Designing the Application of Security Text Messages Into Audio Files Using Data Encryption Standard (DES) Algorithms Using the End Of File (EOF) Method

A M H Pardede¹*, Anggi Pramana¹, Muhammad Zarlis², Akbar Iskandar³, Rosida Tiurma Manurung⁴, S Sriadhi⁵, Citra Kurniawan⁶, Abdurrozzaq Hasibuan⁷, Nurintan Asyiah Siregar⁸, Ayu Esteka Sari⁹, Indrya Mulyaningsih¹⁰, Teguh Hidayat Iskandar Alam¹¹, Ibrahim¹², Tri Listyorini¹³, Edy Winarno¹⁴ and Tulus¹⁵

¹STMIK Kaputama, Binjai, Sumatera Utara, Indonesia
²Department of Computer Science, Universitas Sumatera Utara, Medan, Indonesia
³Department of Informatics, STMIK AKBA, Makassar, Indonesia
⁴Graduate Program in Scientific Psychology, Universitas Kristen Maranatha, Indonesia
⁵Department of Electrical Engineering, Universitas Negeri Medan, Indonesia
⁶Department of Electrical Engineering, Sekolah Tinggi Teknik Malang, Indonesia
⁷Faculty of Engineering, Universitas Islam Sumatera Utara, Medan, Indonesia
⁸Department of Management, STIE Labuhanbatu, Sumatera Utara, Indonesia
⁹Department of Management, STIE Sakti Alami Kerinci, Jambi, Indonesia
¹⁰Department of Indonesian Language Teaching, Institut Agama Islam Negeri Syekh Nurjati Cirebon, Indonesia
¹¹Department of Informatics Engineering, Universitas Muhammadiyah Sorong, Sorong, Indonesia
¹²Department of English Education, Universitas Muhammadiyah Sorong, Sorong, Indonesia
¹³Department of Informatics, Universitas Muria Kudus, Indonesia
¹⁴Faculty of Information Technology, Universitas Stikubank, Semarang, Indonesia
¹⁵Department of Mathematics, Universitas Sumatera Utara, Medan, Indonesia

* akimmhp@live.com

Abstract. There are several ways to deal with security issues of confidential data sent via the internet, including using cryptographic techniques and steganography. Steganography is the science and art of concealing information / messages in a media in such a way that its existence is not detected by other parties who are not entitled to the information. Instead, cryptography disguises the meaning of a message, but does not hide that there is a message because the file looks suspicious. The Steganography technique used here was End Of File (EOF). The EOF technique described how to add data or files at the end of the image file. For this technique, the size of data or files that will be hidden could be larger than the size of the image file. The hidden data will be inserted at the end of the file so that it will not affect the image. This steganography application is also equipped with a cryptographic function Data Encryption Standard (DES) at the time of insertion of data that functions as a generator code and encrypts data, so that the security of a data in the file is more protected and protected from those who are not entitled to know the data.
1. Introduction
Nowadays, the development of technology enabled human to work with computer. It facilitates and helps
human solving problems related to computer. Research from a number of researchers has tried to find
effective algorithms to improve the quality of encryption, such as determining the generation of primes,
This includes involving search problems and also super encryption. This can be done by involving a
combination of several cryptographic algorithms[1]. Research from cryptography basically requires
adequate mathematical programming skills[2]. The success of a cryptographic algorithm also needs to be
determined through the process of measuring effectiveness based on the benchmarking principle[3]. This
opens up many opportunities in developing computer applications but also creates opportunities for
threats to data stealing and modification. Therefore, to protect data from being stolen, data security
devices on a computer must be provided [4]. Data stealing through internet media is now very
widespread, because it is easy to do by tappers and many business people who still do not realize it, so
easily and without thinking send important data through the internet, one of them sending data via email.
The very rapid industrial market competition now allows each competing company to do something that
is unfair and fraudulent, by tapping the data sent through the internet, allowing them to copy or take
patents, which makes competition become unhealthy because of dropping fellow competitors. For this
reason, supporting applications are needed that can make data unable to be tapped, even not attracting
the attention of the thieves, the application in question is the Steganography application.

2. Related Works
Steganography is an art or science used to hide secret messages so that in addition to the intended person,
other people will not be aware of the existence of the secret message. Steganography requires two very
important parts such as file or container media and confidential data that will be hidden. Steganography
serves to disguise the existence of confidential data so that it is difficult to detect, and can also protect the
copyright of a product. Confidential data that is hidden can be re-disclosed the same as the original
without damaging the media files and messages. One of the commonly used Steganography techniques is
the End Of File (EOF) method. This technique is not much different from the Least Significant Bit (LSB)
technique. If LSB adds data files at the end of the bit, then EOF immediately adds data at the end of the
image file, and before the message is marked it is in the form of characters / symbols. For this technique
you can add data or files that will be hidden more than the size of the image file. The hidden data will be
inserted at the end of the file so that it does not affect the image.

3. Research Methods
There are several steps done in order to solve the problem of application design Security Text Messages
into Audio Files Using Data Encryption Standard (DES) Algorithm By Utilizing the End Of File Method
(EOF):
1. Collecting Theories and Example of Cases
The theories related to the problem of steganography, cryptography, EOF techniques and DES algorithms
were collected. These collected from several sources such as books in the library, articles on the internet
and references from other student final assignments related to the problem at hand.
2. Designing Programs
The program was designed to be able to do the technique of hiding text in other data without changing the
data that is boarded, where the technique used was the EOF method and the DES algorithm. The first step
in designing this program was designing a system work process. The process of work described by a
flowchart which explained in detail the processes that the program was doing in inserting a text on an
audio document. The next step was to design the form of the program. The form would be required with
buttons that can be used by the user to interact with the program that is designed. In this step, a
programming algorithm also needed to be designed to be used in implementing the program design.
3. Implementing the Program Design
The programming language in the implementation of the program design was Microsoft VB.net 2010.
This programming language was more familiar than other programming languages. At this stage, the
program display design and coding according to the programming language used needed to be
implemented. The implementation stage of the program was making the form display, making the required modules and coding the buttons and menus on the form and at the end, testing the program. In this final stage, a series of tests on the resulting program was conducted. These tests are carried out to find errors in the program and make necessary improvements. The scheme of problem solving method that the writer did can be seen in Figure 1.

In order for this data security software to work properly, there are several requirements that must be met such as:
1. Hardware (Hardware)
   Intel® Core TM 13-3217U CPU @ 1.80 GHz, 500GB hard drive and 2GB RAM.
2. Software (Software)
The programming language used is Visual Studio 2010 and runs on a Windows operating system.

4. Results and Discussion
Application Program for Security Text Messages Into Audio Files Using Data Encryption Standard (DES) Algorithm By Utilizing the End of File (EOF) Method was built with the aim to maintain the security of text sent to other users by inserting the contents and rereading the contents so that the original message can be read, in this case the user must have this application. The implementation of the program was done using Visual Basic .Net 2010 that already existed when installing Visual Studio 2010. Visual Studio 2010 was used to create applications in a computer so that the applications created can be run and tested directly on the computer. To run an application, a user must click the data security application icon. Then the home screen will appear which contains the audio load button, read text, insert text, password box and text box. The trial process that I do includes the process of inserting text through the text insert button and reading text through the text read button.
Figure 2. Steps how to insert texts

The original text is converted into encryption with cryptography using the DES algorithm. After the text becomes encryption, the text and password are inserted into the audio with the key as an identifier in steganography using the End Of File (EOF) method. The key functions when reading text in audio which indicates there is text in the audio.

Figure 3. Steps how to read texts

Encryption text is decrypted using DES algorithm. The file in the audio is read by steganography using the End Of File (EOF) method which the key will be read as an identifier, the text is hidden in the audio. The original text (plaintexts) appeared as a result. Based on a series of planning and testing of each element or menu, the author can report that the application run according to planning. The application could insert text on audio. Then the texts were readable in the audio into the original text in the recipient's text application. For more details, see Figure 4 and Figure 5 below.

Figure 4. Appearance of text insertion using application

The form above is a text insertion form. Sender can input audio as a container media and the desired text to be inserted and password as a key. The inserted password will be changed to the DES form, after which it is inserted using the End Of File (EOF) method.
Figure 5. Appearance of text read using application

The form above is a text reading form. Receiver can input audio that has been inserted text, then password as key. Audio that has been inserted text will be read using the End Of File (EOF) method, to output text in audio. Text removed from audio is still plaintext. Program evaluation is one of the things that need to be done in every application development to analyze and find out the results achieved by the application developed. Likewise for text messaging security applications into audio files using data encryption standard algorithm (DES) by utilizing the End Of File (EOF) method, a program evaluation is performed to analyze the results achieved in this application. And in the evaluation found several advantages and disadvantages of the program which was seen from several conditions and situations. The advantages and disadvantages of the applications developed are as follows:

a. Advantages
   1. The size of hidden text is unlimited.
   2. Can be password protected with unlimited length.
   3. With this application, it can make it easy for users to encrypt text without having to do calculations.
   4. Maintain the security of the contents of the text that will be sent.

b. Disadvantages
   1. Just insert text, it can't be any format file.
   2. Can only use the introductory media in the form of audio, cannot use other media.
   3. Applications can only run on Windows operating systems.

5. Conclusion

From the results of the research, it can be concluded that:
1. The texts can be protected with limitless password.
2. The smaller files can accommodate larger texts.
3. Cryptography using the DES algorithm by utilizing the EOF method can be done by hiding the results of encrypted text messages into audio media.
4. Audio with inserted messages had larger capacity than audio with no message inserted.

References
[1] M. Mesran et al., “Combination Base64 and Hashing Variable Length for Securing Data,” J. Phys.: Conf. Ser., vol. 1028, no. 1, p. 012056, 2018.
[2] Munir, Rinaldi. 2006. Kriptografi. Informatika, Bandung.
[3] Y. Anggraini and D. V. S. Y. Sakti, “Penerapan Steganografi Metode End of File (Eof) Dan Enkripsi Metode Data Encryption Standard (Des) Pada Aplikasi Pengamanan Data Gambar Berbasis Java,” Konf. Nas. Sist. Informasi, STMIK Dipanegara Makassar, no. September 2016, pp. 1743–1753, 2014.

[4] Ariyus, Dony. 2006, Keamanan Multimedia. Yogyakarta: Penerbit ANDI