International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

Data Hiding using Cryptography and Image/Audio Steganography

Pooja Paniker[1], Vaidehi Dahare[2], Anand Saurkar[3]

[1,2]*Student, RGCER, Dept. of Computer Science and Engineering, Maharashtra, India*
[3]*Professor, RGCER, Dept. of Computer Science and Engineering, Maharashtra, India*

Abstract - *Data hiding is an important task that has to be taken into account to maintain the integrity and security of the information to be transmitted in addition to avoid the tampering of the data. An adversary is not just modifying someone else's data but to use if for one's own benefit. Data hiding task is performed to protect it from a third party user who may misuse the information. Certain approaches aim to successfully implement the security method of data hiding to secure and protect the data to be transmitted. Cryptography and Steganography are two of the three methods of data hiding. So to provide enhanced data security we have proposed a method that combines the two different data hiding methods in a single system. This combination of two different processes enhances the secrecy of the data by first encrypting the data and then embedding this encrypted data inside an image or an audio file. Thus this paper eventually focuses on ensuring that the data to be transmitted is hidden with double protection.*

Key Words: Cryptography, Image Steganography, Audio Steganography, Encryption, Decryption, LSB, RSA.

1. INTRODUCTION

With the advent of technology and its fast pace development, the security of information or data has been the utmost concern or say the utmost priority. Data security refers to its protection from unauthorized users or hackers and provides high security to prevent the information's retrieval, modification, and misuse. The data needs to be secure to maintain its accessibility only by its authorized personnel and any unofficial user cannot access it by any means. Thus the security of the information is maintained by using data hiding techniques. The various methods of data hiding techniques are Cryptography, Steganography, and Watermarking which provide means for secret communication.

1.1 Cryptography

In Cryptography, the information is protected through the use of codes that will only be decrypted by the person for whom it was intended to be sent. Ciphertext is the result of the encryption process that is performed on the plaintext and can be retrieved back into its original form by performing the decryption process on it.
Cryptographic systems are classified as:

A. Type of Operation on Plaintext

Two kinds of tasks are performed on the plaintext to change it into the ciphertext. The principal activity is that every component in plaintext (i.e., bit, letter) is subbed with each other in the ciphertext. In the second type of activity, each character in plaintext is transposed with each other dependent on a mapping directed by the key. Plaintext characters remain equivalent; however they are simply moved into various positions.

B. The Number of Used Keys

On the off chance that the sender and the recipient utilize one key to encode and unscramble the plaintext, the framework is alluded to a lopsided, single key, mystery key or traditional encryption. Symmetric encryption is genuinely clear and quick. On the off chance that the sender and collector utilize various keys, open key, and private key, to scramble and decode the plaintext separately, the framework is alluded to as asymmetric, two – key, or public-key encryption.

C. How The Plain Text is processed

Block figure works on fixed-length gatherings of bits, called squares, and creates a yield hinder for each info block. A stream figure works on each plaintext component constantly, and produces each component in turn, as it comes.

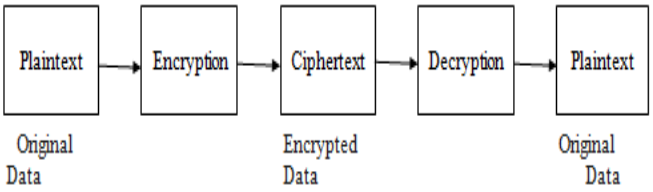

Fig -1: Cryptography Steps

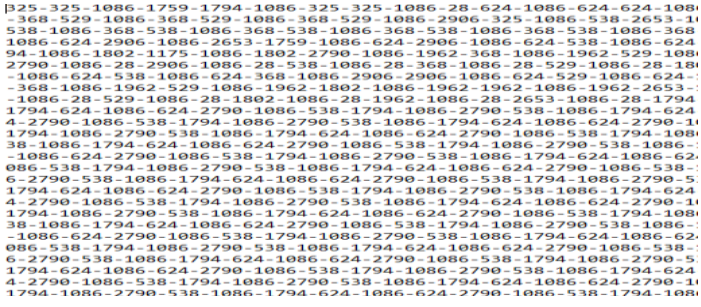

Fig -2: Snapshot of Cipher text

1.2 Steganography

Image Steganography: In Image Steganography the data is hidden within an image. The main aim of Image Steganography is to hide the information or data in an image file so that the unauthorized user will not notice the existence of the information and will only be able to see the ordinary image. The image which is selected for this purpose is called the "cover-image" and the image which is obtained after performing Steganography is known as the "stego-image".

Image Steganography consists of two process, embedding and extraction. In the embedding process, the data is hidden within a cover-medium which results in stego-image as output. The extraction process is inverse of the embedding process; here the embedded data is retrieved from the cover-image.

Audio Steganography: In Audio Steganography the data is hidden within an audio. The main objective of Audio Steganography is to conceal the data inside an audio file. The audio selected in audio steganography is known as "cover-audio" and the audio obtained after performing Steganography is known as the "stego-audio".

Audio Steganography consists of two process, embedding and extraction. In the embedding process, the data is hidden within a cover-medium which results in stego-audio as output. The extraction process is inverse of the embedding process; here the embedded data is retrieved from the cover-audio.

A digital audio is a continuous signal rather a discrete signal as in a traditional analog signal. Eventually by sampling a continuous analog signal a particular discrete signal can be created. The below figure, gives a glimpse of a continuous analog sound wave that is being sampled in order to produce a digital audio.

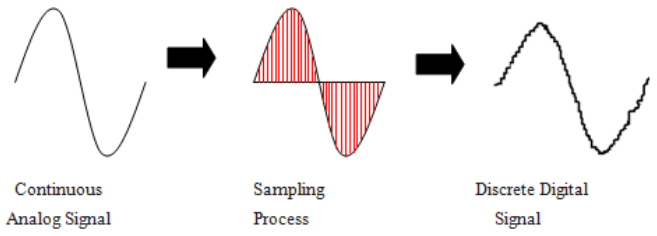

Fig -3: Continuous analog sound wave sampled to produce a digital audio

The major difference between Cryptography and Steganography is their process of hiding the data. With these two different methods, one can combine them to increase the secrecy of the data to be hidden.

2. PROPOSED METHOD

The proposed approach is the merging of two separate algorithms RSA and LSB. There are certain steps in between hiding the data and getting back the original data. The first step of the system is to ensure the format of the data to be hidden is in .jpg format. Then after converting the data in a .jpg format, the resulting .jpg file is encrypted using RSA algorithm of Cryptography to perform encryption on the plaintext to transform it into a ciphertext. The second step is to embed this ciphertext (encrypted data) in an image/audio using the LSB algorithm of Image/Audio Steganography. The third step is to retrieve the embedded ciphertext (encrypted data) from the image/audio file selected during the embedding process. The final step is to decrypt the retrieved data which is in the form of ciphertext into plaintext i.e., in its original form using the decryption method of RSA algorithm.

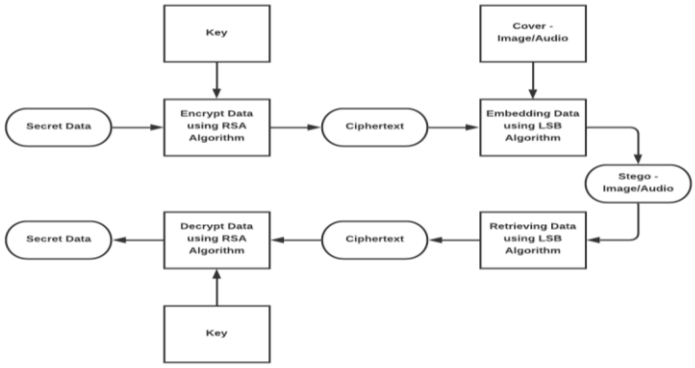

Fig -4: Flow Diagram of whole system

2.1 The RSA Algorithm

It is a cryptographic technique to encrypt and decrypt the messages. RSA is an asymmetric type of algorithm which means that there are two different types of keys. In this cryptographic algorithm, both the public key and the private key can be used to encrypt the message, whereas the other key rather than the one used to encrypt the message is used for decryption. This algorithm provides the following advantages: Integrity, Authenticity, Confidentiality, and Non-Repudiation of the data to be transmitted.

Algorithm:

Step 1: Choose two prime numbers
p and q such that, both are prime numbers and $p \neq q$.

Step 2: calculate the value of 'n' and '$\phi(n)$'
$n = p * q$

$\phi(n) = (p-1) * (q-1)$

Step 3: Find the random value of 'e' (pubic key)
Choose 'e' such that 'e' should be co-prime i.e., it should not be multiple by the factors of ϕ and also should not be divisible by it.

Gcd (ϕ(n)), e) = 1; 1 < e < ϕ(n)

Step 4: Compute the value of 'd' (private key)

- Find the value of 'd' such that 'ϕ(n)' divided (e*d - 1)
- d = e^{-1}(mod ϕ(n))

de % ϕ(n) = 1
de = 1 + N * ϕ(n)
d = $\frac{1+N*\phi(n)}{e}$; where N is such a number

that gives an integer solution for 'd'.

Step 5: Public Key, PU = { e, n }

Private Key, PR= { d, n }

Step 6: For Encryption and Decryption,

1. Encryption or Ciphertext, C = M^e mod n
2. Decryption or Plaintext, M = C^d mod n

This algorithm is used as the first step in the proposed system to change the original data into a cryptic format.

2.2 Least Significant Bit (LSB) insertion Method

Image Steganography: In this technique, the bits of the image are replaced by the bits of the data to be embedded or hidden. The secret message can be inserted inside the image by altering only the first rightmost bit of the image. While using this algorithm it should be noted that, when we apply this algorithm to each byte of the 24-bit image, only three bits are capable to be embedded in each pixel of the image.

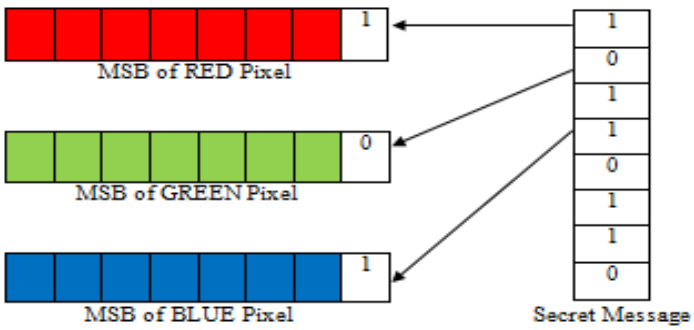

Fig -5: Image Steganography

Algorithm: For Image Steganography

1. Embedding Algorithm

Step 1: Extract pixels of the image where the data has to be embedded.

Step 2: Extract the entire characters of the secret message that has to be embedded; these characters are stored in a place called the Character-Array.

Step 3: Extract the entire characters from the Stego-Key; these characters are stored in a place called Key-Array.

Step 4: Choose the first pixel of the cover image and choose the characters that were stored in the Key-Array and put it in the pixel. In case there are more numbers of characters then, place the rest of the characters in the next pixel.

Step 5: Put some terminating symbols that will indicate the end of the key.

Step 6: Put characters of the Character-Array in each pixel of the image by replacing it.

Step 7: Repeat the above step until all the characters are embedded in the image.

Step 8: Repeat the placing of terminating symbols, this time it indicates the end of the data.

Step 9: The obtained image after performing the above steps will hide/ embedded all the characters inside it.

2. Extraction Algorithm

Step 1: Consider the following three arrays: Pixel-Array, Character-Array, and Key-Array.

Step 2: Extract the entire pixel of the cover image and then store them in the array called Pixel-Array.

Step 3: Scan the pixels from the beginning and extract Key-Characters from the first and second pixels and then store them in the Key-Array. Do this step until the terminating symbol.

Step 4: If the key that is extracted matches with the Key that was entered by the receiver, then go in the next step, otherwise, terminate the program with a message saying "Key entered is wrong".

Step 5: If the entered key is correct, then re-scan the next pixels and extract the message characters from the beginning pixels and put it in the Character-Array. Does this step until a terminating symbol id found. Otherwise, go to the next step.

Step 6: Secret message extraction from Character-Array.

Audio Steganography: In the technique, a particular data is hidden inside a digital audio file. To do so it is first important to understand a continuous analog sound wave that eventually results in a digital audio. One even has to consider the sinusoidal nature of a sound wave. Take a note that a digital signal is stored as a sequence of 0's and 1's in a computer. By slightly changing/altering the binary sequence of the selected audio file, a data can be embedded inside the audio.

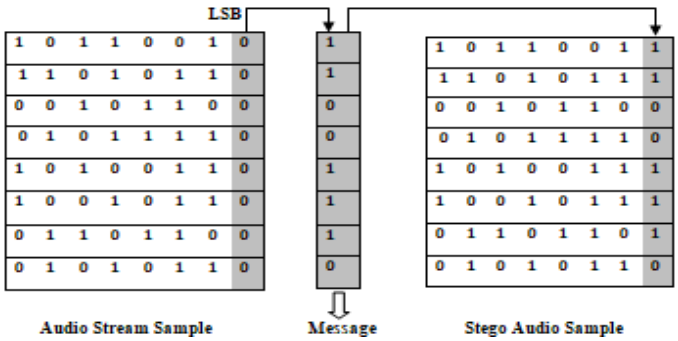

Fig -6: Audio Steganography

Algorithm: For Audio Steganography

1. **Embedding Algorithm**

Step 1: Select an audio file that will act as a cover medium to hide a particular data inside it.

Step 2: Select data/ information that has to embed in the audio file. Save the length of the file into binary stream.

Step 3: Extract frequency values of the audio. Here frequency value is nothing but the binary sequence of the audio file.

Step 4: The proposed algorithm reads the frequency values (binary stream) of the audio file in form of Bit pattern.

Step 5: A key is used to encode the information bit by bit or even byte by byte inside the stream of bits/bytes of the audio.

Step 6: Replace the binary stream of the message with the least significant bit of the audio file. In this step the LSB bit from the audio is replaced by the LSB bit from characters in the message.

Step 7: Repeat the above step until all the characters are embedded in the audio.

2. **Extraction Algorithm**

Step 1: Read the entire bit stream of the audio file.

Step 2: Use the key stream in order to locate/ find the right samples.

Step 3: Read the very last bit of the stego-audio and shift it into the current byte of the message.

Step 4: When the byte is completed, we then write it into the message stream and then continue with the next one.

Step 5: Repeat the above steps until all the message stream is extracted.

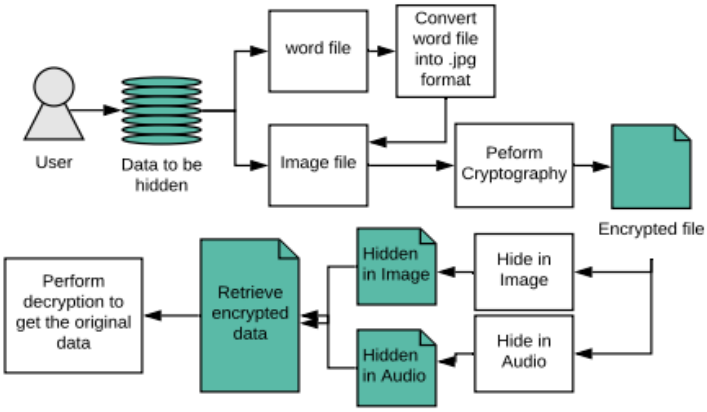

Fig -7: System Architecture proposed approach

3. RESULT AND DATA ANALYSIS

To verify whether our proposed system provides better output or not, the following comparison has been done on the before and after properties of the data gone through the suggested method. As the data to be hidden in certain cases might be of greater importance thus it is essential to produce an almost accurate output.

Table 1: Properties of the Word file before converting into .jpg format

Properties	Values
Name:	extralines.doc
Type of file:	Microsoft Office Word Document (.docx)
Opens With:	Microsoft Office Word
Size:	11.5 KB (11,861 bytes)

Table 2: Properties of the Word file after converting into .jpg format

Properties	Values
Name:	Extralines
Type of file:	JPG File (.jpg)
Opens With:	Photos
Size:	50.6 KB (51,892 bytes)
Dimensions (width*height):	714 * 924
Bit Depth:	24

Table 3: Properties of the resulting text file after performing cryptography in the converted image

Properties	Values
Name:	Extralinescrypt
Type of file:	Text Document (.txt)
Opens With:	Notepad
Size:	563 KB (5,77,158 bytes)

Table 4: Properties of the Image before embedding the Encrypted Data

Properties	Values
Name:	Sampleimage
Type of file:	BMP File (.bmp)
Opens with:	Photos
Size:	3.25 MB (34,11,338 bytes)
Dimensions (width*height):	1066 * 800
Bit Depth:	24

Table 5: Properties of the Image after embedding the Encrypted Data

Properties	Values
Name:	Stegoimage
Type of file:	BMP File (.bmp)
Opens with:	Photos
Size:	1.39 MB (14,67,505 bytes)
Dimensions (width*height):	1066 * 800
Bit Depth:	32

Table 6: Properties of the retrieved crypt data from the stego-image

Properties	Values
Name:	Extralinescrypt
Type of file:	Text Document (.txt)
Opens With:	Notepad
Size:	563 KB (5,77,158 bytes)

Table 7: Properties of the Audio before embedding the Encrypted Data

Properties	Values
Name:	file_example_WAV_2MG
Type of file:	VLC (.wav)
Opens With:	VLC
Size:	2.04 MB (21,46,166 bytes)

Table 8: Properties of the Audio after embedding the Encrypted Data

Properties	Values
Name:	Stegaudi
Type of file:	VLC (.wav)
Opens With:	VLC
Size:	722 KB (7,39,502 bytes)

Table 9: Properties of the retrieved crypt data from the stego-audio

Properties	Values
Name:	extralinescrypt
Type of file:	Text Document (.txt)
Opens With:	Notepad
Size:	563 KB (5,77,158 bytes)

Table 4.1.10: Properties of the decrypted ciphertext retrieved from stego-image/ audio steganography

Properties	Values
Name:	extra lines
Type of file:	JPG File (.jpg)
Opens With:	Photos
Size:	50.6 KB (51,892 bytes)
Dimensions (width*height):	714 * 924
Bit Depth:	24
Image resolution:	96 dpi * 96 dpi

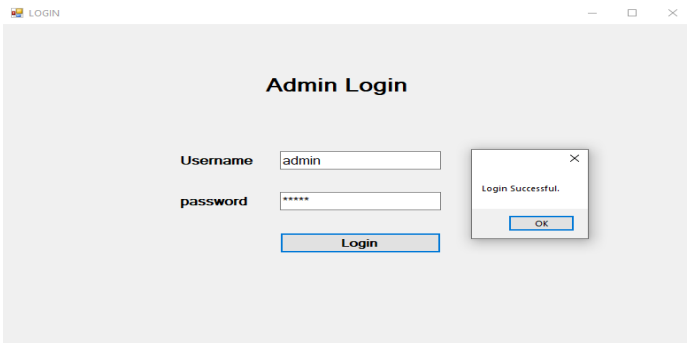

Fig -8: Login Page.

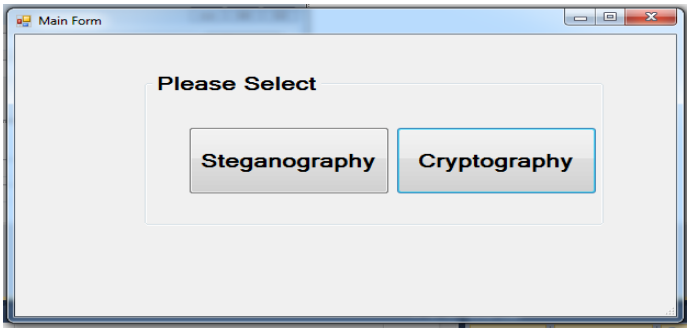

Fig -9: Choose Between Steganography and Cryptography

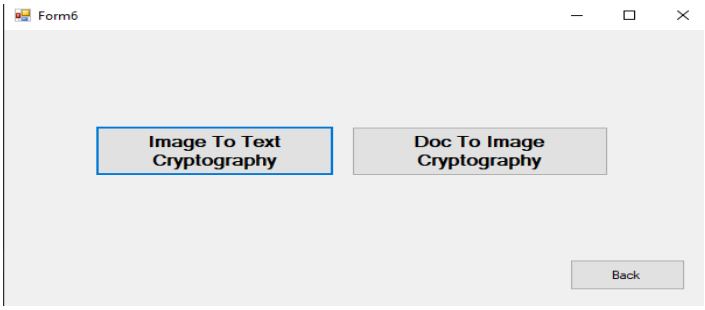

Fig -10: Choose Between options to encrypt a word file or an image file

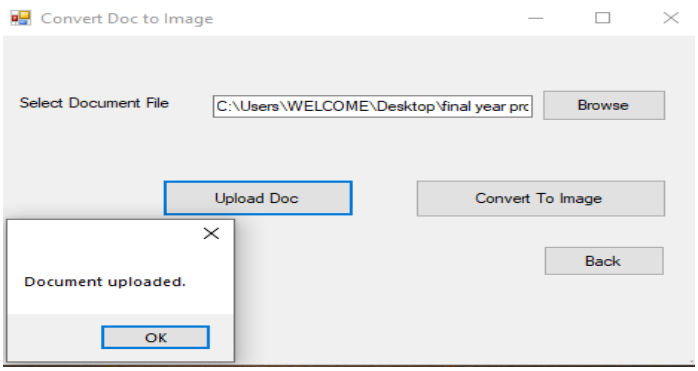

Fig -11: Converting of word file to .jpg format

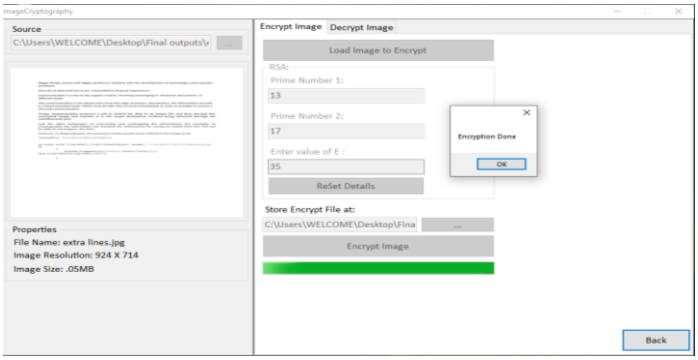

Fig -12: Load Image to Encrypt

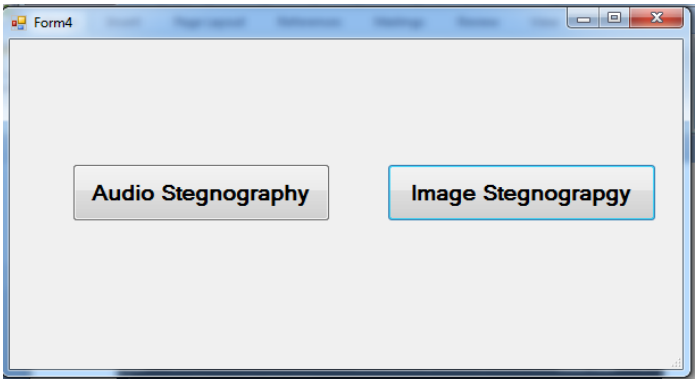

Fig -13: Choose Between Audio Steganography and Image Steganography.

Fig -14: Load encrypted file to hide inside another image

Fig -15: Retrieve Encrypted data from stego-image

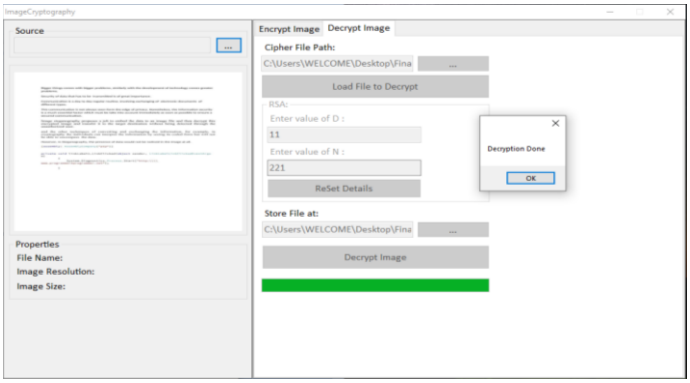

Fig -16: Decrypt the Encrypted Image

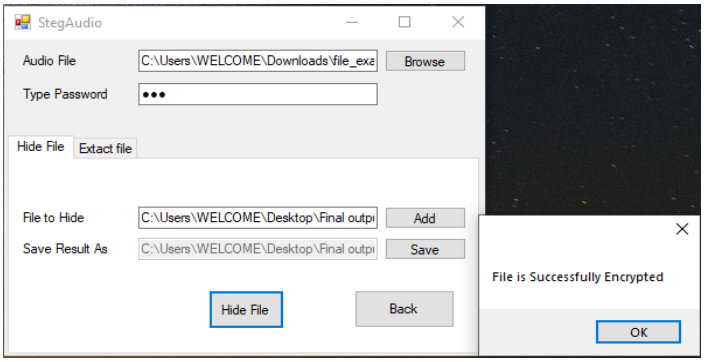

Fig -17: Hide Encrypted data in the chosen audio

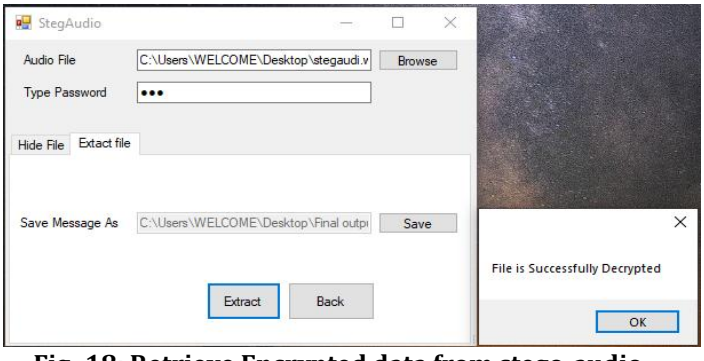

Fig -18: Retrieve Encrypted data from stego-audio

4. CONCLUSIONS

This paper provides a novel approach for implementing the image and audio steganography with separate encryption and decryption of data as done in cryptography and then embedding this encrypted data into the image or audio so that it will be invisible to the unauthorized users with extra privacy by fist encrypting the data. Hence a new approach of combining the two techniques of data hiding was introduced.

The outcome of the evaluations made from this system proves that it has the potential to improve upon the existing methods. To sum up, the overall contribution of this thesis lies in the development of a new approach combining cryptography and steganography is shown to be both robust and imperceptible and thus we conclude that our proposed system can be used to secure and maintain the privacy of the data that has to be transmitted.

5. FUTURE WORK

Performing Cryptography on a Video File:

We are in a working progress to implement the concept of cryptography on a video file of type: MP4, MOV and WML. This will eventually help the user to crypt a video file that the user intends to securely transmit.

Performing Cryptography on a Audio File:

We are in a working progress to implement the concept of cryptography on an audio file of type: MP3 and WAV. This will help the user to encrypt an audio file that the user wants to transmit securely.

Video Steganography:

We are planning to upgrade are application in future by enabling the concept of video Steganography. By this the user will not only be able to embed the crypt data inside an image or audio but also inside a video file.

Combining Watermarking:
Though we have combined two out of three concepts of data hiding process but we are also looking forward to include the conception of Watermarking i.e., the third type of data hiding method in which the digital information is hidden inside a carrier signal. This addition of watermarking will works in such a way that it will verify the authenticity plus the integrity of the carrier signal i.e., it will display the identity of its authorized user or say owner.

REFERENCES

[1] Rituparna Halder, Susmit Sengupta, Sudipta Ghosh, Debashish Kundu, “A Secure Image Steganography Based On RSA Algorithm And Hash-LSB Technique”, IOSR-JCE, Volume 18, Issue 1, Ver. Iv Jan – Feb. 2016

[2] Mehdi Hussain And Mureed Hussain, "A Survey Of Image Steganography Techniques", International Journal Of Advanced Science And Technology, Vol. 54, May 2013

[3] Marwa E. Saleh, Abdelmgeid A. Aly, Fatma A. Omara, "Data Security Using Cryptography And Steganography Techniques", Ijacsa, Vol. 7, No. 6, 2016

[4] Sahil Lotlikar, Ashish Gupta, Jayesh Thorat, Sandhya Kadam, "Image Steganography And Cryptography Using Three Level Password Security", IJRASET, VOLUME 5 ISSUE Iv, APRIL 2017

[5] Ahmed Al-Shabby, Talal Alkharobi, "Cryptography And Steganography: New Approach", TNC, VOLUME 5, NO. 6, ISSN: 2054 -7420, Year: DECEMBER 2017

[6] Hayfaa Abdulzahra, Robiah Ahmad and Norliza Mohd Noor, "COMBINING CRYPTOGRAPHY AND STEGANOGRAPHY FOR DATA HIDING IN IMAGES", ISBN: 978-960-474-368-1

[7] Radha S. Phadte and Rachel Dhanaraj, “Enhanced Security with Steganography and Cryptography”, IOSR Journal of Computer Engineering, Year: 2017

[8] Mustafa Sabah Tah, Mohd Shafry Mohd Rahim, Sameer Abdul Sattar lafta, Mohammed Mahdi Hashim, Hassanain Mahdi Alzuabidi, "Combination of Steganography and Cryptography: A short Survey", IOP Conference Series: Materials Science and Engineering, Year: 2019

[9] Vishnu S Babu and Prof. Helen K J, “A Study on Combined Cryptography and Steganography”, International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), Year: May 2015, Volume 2, Issue 5, PP 45-49

[10] Sharmin Sultana, Afrida Khanam, Md. Rashedul Islam, Adiba Mahjabin Nitu, Md.Palash Uddin, Masud Ibn Afjal and Md. Fazle Rabbi, "A Modified Filtering Approach of LSB Image SteganographyUsing Stream Builder along with AES Encryption”, Year: 2018, Volume 1, Issue 2

[11] Pashang Engineer, Priyanka A. Bansode, Shreya Vitthalrao Surnar, Prathmesh N. Gunjgur, “Secured Crypto-Stegano Communication”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 8, Issue 4, April 2019

[12] Vipul Sharma and Madhusudan, “Two New Approaches for Image Steganography Using Cryptography”, Year: 2015

[13] Varsha1, Dr. Rajender Singh Chhillar2, "Data Hiding Using Steganography and Cryptography", International Journal of Computer Science and Mobile Computing, Vol. 4, Issue. 4, April 2015, pg.802 – 805