Implementation of Securing Data in the Cloud using Combined Cryptography and Steganography

http://dx.doi.org/10.28932/jutisi.v5i2.1922

Rosalina ✉ #1, Nur Hadisukmana#2

President University, Faculty of Computing
Jl. Ki Hajar Dewantara, Cikarang Baru, Bekasi
[1]rosalina@president.ac.id
[2]nurhadisukmana@president.ac.id

Abstract — **The recent advance in the information technology field, forcing us to ensure the privacy of the digital data. It is very important to develop a method that may satisfy the needs. Many methods/techniques applied to reach that goal. One of the efficient way to reach that secrecy can be achieved by implementing steganography. TheStego application is using Steganography to work in the digital domain and hides the data information within a speech signal. To increase security, TheStego combines steganography techniques with MD5 encryption techniques. Steganography techniques applied in TheStego application is LSB (Least Significant Byte) method. This application has three main features: hide text in an audio carrier, hide image within the audio and audio inside a wave signal of an audio carrier. TheStego also required the user to enter a password before the processing of data hiding begins. The password will act as a decryption password. Such an approach is implemented to increase the security of this application. So, only the one who knows the password that can extract and decrypt the data inside the application. The paper represents that, the proposed method could secure the hidden data but the quality of the output may create noticeable noise/distortion but it did not have many differences as the original.**

Keywords— **Cloud; Cryptography; Steganography; Securing Digital Data**

I. INTRODUCTION

Cloud computing enables users to transmit their data to cloud servers, users could access those data remotely over the Internet. It is also known for its flexibility and cost saving, that is the most basic reason for many companies to use this technology, they don't need preparing the infrastructure and maintenance of their own servers. The company can also freely choose the appropriate services and can be changed as needed at any time, and they don't need to care with the complexities of managing servers directly. The critical aspect related to the importance of data that is transferred on the cloud is security since the data can be confidential. Thus, the data security should be enhanced and the data is protected from malicious attracts.

Deputy Chief of police of the Republic of Indonesia, Commissioner General Syafruddin [1] said that the cybercrime vulnerability in Indonesia is number two highest in the world after Japan. The type of cybercrime that mostly did spread hoax and stealing of secret personal data like document or photo. Data usually stolen in a process of data transfer through email or file transfer. It usually happened because there is a lack of data protection or security method in that process.

Cryptography and Steganography are a technique that could be used as a data protection method. Cryptography is a technique to protect a data by changing the content of that data into a character that could not be understandable by the other person. While steganography is a technique of hiding a data inside other data. The use of steganography technique makes the other people do not realize that there is existing a confidential data in the data transfer. Media that commonly used to carry the secret message or data are image or audio.

Many researches have been conducted to secure the data by combining cryptography and steganography, combining these two techniques could enhance the security [2-5]. A new approach proposed for encrypted the image by shuffling the RGB pixels [6], in the proposed approach the cipher image were retrieved by extracting the RGB pixels of the input image, then the RGB values were swapped by changing the position and the values of the RGB pixels. [7] also proposed encryption technique by shuffling the RGB pixel values by displacing the RGB pixels and also interchanging the RGB pixel values, and at the end the total image size before encryption is the same as the total image size after encryption. While [8] proposed on key generation on a 2D graphics using RGB pixel shuffling and transposition, it fetched the RGB pixel values from cipher algorithm of m*n size image. Securing image digital data could be done using ANN Method [9]. Combination of cryptography and steganography used to secure digital data by combining three techniques: image compression, cryptography, and steganography [10]. [11] Conduct a research on video steganography using Arnold Scrambling and DWT, in [12] using block matching in DWT domain to

improve the quality of the reproduced secret image. In [13] presented combination of cryptography and steganography by using sequential techniques and symmetric XOR technique. In [14] presented another steganography method which is used Least Significant Bit applied in cover image and Most Significant Bit applied in secret image.

The objective of this research is to develop an application using md5 encryption and LSB method that can be used to easily hide a data in the form of text, image, or audio in an audio as the media carrier. The goal is the secret data could be transferred safely without being noticed by another person.

This research is expected to achieve the objective. Therefore, this research focuses on the following:

- Application will be developed only for Windows OS
- Steganography method used is the Least Significant Bit (LSB)
- Encryption method used is MD5
- Data that could be hidden only text, image with .png format, and audio with a .wav format
- The carrier media that used to hide the data is using .wav audio format
- The LSB method used may cause noticeable noise in the audio output
- Maximum width and height for image hiding is an image with 100x100 pixels
- WAVE audio file accepted only 8bit WAVE audio

II. LITERATURE REVIEW

This research uses a combination of cryptography and steganography methods to improve security of data which is will be stored in the cloud servers. This combination method manages data in three formats: text in audio, images in audio, audio in audio.

This research implemented LSB as the steganography method and the RGB-Shuffling method, while the priority of this research is to request and secure confidential data from unauthorized users.

A. Cryptography

The encryption process is the process to change files that can be read into files that cannot be read. This research implements Encryption using MD5 algorithm. MD5 is short for Message-digest Algorithm 5. MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual.

B. Steganography

Technically, steganography means hiding the right message or insert messages in the container media. Secret message inserted into the media container so that someone will not be aware of the existence of the message. Steganography not only could conceal data in an audio, but also could conceal the data in an image or a video. All of the type of carrier is unique, how to hide a data inside it depend on its own characteristic. Multimedia file like an image, audio, or a video may have a noticeable noise/distort in its quality.

The method of hiding an information on this research is using Least Significant bit (LSB) method. This method will change the value of the bit in the rightmost position. Because of the value of that bit is low, the file expected not to affect much of the final bit value that have been altered. The alteration for an audio file should only change the content of that audio without altering the header of that audio. Because if there are changes in the header, the file format may become unknown and could corrupt that audio. For the example, the audio WAV file header contains an information like bit rate, channel, mono or stereo. If the header information is altered, the player may not be able to play that WAV file.

C. WAV Audio Format

The WAV stands for Waveform Audio Format . A wave file is a collection of a number of different types of chunks: main chunk, chunk format, and data chunk [15]. Header format of wave audio file is listed in Table I and data chunck of wave audio file is listed in Table II.

TABLE I.

HEADER FORMAT OF WAVE (.WAV) AUDIO FILE

Field Name	**Size(Byte)**	**C# Data Type**	**Value**
ChunckID	4	Char [4]	“RIFF”
ChunckSize	32	uint	varies
Format	4	Char [4]	“WAVE”

TABLE II.

DATA CHUNCK OF WAVE (.WAV) AUDIO FILE

Field Name	**Size(Byte)**	**C# Data Type**	**Value**
SubChunck2ID	4	Char [4]	“data”
SubChunk2Size	32	uint	varies
Data	Number of element in sample data: SampleRate * NumChannels * audio duration(seconds)	Byte[] for 8-bit audio Short[] for 16-bit audio Float[] for 32-bit audio	Sample data

D. Related Works

There are many steganography applications that already developed, but with differences in the feature and the format for the carrier to conceal the information. Some of the applications that already developed are:

1) Xiao Steganography

Figure 1. XIAO Steganography Screenshoot [16]

Figure 1 shows Xiao Steganography, a cross-platform utility that comes packed with encryption capabilities. XIAO steganography could hide text messages or other files within images or audio tracks. This application also offers step-by-step guidance through the entire operation. The application have the compatibility to use image files and WAV format as the carrier.

Xiao steganography is able to preview the file in a dedicated pane and view details about the file, such as name and size. This application also could add multiple items to the list. Xiao Steganography enables users to choose between different encryption algorithms (e.g. RC2, DES, Triple DES, MD5), and set up passwords. User need to pick a saving directory and specify the filename. It also offers time estimation for completing the job. When it comes to extracting the hidden content from the encrypted files, user have to upload the items to the list. During the testing of this application, it shows that the program processing the task fast and without errors. All things considered, Xiao Steganography offers an intuitive layout for helping user encrypt data within images or audio files. Moreover, the performance is considered light for the system [16].

2) Quick Stego

QuickStego does not ENCRYPT the secret text message though it is well hidden in the image. If the user require the message to also be encrypted (for the case if the file is stolen, it can't be read without knowing a password), this application could also have the encryption feature. To conclude, this application allows user to securely encrypt text and files and even hide files on the computer [17].

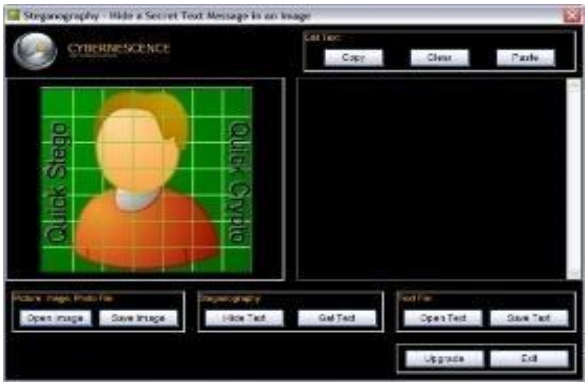

Figure 2. QuickStego screenshot [17]

Figure 2 shows QuickStego application, it lets user to hide text in pictures so that only other users of QuickStego can retrieve and read the hidden secret messages. Once the text is hidden in an image the saved picture is still a 'picture', it will load just like any other image and appear as it did before. The image can be saved, emailed, uploaded to the web (see the picture of the lady with a laptop above - this image has hidden text) as before, the only difference will be that it contains hidden text.

3) Deep Sound

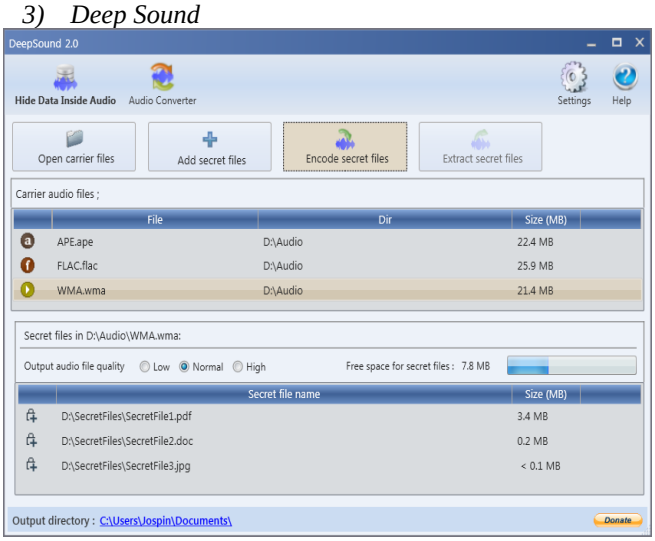

Figure 3 Deep Sound screenshot [14]

Figure 3 shows DeepSound application, a steganography tool and audio converter that hides secret data into audio files.

The application also enables user to extract secret files directly from audio files or audio CD tracks. DeepSound might be used as copyright marking software for wave, flac, wma, ape, and audio CD. DeepSound also support encrypting secret files using AES-256(Advanced Encryption Standard) to improve data protection. The application additionally contains an easy to use Audio Converter

Module that can encode several audio formats (FLAC, WMA, WAV, APE) to others (FLAC, WAV, APE). There are several differences of this research application with the other related works applications [18].

Table III. shows the comparison between TheStego, Xiao Steganograpy, Quick Stego, and Deep sound.

TABLE III.

FEATURE COMPARISON BETWEEN THESTEGO AND RELATED WORKS

Features	**Xiao Steganography**	**Quick Stego**	**Deep Sound**	**TheStego**
Encryption	RC2, DES, Triple DES, MD5	None	AES-256	MD5
File Input	Jpg, png, WAV	Jpg, png, text	WAV, WMA, audio CD	Bmp, Text, WAV
File Output	Jpg, png, WAV	Jpg, png	WAV	WAV

III. RESEARCH METHODS

The development of this application is focused on how to secure confidential data or information from cybercrime. The solution is provided by using technique of data concealment called steganography. The data that can be concealed is a text, an image, or an audio. The secret information will be hidden in an audio. This research chooses an audio as the carrier and LSB for the steganography method. But, one thing to remember is that the quality of the output may create noticeable noise/distortion even though the bit did not have many differences as the original.

As mentioned above, steganography method that used in this research is Least Significant Bit (LSB). This method works by hiding the information or file into the rightmost bit. With this method, there are not much alteration that affects the carrier file, even it is so close to the original quality. The concern using this method is the message that could be hidden is not much, because of the bit capacity of the carrier file.

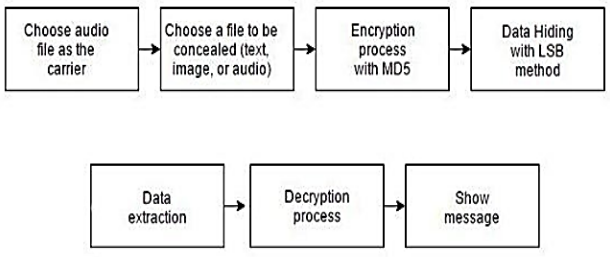

Figure 4. Application flows for TheStego Application

Based on Figure 4, the first process is choosing the audio file as the carrier for the concealed information or for extracting data from the existing hidden information from the carrier. The type of file that could be hidden are text, image, and audio. After user choose the audio carrier and the information to be hidden, it will be encrypted with MD5 before hiding process. After that, it will be hidden using the LSB method.

The data that already concealed could be extracted to see the content of the secret data. Extraction will process the binary data of the audio carrier to be reconstructed into the original form. Before it could be seen as the original data, it still encrypted with MD5 so the process of decryption with MD5 is required for the data could be recovered like the original state.

In this research to hide audio files, whether audio to audio or text to audio, the first step to do is process of initialization of recognizing a signal audio by creating the memory stream and binary writer, then convert it to binary. The data of the wave audio should be converted into binary because when the data of signal audio is still in hex, it cannot be modified by using LSB method. The next step is taking the information of the leftstream and rightstream of an audio. So the hex of the both stream will be converted into a string and after that, the data will be converted into char (example: from 13 14 15 16 into 1 3 1 4 1 5 1 6). The next is converting the stream into binary. For the message that will be embedded, the message will be converted into char and then converted into a binary. And the third step is the process of the LSB method. The original leftstream of the wave audio signal will be duplicated to be modified. Then it will count the size of the leftstream available and compare it with the message size that will be hidden. If it satisfied the requirement, then the LSB process will start by replacing the last digit of the leftstream with the message. If the leftstream size did not fulfil the requirement, then an error message will be displayed. After that, the data of the modified leftstream will be converted again back to string to

be replaced the original leftstream. The last step is the process of recognizing the format of the file. When program found string "START", it means there are hidden data in the audio wave signal. The program then searches for the end message. The end message could form string "TXT", "GBR", or "WAV" which represent the hidden data. "TXT" for text, "GBR" for an image, or "WAV" for audio.

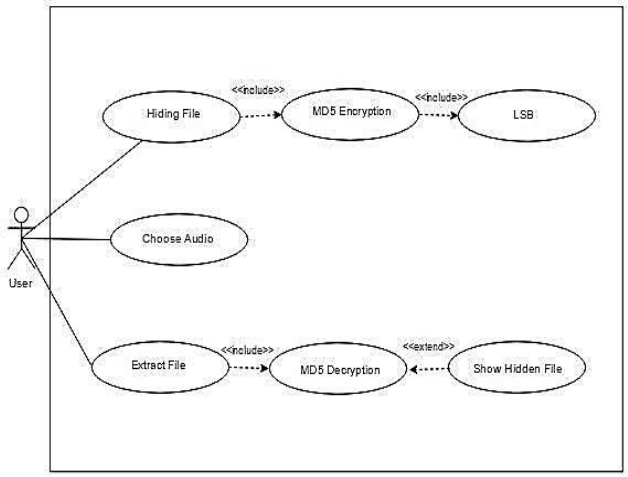

Figure 5. Browsing Audio File

Based on Figure 5, the first process is choosing the audio file as the carrier for the concealed information or for extracting data from the existing hidden information from the carrier. The type of file that could be hidden are text, image, and audio. After user choose the audio carrier and the information to be hidden, it will be encrypted with MD5 before hiding process. After that, it will be hidden using the LSB method.

The data that already concealed could be extracted to see the content of the secret data. Extraction will process the binary data of the audio carrier to be reconstructed into the original form. Before it could be seen as the original data, it still encrypted with MD5 so the process of decryption with md5 is required for the data could be recovered like the original state.

Figure 6 shows the process of LSB method that takes the data that already encrypted and change it into the form of binary. Secret data in a binary form will be hidden in the file of audio carrier.

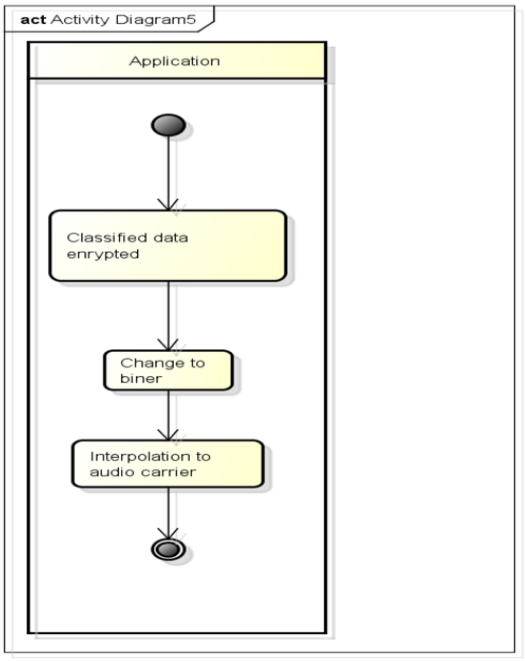

Figure 6. LSB Swimlane Diagram

IV. IMPLEMENTATION RESULT

TheStego developed with using C# programming language with the visual studio as the editor. This research uses C# as the programming language and visual studio as the editor because the simplicity that it offers in making the application form for the development process.

TheStego consist of one main form. The feature in this main form is hidden text, hidden picture, and hidden audio. The main form display can be seen at Figure 7.

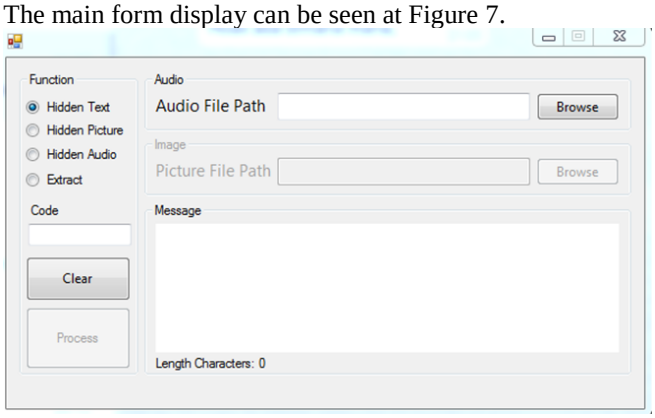

Figure 7. Main Interface

Referring to Figure 5, the Main Form function will be explained in detail as follow:

- Function section will provide the application feature. Every single function will have a different response from the application.
- Code textbox is used to input string that will act as the key for the encryption and decryption process.

p-ISSN : 2443-2210
e-ISSN : 2443-2229

- Audio Column will be used to browse the audio file that will act as a carrier for the secret data/file that will be embedded. While the column below it will be used to browse the file that will be hidden.
- Message column is used to input/previewing the secret text that will be embedded.
- Clear button is used to clear the information that existed in the form.
- Process button have the function to runs the process of data hiding.

A. Hidden Text

In order to hide the text in the audio file, first the user need to browse for the audio carrier. When the user click browse button, the user will be able to search for audio file as shown in Figure 8.

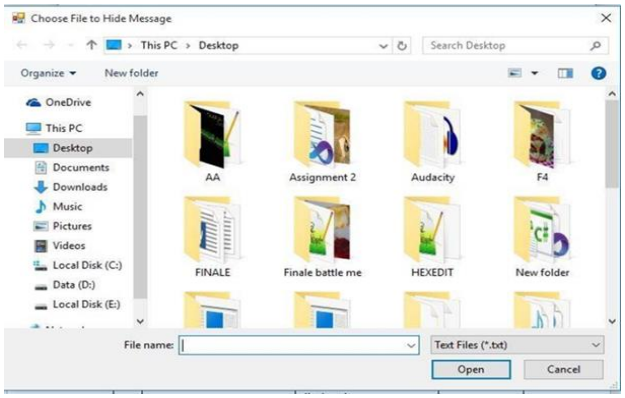

Figure 8. Browsing Audio File

After selecting the audio carrier, then the user need to fill in the hidden text in the message area, if the text is ready as a file txt then the user could import the file by clicking browse button. The user also required to fill in the secret code as shown in Figure 9, then to process hiding the text in an audio file, the user can click the process button.

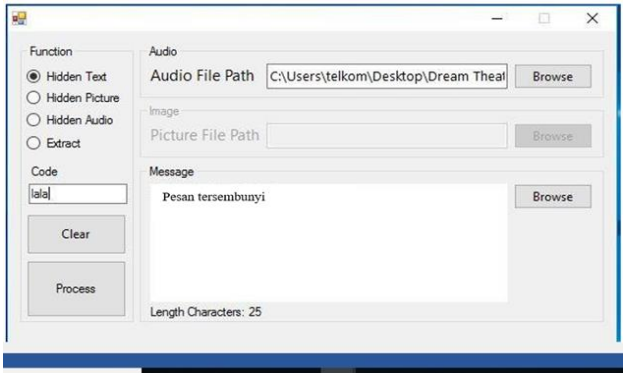

Figure 9. Hidden Text Interface

```
if (radHiddenText.Checked == true)
{
prosesStatus(true);
message = txtMessage.Text.Trim();
message = CryptorEngine.Encrypt(message, true);
message = message + #TXT";
if (message == "")
MessageBox.Show(this, "Write Message to Hide!", "",
MessageBoxButtons.OK,
MessageBoxIcon.Exclamation)
```

Figure 10. Hidden Text Code

The audio carrier is shown in Figure 11. After it is inserted with hidden text, the result is shown in Figure 12.

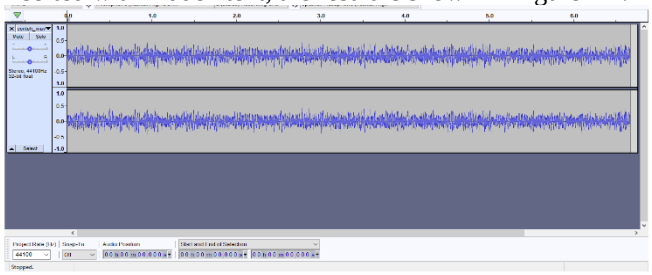

Figure 11. Audio Carrier

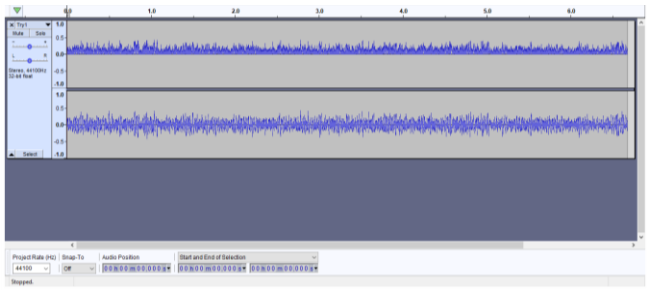

Figure 12. Hidden Text in Audio Carrier

Every different type of file that would be hidden require a different have a different approach on how the application should processed it. Every different type of file already given mark at the processing step. The message at the end of text type of the file will have #TXT at the end of the message, for the image and audio are #GBR and #WAV, as shown in Figure 10 and Figure 13.

B. Hidden Picture

Hidden picture could be done by selecting the audio carrier first, and then select the image by clicking the browsing button (shown in Figure 13).

JuTISI
Jurnal Teknik Informatika dan Sistem Informasi

```
if (radHiddenGambar.Checked == true)
{
prosesStatus(true); rgbMessage = ""; try{
Bitmap img = new
Bitmap(dlgBrowseImage.FileName);
Color c;
  sizeMessage = "(("+img.Width.ToString() + "X" +
  img.Height.ToString()+"))";
   for (int i = 0; i < img.Width; i++)
   {
   for (int j = 0; j < img.Height; j++)
   {
   c = img.GetPixel(i, j); string hexName = c.Name;
   hexName = hexName.Substring(0, 8); rgbMessage =
   rgbMessage + hexName;}
   }
   txtMessage.Text = rgbMessage;
   }
```

Figure 13. Hidden Picture Code

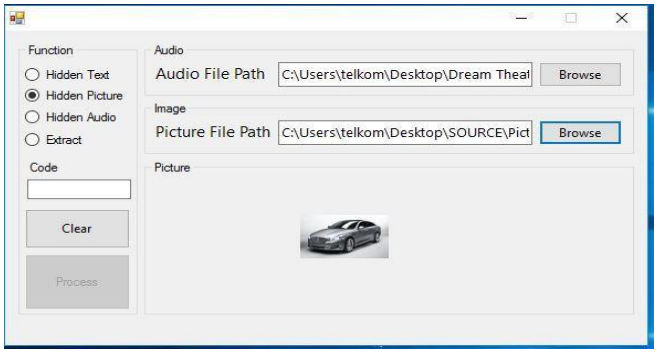

Figure 14. Selecting Audio Carrier and Image Path

The maximum size for the image is 100x100 pixel, if the user chooses the image file which is larger than what is required by the system, then the pop up menu will show up as shown in Figure 15.

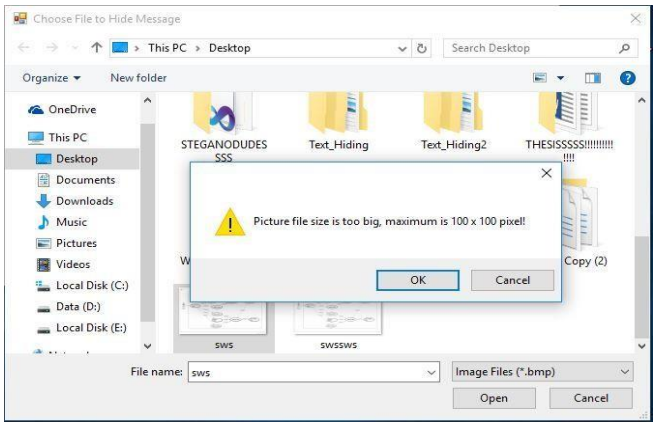

Figure 15. Notification of image size

The next step to hide images in audio carrier is filled with secret code (as shown in Figure 14) as without this secret code the process button will still disabled or cannot be used to process to hide the file. After the secret code is inserted, then, the process button will be enabled as shown in Figure 16.

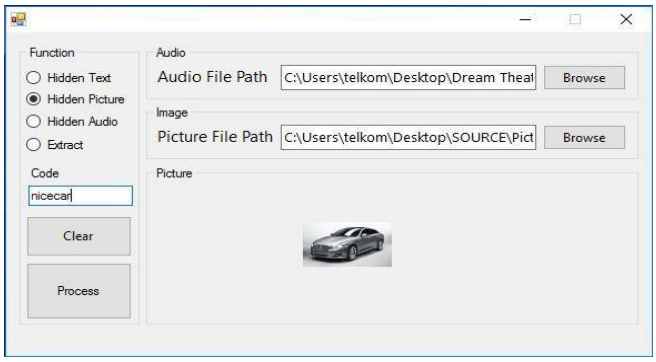

Figure 16. Hidden Picture in Audio Carrier

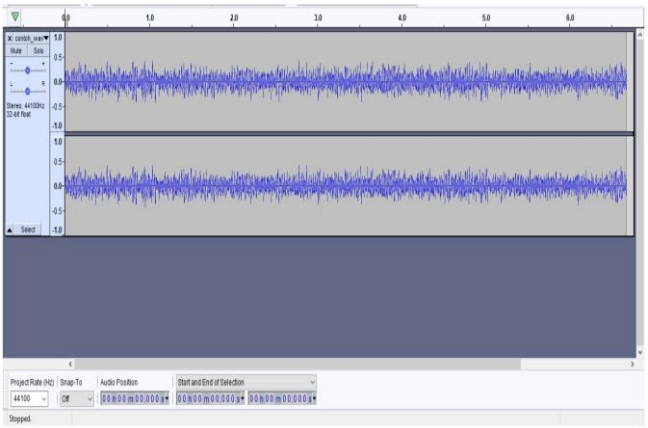

Figure 17. Audio Carrier

When the audio carrier as shown in Figure 17 is inserted with hidden image as shown in Figure 18. The audio result is shown in Figure 19.

Figure 18. Hidden Image

p-ISSN : 2443-2210
e-ISSN : 2443-2229

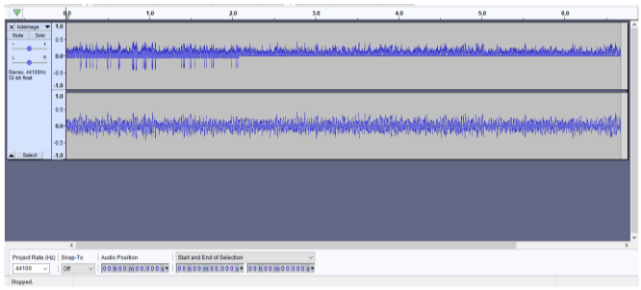

Figure 19. Audio Result after Inserted with Hidden Image

C. Hidden Audio

Hidden audio in an audio carrier can be done by selecting the hidden audio in the main menu. Then, the user need to choose the audio carrier as well as choosing the audio to be hidden as shown in Figure 20.

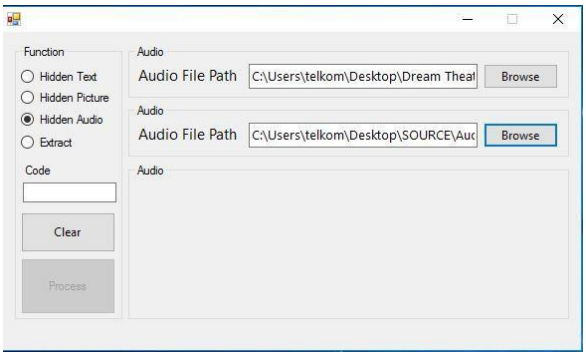

Figure 20. Hidden Audio Interface

If the audio file is too big which might take long time to process hidding the audio then the pop up window will show up as shown in Figure 21.

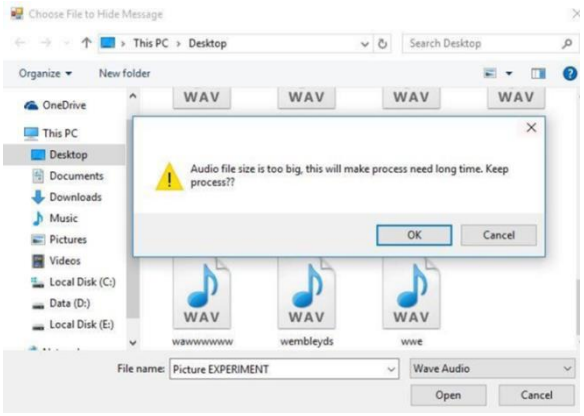

Figure 21. Audio Size Notification

When the carrier audio file (Figure 22) and audio file to be hidden have been selected (Figure 23) , the next step is to enter the secret code, and clicking the process button, the result is shown in Figure 24.

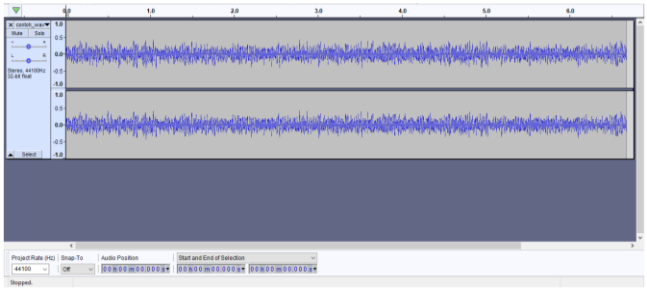

Figure 22. Audio Carrier used to hide the audio

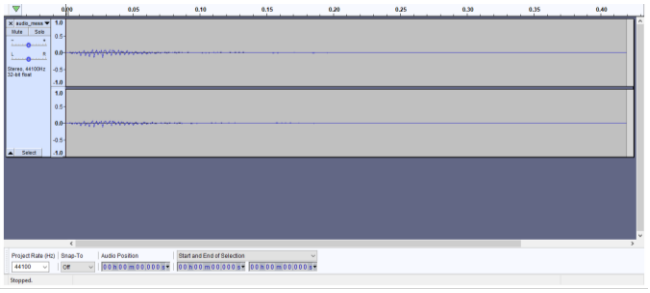

Figure 23. Hidden Audio

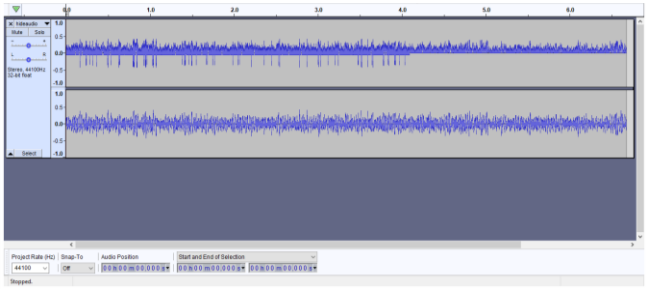

Figure 24. Result of Audio inserted with Hidden Audio

D. Extract File

To extract the file, the user need to choose The Extract option in the main menu. The steps to do are to select an audio file, then enter the secret code, and press the Process button (Shown in Figure 25).

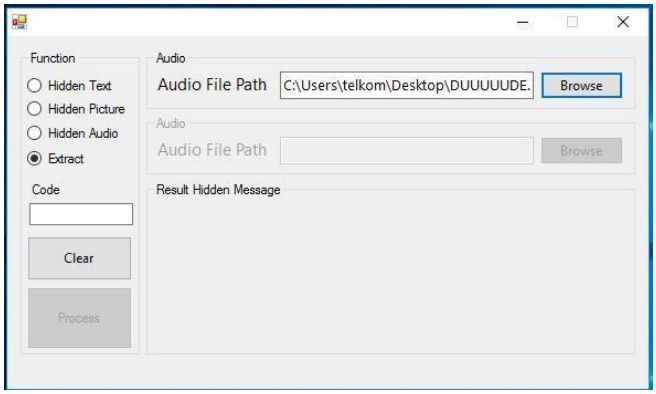

Figure 25. Extract File Interface

If the selected audio file does not have hidden data on it, then when the Process button is pressed, a notification will appear, if the file has no hidden data, as shown in Figure 26.

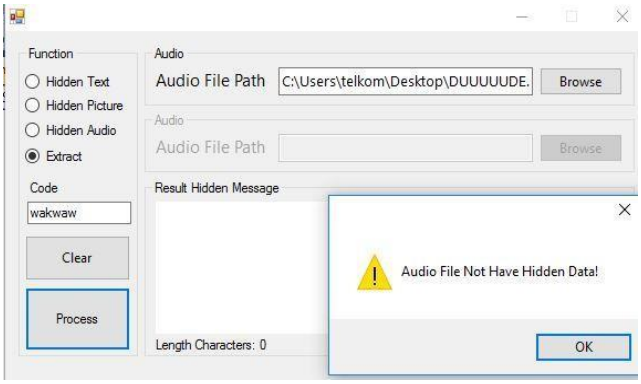

Figure 26. Extrating File Notification

Figure 27 shows the extraction results from the selected audio file and by entering the correct code, the results can be seen in the Result Hidden Message Area, then the extraction results can be saved.

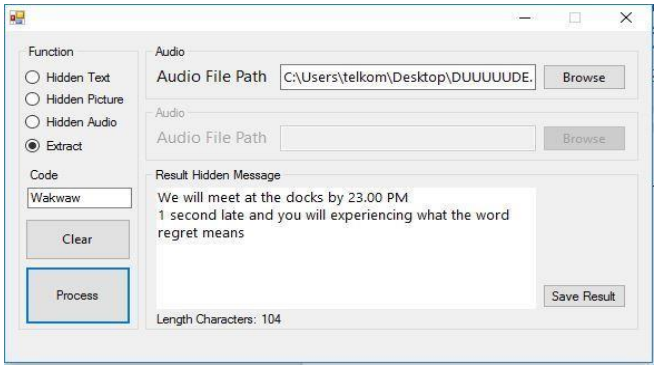

Figure 27. Result of Extracting File

E. Audio Size Evaluation

In this step, TheStego application will be evaluated if the audio size selected is too big. The evaluation can be seen in Table IV.

TABLE IV.

AUDIO SIZE EVALUATION

No.	Scenario	Expected Result	Result
1.	Run the application	Main form will be displayed	As expected
2.	Choose hidden audio button	Column for browsing the audio will be displayed	As expected
3	Choose the audio carrier	Application will save the file path for the selected audio carrier	As expected
5	Browse the audio with big size to be embedded	Application will warn “audio file is too big”	As expected

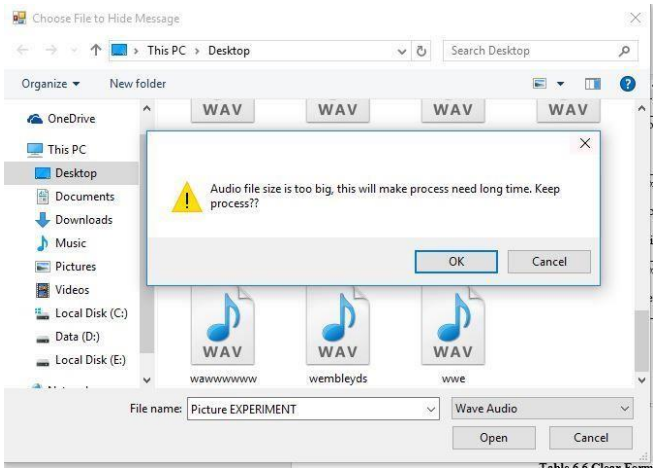

Figure 28. Audio Size Evaluation

Figure 28 shows that the application will send a warning if the selected audio to be embedded have a big size.

p-ISSN : 2443-2210
e-ISSN : 2443-2229

F. Wrong Decryption Code Evaluation

This step shows the process of TheStego application if wrong decryption code is entered by the user when extracting the data. The evaluation can be seen in the Table V.

TABLE V.

WRONG DECRYPTION CODE EVALUATION

No.	Scenario	Expected Result	Result
1.	Run the application	Main form will be displayed	As expected
2.	Choose any type of file to be hidden	Column for browsing the file will be displayed	As expected
3	Choose the audio carrier	Application will save the file path for the selected audio carrier	As expected
5	Click “Browse” button	Application will save the file path for the selected file	As expected
6	Input wrong decryption code	Decryption Code successfully inputted	As expected

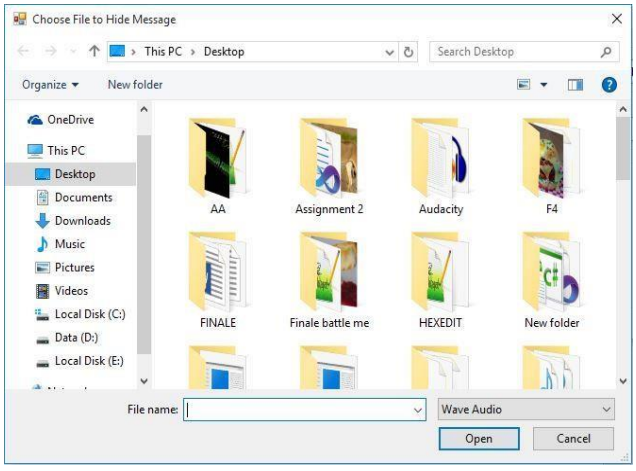

Figure 29. Browse Extract Audio Evaluation

Figure 29 shows us the dialog that pop up when user click browse audio.

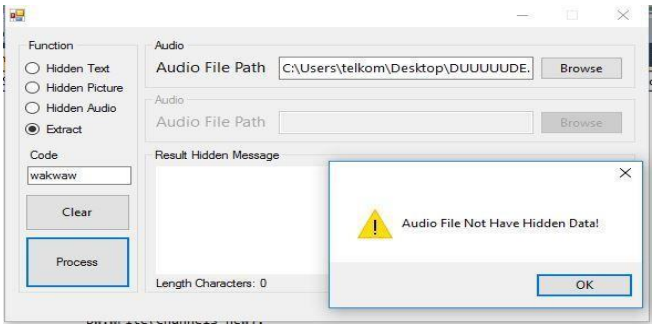

Figure 30. Wrong Code Evaluation

Figure 30 shows that the application show error message if the extraction code is wrong.

V. CONCLUSIONS

There are several conclusions gained from this research:

- TheStego application could hide the data intended into the audio with WAV format
- TheStego application could extract the data that embedded in the audio carrier.
- TheStego could encrypt and decrypt the file using the MD5 method with the inputted keycode by the user.
- TheStego may not have the latest steganography method, but TheStego mobility is high as user no need to install the application.

This application is running as expected but there is some room for improvement for satisfying the technology growth for the data transfer along with its security. Some improvement that could be done is as follows:

- Have multi platforms
  This research only uses windows platforms, in the future it is better if this application will be created into various platforms such as Linux, Mac, android, and IOS. So, all people especially mobile users could also use this application.
- Encryption Method
  The encryption method should be improved with applying another encryption method other than using MD5.
- File format compatibility
  The variety of file format for the carrier or the data that will be hidden should have more varieties and compatible for the application. For example, video format file to be hidden and another common file format.

ACKNOWLEDGMENT

This research received funding from the Ministry of Research, Technology and Higher Education of the Republic of Indonesia, scheme Penelitian Dosen Pemula.

REFERENCES

[1] Rizki, Ramadhan. (2018) CNN Indonesia. [Online]. Available: https://www.cnnindonesia.com/nasional/20180717140856-12-314780/polri-indonesia-tertinggi-kedua-kejahatan-siber-di-dunia.

[2] Abdulzahra, Hayfaa, Ahmad, Robiah and Noor, Norliza Mohd "Combining Cryptography and Steganography for Data Hiding in Images" Applied Computational Science, pp. 128-134, 2014

[3] Poduval, Aditya, et al. "Secure File Storage on Cloud using Hybrid Cryptography", International Journal of Computer Science and Engineering, Vol. 7, 2019

[4] Garg, Nancy and Kaur, Kamalinder. "Hybrid Information Security Model for Cloud Storage Systems using Hybrid Data Security Scheme", Vol. 3, 2016

[5] Rahman, Mohammad Obaidur, et al. "An Approach for Enhancing Security of Cloud Data using Cryptography and Steganography with E-LSB Encoding Techniques" International Journal of Computer Science and Network Security, Vol. 18, pp. 85-93, 2018.

[6] Navita Agarwal, Prachi Agarwal "An Efficient Shuffling Techniques on RGB Pixels for Image Encryption", MIT International Journal of Computer Science & Information Technology, Vol. 3, No. 2, pp. 77-81, 2013

[7] Quist-Aphetsi Kester, MIEEE "Image Encryption based on the RGB Pixel Transposition and Shuffling" International Journal Computer Network and Information Security, No.7 pp. 43-50, 2013

[8] Londhe Swapnali, Jagtap Megha, Shinde Ranjeet, P.P. Belsare and Gavali B. Ashwini "A Cyrptographic Key Generation on a 2D Graphics using RGB Pixel Shuffling and Transposition", Proceedings of the International Conference on Data Engineering and Communication Technology, Advances in Intelligent Systems and Computing 469, Vol. 2, Springer, 2016

[9] Sanjay Kumar Pal, Sumeet Anand,"Cryptography Based on RGB Color Channels using ANNs", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.5, pp.60-69, 2018

[10] Aumreesh Kumar Saxena, Sitesh Sinha, Piyush Shukla," Design and Development of Image Security Technique by Using Cryptography and Steganography: A Combine Approach", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.10, No.4, pp. 13-21, 2018

[11] Hnin Lai Nyo, Aye Wai Oo, "Secure Data Transmission of Video Steganography Using Arnold Scrambling and DWT", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.6, pp.45-53, 2019

[12] Jaeyoung Kim; Hanhoon Park; Jong-Il Park "Image steganography based on block matching in DWT domain", IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Page(s):1 – 4, Italy 2017

[13] M. Saritha; Vishwanath M. Khadabadi; M. Sushravya "Image and text steganography with cryptography using MATLAB" International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES) page(s): 584-587, India-2016.

[14] Nikhil Patel; Shweta Meena "LSB based Image steganography using Dynamic key cryptography", 2016 International Conference on Emerging Trends in Communication Technologies (ETCT), Pages(s): 1- 5,India-2016, 2016

[15] A. Tamimi and A. M. Abdalla, "An Audio Shuffle -Encryption Algorithm", The World Congress on Engineering and Computer Science 2014 WCECS 2014, 22-24 October, 2014, San Francisco, USA, 2014

[16] Xiao Steganography. (2017) [Online]. Available: http://www.softpedia.com/get/Security /Encrypting/Xiao-Steganography.shtm

[17] Quickstego. (2015) [Online]. Available: http://www.quickcrypto.com/free-steganography-software.html

[18] Deep Sound. (2019) [Online]. Available: https://deepsound.soft112.com/