DOUBLE AUDIO STEGANOGRAPHY USING LEAST SIGNIFICANT BIT WITH DES CRYPTOGRAPHY

R.M. Adhika Wira W[1], Jangkung Raharjo[2], Irma Safitri[3]

[1,2,3]Telecommunication Engineering Department, School of Electrical Engineering, Telkom University
[1]dhikawira@student.telkomuniversity.ac.id, [2]Jangkungraharjo@telkomuniversity.ac.id,
[3]irmasafitri@telkomuniversity.ac.id.

Abstract

Steganography is the practice of concealing a file, message, image, or video within another file, message,image, or video. The word steganography com- bines the Greek words steganos, meaning ”covered, concealed, or protected,” and graphein meaning ”writing. As for these days, we would like to keep some files securely so it will not be altered, or removed by someone irresponsible. In this thesis, we proposed a method for Audio steganography using Data Encryption Standard (DES) and embedded to not just one but two hosts using Least Significant Bit (LSB) algorithm thats why its called Double Audio Steganography. The main objectives of this thesis is to hide audio steganography information inside another audio without people being suspicious and we can do it more safely and more securely. Also, this thesis resulted an audio greater than 20 dB, which is a standard distorted file and successfully embed and extract the secret message completely with anoise of 100 dB or higher and without noise attacking the audio.

Keywords: ***Concealing a file, DES algorithm, Double Audio Steganography, LSB Method.***

1. Background

1. Background

These days, most people are already familiar with exchanging data to one an- other. We can even say, everyday, almost everyone do exchange data, not just in a form of text, but also in a form of audio or video. As the technology grew faster more than ever, exchanging data is even more easier for people to get access to. Exchanging data can be done using internet. Knowing, theres a lot of irresponsi- ble people out there, we proposed an application that can deliver a secret message, while not preventing unintended observer from learning its existence. For example, on December 2009, there was a case about a leak of data of Gmail Users in China. A dozens of gmail users, reported that their data was stolen. This problem was di- rectly responded by Google with a lot of investigation. And was a matter of fact, are true, there were at least 20 companys datas that was successfully hacked by hackers from China. Google gave statement, that this happened, because the hackers might use the gap of the old version of internet explorer as an opportunity.

One of the way to overcome this type of problem is to use Steganography and Cryptography. Cryptography is an art of science for keeping a message and secretly randomize the message to a form that cannot be read [2]. Steganography is the practice of hiding information in plain sight [3]. Steganography is an encryption technique that can be used along with cryptography as an extra secure method in which to protect data. Steganography techniques can be applied to images, a video, file, or an audio file. In cryptography, the structure of the message is altered, so that it is difficult to understand, unless there’s a decryption key. Meanwhile, on steganography, the message is not altered, it is hidden inside a cover medium such a way that the message cannot be detected [4]. Comparing to other method, like Spread Spectrum, that spreads the secret information over the frequency spectrum of the sound file using a code which does not depend on the actual signal and calculated using a psycho-acoustic model [1], this thesis proposed to use Least Significant Bit algorithm, a more simple yet effective approach. To make it even more secure, this thesis used two audio hosts to embed the secret message, that’s the reason why it’s called double audio steganography. The type of audio used is WAV audio.

This thesis successfully embed and extract the secret message completely with a noise of 100 dB or higher, and without noise attacking the audio. To tampered with the audio, this thesis used Additive White Gaussian Noise and the parameters used to test the robustness are Signal to Noise Ratio and Bit Error Rate

2. Basic Concept

2.1 Steganography

Steganography is the art of science dealing with hiding secret data inside image, audio, video or text files. In audio steganography, the message is embedded using binary sequence of the sound file. The usual form of audio steganography are WAV,AU, and MP3 files. while in this thesis, we chose to use the WAV file[2].

Audio steganography hides the secret message on an audio signal called cover audio. Once the secret message is embedded in the cover audio, the resulting mes- sage is called stego message and It is transmitted to the receiver side [4]. There are two process of embedding the audio, thats why its called double audio steganog- raphy. The secret message is encrypted using DES, which produced a chipertext for the first cover audio and stego key which later will be used for the extraction process. The whole Steganography system is shown on Figure 2.1 [5].

There are some parameters that need to be noticed in steganography method, such as:

- Imperceptibility
  Situation where the message can be sense by humans sense, in this case hear- ing.
- Fidelity
  The quality between stego file and the cover object cannot have a big differ- ence between both of them.
- Recovery
  The message that is hidden have to be able to be shown back in the end.
- Robustness
  The message that is hidden have to be resistance to any kind of manipulation.

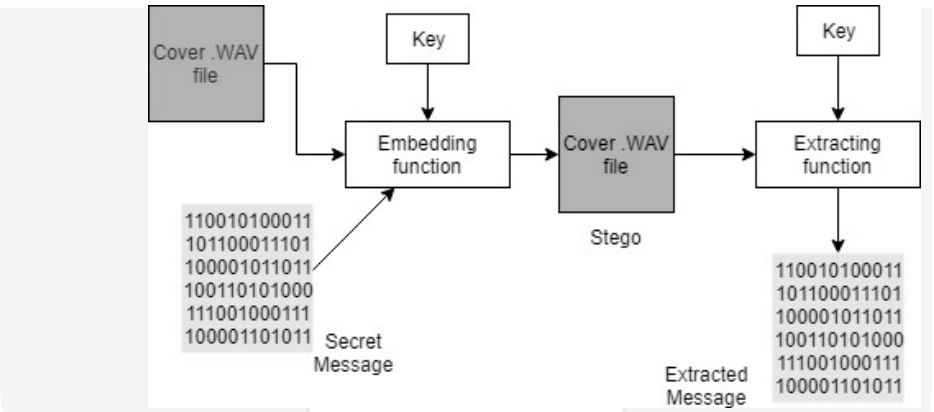

Figure 2.1 Audio Steganography System [5]

2.2 Least Significant Bit Algorithm

The Least Significant Bit (LSB) algorithm, works by replacing the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data. The LSB substitution doesnt degrade the quality of the message in large scale [6]. This algorithm is consider one of the simplest and commonly used technique for audio steganography. The length of the secret message that are meant to be encoded must be smaller than the samples in the audio file. Figure 2.2 shows the LSB procedure in audio steganography.

.

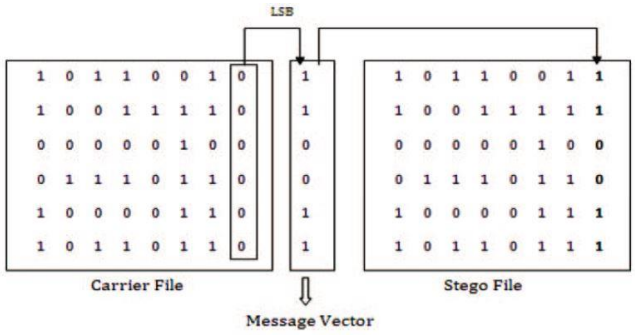

Figure 2.2 The whole process in LSB Algorithm [1]

The major advantage of LSB algorithm are:

1. High watermark channel bit rate low computational complexity of the algo- rithm compared with other techniques.

2. No computationally demanding transformation of the host signal, therefore, it has very little algorithmic delay [6].

For example on Figure 3, if the message is 10 bits, then the bytes that are used are also 10 bytes. Supposed the binary of the embedded message is 1110101011. The result of it is only partly changed. That means the original file size didn't significantly changed, so it is difficult for human senses to tell the difference [1].

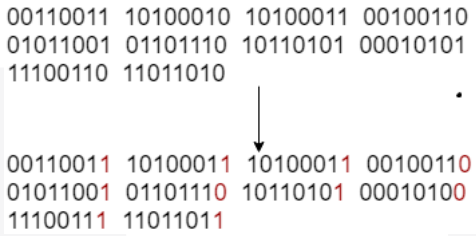

Figure 2.3 The example of LSB procedure [1]

2.3 Cryptography

Cryptography is an art and science for keeping a message secretlychanging the message into a form that cannot be read or understood. In this case, the use of the cryptography method is to keep and secure the content of secret messageitself [2]. There are two process that had to be done in cryptography, the first is encryption and the next one is decryption. Encryption process is a changing process of the orig- inal message (plaintext) into a coded message (ciphertext). Meanwhile, decryption process is the opposite of the encryption, where ciphertext become plaintext. There are two techniques of cryptography,

1. Symmetric Key Cryptography

   In this technique, the key that is being used is private key where both the sender and the receiver uses one key to encrypt and decrypt the message. Various algorithm that use this mechanism are AES, DES, Blowfish, TDES [7]. Figure 2.4 shows the block diagram of symmetric key cryptography.

2. Asymmetric Key Cryptography

   In this technique, the key that is being used is public key. The sender use two different keys for encryption and decryption. The algorithm that usually used this mechanism is RSA [7]. Figure 2.5 shows the block diagram of asymmetric key cryptography.

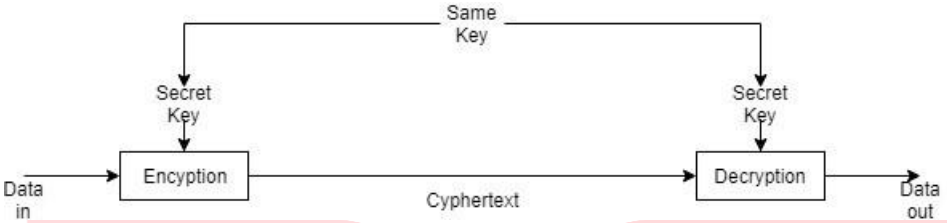

Figure 2.4 The block diagram of Symmetric Key Cryptography [7]

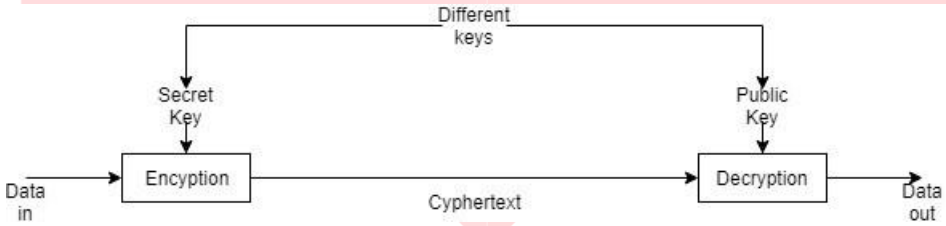

Figure 2.5 The block diagram of Asymmetric Key Cryptography [7]

2.4 Data Encryption System (DES) Algorithm for Cryptography

DES is the archetypal block cipher. An algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bitstring of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can sup- posedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits. In Fig. 2.6 showed that this the- sis need two private key to encrypt and decrypt the cryptography. Figure 2.7 shows the general structure of DES cryptography. The encryption is consist of two permutation (P-boxes), called initial and final permutations, and sixteen Feistel rounds. Each round uses a different 48 bit round key generated from the cipher key according to predefined algorithm [8].

The DES function is made up of three section:

1. An expansion D-box: The expansion D-box is to divided a rate bit key.
2. A whitener (XOR): after the expansion permutation, DES uses the XOR op- eration on the expanded right section and the round key
3. A group of S-boxes: The S-boxes do the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output.

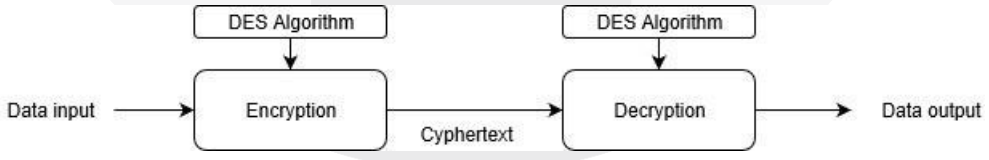

Figure 2.7 The block diagram of DES Cryptography

2.5 Additive White Gaussian Noise (AWGN)

Additive White Gaussian Noise is added to the extracted messages to evaluate the system performance. The values that are taken by this type of noise are Gaussian distributed and it can be defined as statistical noise. The Gaussian random variable are expressed as follows:

$$P_G(z) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(z-\mu)^2}{2\sigma^2}} \qquad (2.1)$$

μ in the expression above is represented as the mean value, while σ are repre- sented as the standard deviation. The white Gaussian noise signal can be produced with a random number generator, in which the whole signal samples follow a spe- cific distribution. For the most part, this type of noise is used in system modelling, where it can be added to audio signals using MATLAB program [9].

2.6 WAV Audio File

WAV is a variant of the bitsream format Resource Ainterchange File Format (RIFF) that works the same as IFF and AIFF. Generally, WAV format is an uncom- pressed audio [10]. WAV consisted of three part, which are RIFF chunk descriptor, sub chunk data, and sub chunk fmt. This thesis used WAV audio file that has 44100 Hz value of frequency sampling and 16 bit of number bits per sample. Figure 2.8 [5] below shows the specifics format of WAV audio file.

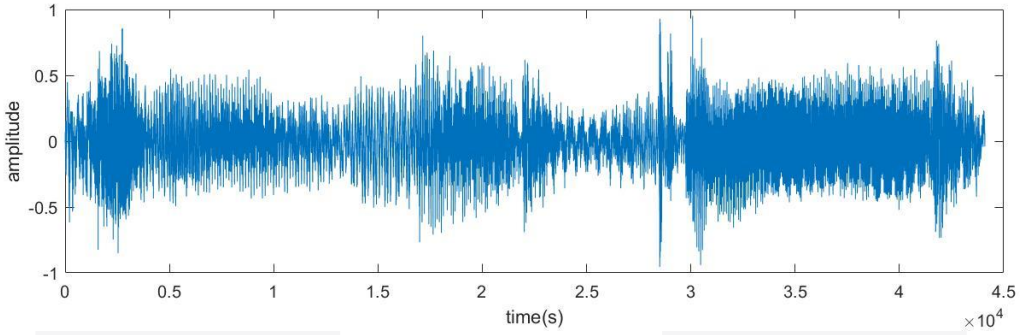

Figure 2.8 WAV File Format [5]

3. System Model and Proposed Technique

3.1. System Model

The system design is explained with the block diagram below. In Figure 3.1, shows there are 4 processes in the system, which are, Encryption, Embedding, Noise, and Extraction process. The first step is to encrypt the secret message which resulted the ciphertext. Then the ciphertext is embedded into the audio secret mes- sage. After the embedding process, the noise is given to the audio to tampered with the quality. To measure the robustness, this system used noise ratio. The last step of the system is to extract the audio stego, and recover the secret message. The input that is being used in the system is an audio message in the form of WAV.

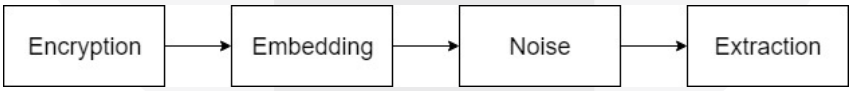

Figure 3.1 The block diagram of system design.

3.1.1 Encryption Scheme

The encryption is done to randomize the secret message. The first step of this thesis is to read the audio that contained a 8 characters long secret message. then the text is processed into a binary rate. After that, the binary rate is vectorized into 64 bit. The final step is to encrypt the vectorized bit using DES algorithm, which then produced a ciphertext for the embedding process and stego key for the extraction process later on. Figure 3.2 shows the flowchart of encryption process.

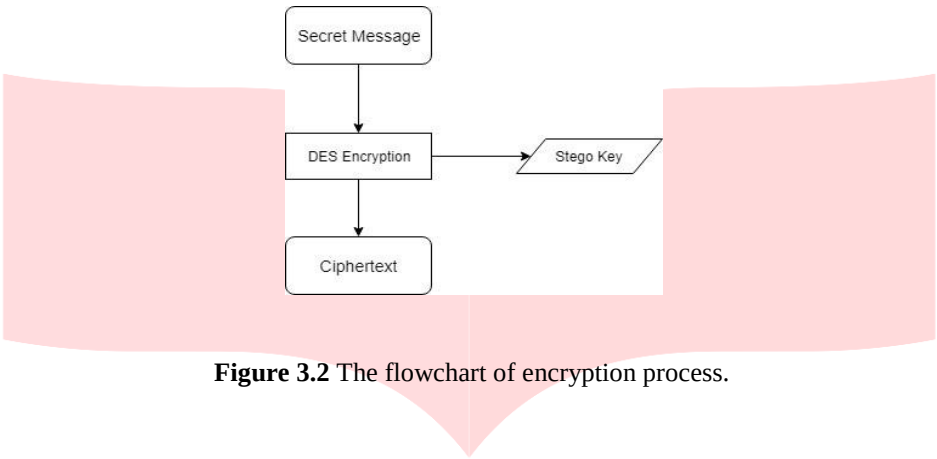

Figure 3.2 The flowchart of encryption process.

3.1.2 Embedding Scheme

The process continues by embedding the ciphertext obtained in the previous Encryption process, into the first cover audio that lasted 1 second. this audio is the first host. The next step is to make the first host as the the second cover audio, which then being embedded into the second host that lasted 16 seconds. This particular step is the reason why this thesis is called Double Audio Steganography. Figure 3.3 shows the flowchart of embedding process.

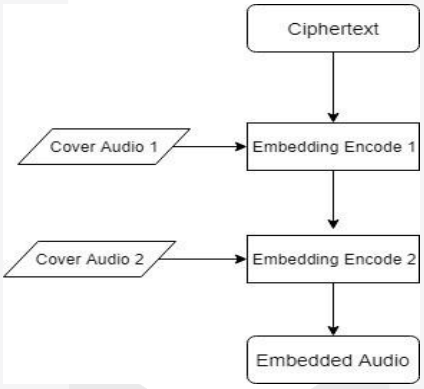

Figure 3.3 The flowchart of embedding process.

3.1.3 Noise Scheme

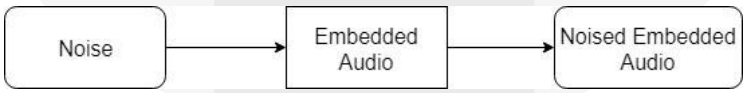

Figure 3.4 The flowchart of inputting noise process.

To test the quality of the audio and to make sure the quality stays the same as the original audio, we input some noise to the embedded audio. Which resulted the noised embedded audio. Using Additive White Gaussian Noise (AWGN), the parameters used for this test is Signal to Noise Ratio (SNR) and Bit Error Rate (BER). Figure 3.4 shows the flowchart of inputting noise process.

3.1.3 Extraction Scheme

The final step of this thesis is to extract the secret message from the previous noised embedded audio. The first part of the extraction process is to extract the noised embedded audio. From this, the writer obtained the audio 1. After that, to obtain the secret message, the writer did a decryption process. Figure 3.5 shows the flowchart of extracting process.

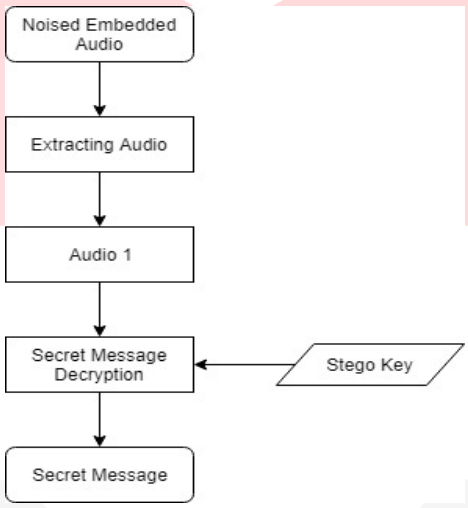

Figure 3.5 The flowchart of extracting process.

3.2 System Performance

Assessment of the performance or quality of this system is done by objective assessment. The assessment is done by tampering the quality of the audio using Additive White Gaussian Noise (AWGN). the results of the assessment are used in the process of feasibility analysis of the designed system. The objective assessment is to evaluate the following steganographic and cryptographic methods as folows:

1. Signal to Noise Ratio (SNR)

   Signal to noise ratio (SNR) is a technique for measuring the quality of the audio, objective and subjective. Subjective measurement is done by listening to the stego file and compare it with the initial file, while objective measurement is estimated by computing Signal to noise ratio (SNR) of stego file. SNR is calculated the decible (db) of the audio stegano file. [11]

$$SNR = 10log10\left[\frac{\Sigma_{i=0}^{n} f^2(n)}{\Sigma_{i=0}^{n}(g(n) - f^2(n))^2}\right] \quad (3.1)$$

   where *f(n)* is the original audio and *g(n)* is the stego audio. A quality can be considered good when the SNR is higher than 20 dB, which is a standard distorted file.

2. Bit Error Rate (BER)

   Bit Error Rate is used to knowing the percentage of comparison between the bit that resulted from the process of message extraction and the bit that is embedded.

$$BER = \frac{h(n)}{i(n)} \times 100\% \quad (3.2)$$

where *h(n)* is the number of error bit and *i(n)* is the number of bit. The value of BER plays a huge role in deciding the percentage of the level of mistake and the level of preciseness in message extraction. The lower the BER, the lower the level of mistake had been done, and vice versa [12].

4. Conclusion

This thesis proposed a method to embed the secret message using double au- dio steganography and DES cryptography with least significant bit method. The main objectives of this thesis is to sent a secret message securely while still maintaining the quality of the audio and to recover the secret message after the message is sent. By attacking the secret message using Additive White Gaussian Noise (AWGN) on both audio host 1 audio host 2 with Sig- nal to Noise Ratio (SNR) and determine the Bit Error Rate (BER) values. After 20 trials of both the attack on audio host 1 and audio host 2, this thesis concluded that the secret message can only be recovered on parameter of 100 dB and higher. This means that LSB method is fragile to noise attack. Be- cause, on LSB the noise attacks the amplitude of the audio, a slight change in amplitude of an audio affected the audio in significant way. Even though all methods in steganography is also fragile to noises, LSB is the most fragile of them all. Regardless, This thesis without noise added, and when the noise is 100 dB and higher, can successfully recovered the secret message and the quality of the audio remains good. another reason is DES cryptography had a capacity message of 64 bit per block, which means it is more suitable to be use for short messages.

Reference:

[1] Mazhar Tayel, Ahmed Gamal, and Hamed Shawky. ”a proposed im- plmenntation method of an audio steganography technique”. 2016.

[2] S. R. Gouda. ”least significant bit (lsb) and discrete cosine transform (dct) based steganography”. In *International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)*, volume 3, 2015.

[3] Zameer Fatima and Tarun Khanna. ”audio steganography using des al- gorithm”. In *Proceeding of the 5th National Conference*, New Delhi, India, 2011.

[4] Jithu Vimal and Ann Mary Alex. ”audio steganography using dual ran- domness lsb method”. In *International Conference of Control, Instru- mentation, Communication, and Computational Technologies*, Trivan- drum, India, 2014.

[5] Satish Bhalshankar and Avinash K. Gulve. Audio steganography: Lsb technique using a pyramid structure and range of bytes. *International Journal of Advanced Computer Research*, 2015.

[6] Harshita Kapadia, Harawane Sneha Haribau, and Harsha Patil. ”audio steganography and security using cryptography”. In *International Journal of Computer Science and Network*, Pune, Maharashtra, India, 2015.

[7] Paddambail, Yashika, Kripa N Bangera, Subba Reddy, and Shivaprasad G.”multilayer security using rsa cryptography and dual audio steganog- raphy”. In *IEEE International Conference on Recent Trends in Electronics Information and Communication Technology*, India, 2017.

[8] Y. Perkhasa, W. Suadi, and B. A. Pratomo. ”implementasi kriptografi dan steganografi pada file audio menggunakan metode des dan parity coding”. In *ITG Workshop on Smart Antenna (WSA)*.

[9] Mahmood Maher Salih and Mohammed Salem Atoum. ”applying awgn mp3 steganography attack in bilsb and slsb techniques”. In *4th Inter- national Conference on Advanced Computer Science Applications and Technologies*, 2015.

[10] Lindawati and Rita Siburian. ”steganography implementation on an- droid smartphone using the lsb (least significant bit) to mp3 and wav audio”. In *The 3rd International Conference on Wireless and Telemat- ics*, July 2017.

[11] Nyoman Putra Sastra Ida Bagus Adisimakrisna Peling. Enhanced au- dio steganografi dengan algoritma advanced encryption standard untuk pengamanan data pada file audio. *Majalah Ilmiah Teknologi Elektro*, 17 (1), Januari - April 2018.

[12] A. S. Hadiningrat. ”analysis of message security using modified en- hanced lsb and four neighbors steganography with chaining hill cipher cryptography algorithm”. 2016.