden picture method. The algorithm that will be used in this process is AES 128 bit. The result of encryption process will be hidden using LSB (Least Significant bit) steganography method. The final result of this process is an image with a hidden message inside.

To open a hidden message, the hidden message is done first using steganography to separate an image file as a place to hide a hidden message. This decryption file will produce two file. After a separation to know the hidden message so second process is decryption using AES 128 Bit Algorithm. It is used to restore a message to its previous form so it can be read by the user.
To know the whole plot system so the flowchart system is built, as well as in Figure 4. The first step is started with input a plaintext and followed by input key that must be 128 bit in length or 16 character, if the step is different it will go back to input key. After the right key process done, there will be an encryption process that produces a ciphertext. This ciphertext then copied for the next process, which is inserted the result of encryption AES 128 Bit into an image using LSB Steganography method. The following step is uploading the image and then filling the plaintext with the result of ciphertext AES 128 Bit, unlimited character on password input and then the LSB encryption is done and resulting an encrypted image.

The first decryption process is uploading a picture, then putting the password if it is already suit with the decryption process that produce a plaintext, the plaintext will be put on the decryption AES 128 process, and then if the input key is appropriate it will continue with decryption AES 128 that produce an original message that has been encrypted before.

The encryption page using algorithm AES 128 bit by putting a plaintext, a key with 16 character. An encrypted Ciphertext will be inserted using LSB method on the JPG formatted Image. The final result is an image that has been inserted a random message.

3.2. Testing
Tests are carried out using a JPG / JPEG image file for inserting a message. Text or message file that will be hidden. The file to be used is a file that will be stored in cloud computing. Files before being saved to the cloud will be processed encryption and hiding messages. Testing by using five samples of different image files of different sizes and messages to be hidden that have been through the encryption process with AES 128 bits. The test results are shown in Table 1. Based on the testing as Table 1, it shows that the change in the file capacity is very significant, this is because the process of inserting images with different characters.

![Figure 4. Encryption and decryption algorithm by AES 128 bit and LSB flowchart](image-url)
The next testing process is done five times using the StegSpy 2.1 application. This StegSpy application is an application that allows identifying hidden files that are used to hide messages. The test results are shown in Table 2.

**Table 1.** The comparison between the size of image file before and after inserting a message

| No. | File Name                          | Dimension size | JPG Capacity Before | JPG Capacity After |
|-----|-----------------------------------|----------------|---------------------|--------------------|
| 1   | 20180709044816.JPG                 | 1200x690px     | 539kb               | 1.47 Mb            |
| 2   | UAD kampus 3.JPG                  | 1024x768px     | 174kb               | 1.16 Mb            |
| 3   | UAD-2.JPG                         | 1303x745px     | 164kb               | 1.14 Mb            |
| 4   | Masjid-UAD.JPG                    | 1080x810px     | 97.5kb              | 1.03 Mb            |
| 5   | Masjid Islamic Center UAD.JPG     | 1600x1067px    | 133kb               | 1.15 Mb            |

The testing process is done four (4) times with different shots, namely from DSLR cameras, cellphone cameras, from the internet, and from Photoshop, this is intended to determine changes to files before and after encryption. Table 2. Described a comparison of the results of stegspy.

**Table 2.** A test using image file taken from different tools

| No | Before Encryption | After Encryption |
|----|-------------------|------------------|
| 1  | Source: Canon EOS 6D  
Dimensions: 5182 x 3456px  
FileSize: 6.75 MB  (7,080,872 bytes)  
Undetected by StegSpy |  
Dimensions: 700 x 466  
FileSize: 726 KB (743,473 bytes) |
| 2  | Source: Internet  
Dimensions: 1024 x 768px  
FileSize: 174 KB (178,485 bytes)  
Detected by StegSpy |  
Dimensions: 700 x 525px  
FileSize: 804 KB (823,315 bytes) |
Source: Smartphone camera
Dimension: 3000 x 4000px
File Size: 3.29 MB (3,456,020 bytes)
Undetected by StegSpy

Source: Photoshop
Dimension: 1920 x 1200px
File size: 189 KB (193,690 bytes)

Source: Kamera HP
Dimension: 700 x 437px
File Size: 459 KB (470,812 bytes)
Undetected by StegSpy
4. Conclusion
The cryptographic application of the AES128 algorithm and LSB method steganography in cloud computing can be used to improve data security in the form of JPG / JPEG image format files. The process of hiding a message successfully done into a JPG / JPEG image using the media canvas as a message insertion process with the LSB method steganography process into the image carried out on the cloud. The Advanced Encryption Standard (AES 128bit) algorithm can be used for message randomization so that messages that will be inserted in the image are in the form of a ciphertext that will be difficult to read.

References
[1] KPMG Advisory N.V 2010 From hype to future: KPMG’s 2010 cloud computing survey in KPMG’s 2010 Cloud Computing Survey p 44.
[2] Webb J, Ahmad A, Maynard S B and Shanks G 2014 A situation awareness model for information security risk management Comput Secur vol 44 pp 1–15.
[3] Zhang Q, Cheng L and Boutaba R 2010 Cloud computing: state-of-the-art and research challenges J Internet Serv Appl vol 1 no 1 pp 7–18.
[4] Zhou L, Varadharajan V and Hitchens M 2013 Achieving secure role-based access control on encrypted data in cloud storage Inf Forensics Secure IEEE Trans vol 8 no 12 pp 1947–60.
[5] Hussain M and Hussain M 2013 A survey of image steganography techniques Int J Adv Sci Technol vol 54 pp 113–24.
[6] Mishra R and Bhanodiya P 2015 A review on steganography and cryptography in Conference Proceeding-2015 International Conference on Advances in Computer Engineering and Applications ICACEA 2015 pp 119–22.
[7] Chia-Chen Lin C C C and Yi-Hui 2009 CLSB-based high-capacity data embedding scheme for digital images Int J Innov Comput Inf Control vol 5 no 11 p 4289.
[8] Qazanfari K and Safabakhsh R 2014 A new steganography method which preserves histogram: Generalization of LSB++ Inf Sci (Ny) vol 277 pp 90–101.
[9] Juneja M 2014 A covert communication model-based on image steganography Int J Inf Secur Priv vol 8 no 1 pp 19–37.