OPEN ACCESS

Middle East Research Journal of Engineering and Technology
ISSN: **2789-7737** (Print) **2958-2059** (Online)
Frequency: Bi-Monthly
DOI: 10.36348/merjet.2022.v02i02.001

KUWAIT SCHOLARS PUBLISHER
Website: http://www.kspublisher.com/
Email: office.kspublisher@gmail.com

Secure Data Encryption and Decryption Using Social Media

Arun Agarwal[1*], Avinash Gourav[2], Kabita Agarwal[3], Devasis Pradhan[4]

[1]Department of Electronics and Communication Engineering, Institute of Technical Education & Research, Siksha „O" Anusandhan Deemed to be University, Khandagiri Square, Bhubaneswar-751030, Odisha, India

[2]Application Developer,Oracle Financial Services Software Ltd,Oracle - Bagmane Laurel, Krishnappa Garden, C V Raman Nagar, Bengaluru, Karnataka 560093, India

[3]Department of Electronics and Telecommunication Engineering, CV Raman College of Engineering, Bhubaneswar-752054, Odisha, India

[4]Assistant Professor, Department of Electronics & Communication Engineering, Acharya Institute of Technology, Bangalore -560107, Karnataka, India

ABSTRACT: The objective this work is to design a secure data transmission process using Social Networks. Security of information in a Personal computer is expected to shield basic information and data from different parties. Now days millions of the people are using messengers and other data transferring apps which can be easily hacked. One way of our objective is to protect data by applying the science of steganography. In this paper we propose an advance arrangement of encoding information that combines the highlights of steganography alongside image and sound information hiding. This system will be more secure than different methods visual steganography is one of the safe types of steganography accessible today. It is most usually executed in image files. In this work the secret message is encrypted before the real procedure begins the hidden message is encoded utilizing LSB strategy and secret key is utilized for installing and extraction of document. This encryption technique is basic, productive and of symmetric sort where just receiver and sender knows the secret key. As similar as inserting text inside an audio and here also after embedding our ear cannot be able to find the difference in both the audio.

Keywords: Data transmission, secure, steganography, encoding, encryption, decryption.

REVIEW PAPER

***Corresponding Author:**
Arun Agarwal
Department of Electronics and Communication Engineering, Institute of Technical Education & Research, Siksha „O" Anusandhan Deemed to be University, India.

How to cite this paper:
Arun Agarwal *et al.;* "Green WPC: Energy Harvesting in Smart Cities". Middle East Res J. Eng. Technol, 2022 Nov-Dec 2(2): 13-23.

Article History:
| Submit: 12.09.2022 |
| Accepted: 20.11.2022 |
| Published: 30.11.2022 |

1. INTRODUCTION

1.1. Motivation

In this world a millions of messages are transferred in a minutes, which can easily hacked by anyone one, there is no security for our important data"s. So to overcome that we are using steganography process. In which we can securely transfer the data with the help of a host that is a picture. We got the idea of using steganography to distract the attention of the hacker because when the hacker will be desperately in the search of any text or doc file we can silently hide the text or audio file embedded with the cipher documents. In this manner, we can complete our task of transmission of data securely.

1.2. Applicability

Steganography is applicable to the following areas:-

Protection of data loss:-

We take the advantage of the delicacy of the embedded data in this application. No one can copy, convert, nor interfere such certificate data. If copied, converted, or interfered then it will be easily detected by the extraction program.

Access control systems for digital contain distribution:-

Here embedded data is "hidden", however it is "clarified" to promote the substance. Today, computerized content are getting increasingly more generally dispersed over web than previously. On the off chance that you have some important substance, which you think it is distributable on the off chance that somebody actually needs it and in the event that it is conceivable to transfer that content on web in some believer way. On the off chance that you can issue an extraordinary access key to extricate the substance specifically, we will be glad about it. A steganography procedure can help understand this kind of framework.

2. Literature Survey

This article will examine several early uses of steganography as well as the general guidelines that guide its application. We will at that point take a gander at why it has turned out to be such a vital issue as of late. There will at that point be a talk of some particular systems for concealing data in an assortment of documents and the assaults that might be utilized to sidestep steganography. By exploiting human recognition it is conceivable to implant information inside a document. For instance, with sound records recurrence concealing happens when two tones with comparative frequencies are played in the meantime. The audience just hears the more intense tone while the calmer one is veiled. So also, fleeting concealing happens when a low-level flag happens preceding or after a more grounded one as it requires us investment to change in accordance with the conference the new recurrence. In this study, a variety of strategies are used and are constantly being created, and methods for finding concealed signals are also developing swiftly. Since detection will never guarantee that all hidden information will be found, it will be used in combination with strategies for defeating steganography to reduce the likelihood that secret communication will occur. As steganography becomes much more prevalent in computing, there are problems that need to be fixed. There are many distinct techniques, each with their own benefits and drawbacks.

To address this, benchmarking should be used more frequently to assess methodologies, and a more uniform notion of robustness is needed. New methods & guidelines for watermarking are likely to develop as a result of the use of digital media. In the future, we'll use video steganography as well.

The idea of concealing messages and information inside of other pieces of information can be useful in many real-world applications, along with encryption and a few other code-writing approaches, according to this study's author, who also conducted a review on audio steganography. A novel area of expertise in covert communication through insecure channels is data concealment. The most common multimedia components employed in modern information-hiding techniques are audio files. Due to its high rate of data transmission and elevated position relative to the ground, it can produce a suitable hiding standard. This led to the wrapping up of certain fundamental ideas regarding audio steganography, HAS, Phase Coding, Least Significant Bit (LSB) Coding, Echo data concealing, and Spread Spectrum (SS). Two well-known methods of embedding MP3 steganography were provided before and after compression. The steganography of audio data has been applied to a variety of formats, including MP3. There are numerous methods for incorporating data into digital audio.3. Design Scheme

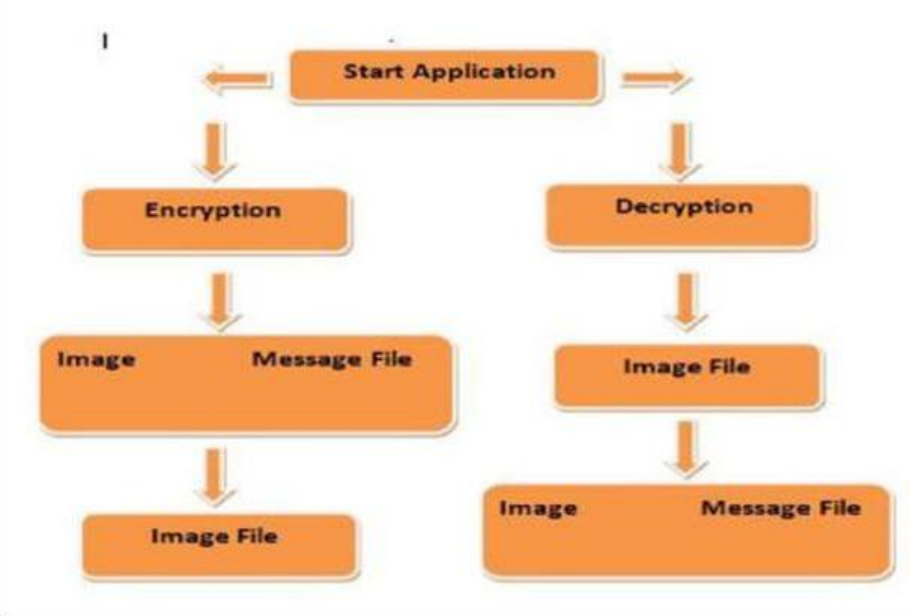
3.1. System Design

Encryption Phase:-

Before adding the data into a picture, the user can construct the message to encrypt the data using the secret keys. According to our theory, the suggested plan encrypts sensitive data using LSB calculations. This method provides stronger security to protect the data user from unauthorized access over a system, making it extremely challenging to recover the data without any of the beneficiary key. After converting each letter into an ASCII code and converting the plain image into a stego picture using LSB computation, the ASCII codes were then converted into a series of double codes to provide greater protection. This suggested method is used to stop the intruder from obtaining the real data when they attempt to retrieve the data. With hardly no bending of the original image, the encrypted data will be incorporated within it.

Encrypted Message Embedding Phase:-

We have suggested a method for embedding an encrypted message into the image after encryption of the secret message. The Least Significant Bit approach is used in this process to replace the Least Significant Bit. The most common steganography technique for inserting data into an image file is called LSB. This technique has been used to convey the image to the designated recipient while concealing the encrypted message within the image. Steganography and cryptography strategies have been suggested in this research to improve security and shield data from hackers by utilizing many layers of security measures. Because some users desire to protect sensitive information from third parties when transmitting data over an open channel, the combination of these two methods will increase the security of data embedding. Early on in the process, we encrypt the message to be included in the cover image, making it challenging for anyone to access it without the recipient's private key. The places were chosen using a hash function, and the suggested method embeds 8 bits of hidden data at a time in the RGB (Red, Green, and Blue) pixel values in the orders of 3, 3, and 2 respectively. Three bits are embedded in the LSB of the Red pixel, three bits in the LSB of the Blue pixel, three bits in the LSB of the Green pixel, and two bits in the Red pixel, according to the procedures we used to embed the secret data into the image.



Decoding Phase:-

The capacity was once again used in a similar way during the decode step to identify the locations of the LSB's where the information bits had already been installed. As the bits are inserted, they are separated from the spot where it had been specified. At the conclusion of this phase, we will obtain the hidden message in double structure, which will then be translated once more into ASCII code structure. The secret message will then be decoded by the recipient.

3.2. Architecture

Least Significant Bit is used in the suggested information steganography techniques to conceal a secret message in image documents (bmp). The system was developed using Windows 10 and tested at the Faculty of Electronics and Communication Engineering Department of the Institute of Technical Education & Research. Because the Graphic User Interface (GUI) is user-friendly, this system can be used by individuals who are not familiar with C programming.

3.3. Component Design

We have used three phases to complete the process of steganography:

1. Encryption phase
2. Embedded phase
3. Decryption phase

As explained above, every steganography consists of 3 phases:

1. Cover Image
2. Message Image
3. Resulting Steganographic Image

We have implemented LSB substitution technique here, and MATLAB is used for the coding purpose.LSB Technique used here, is a best and suitable approach to embed information in a cover file.

The steps which are used for LSB technique are:

1. First we have to convert the hidden message.
2. First read the image only.
3. The image is then converted from decimal to binary.
4. The bytes to be hidden are broken into bits.
5. The first 8 byte of original data are taken from the cover image.
6. The least significant bit are replaced bit by one bit of the data to be hidden.

3.4. Implementation

Embedding proposed algorithm

Stage One: Take encrypted the message
StageTwo: Choose the cover image “f15sm.bmp”
Stage Three: Take four LSB bits of each RGB pixels (Red, Green, and Blue) of the cover image.
Stage Four: Insert eight bits of the encode message into four bits of LSB of RGB pixels of cover picture in the sequence of three, three, and two individually.

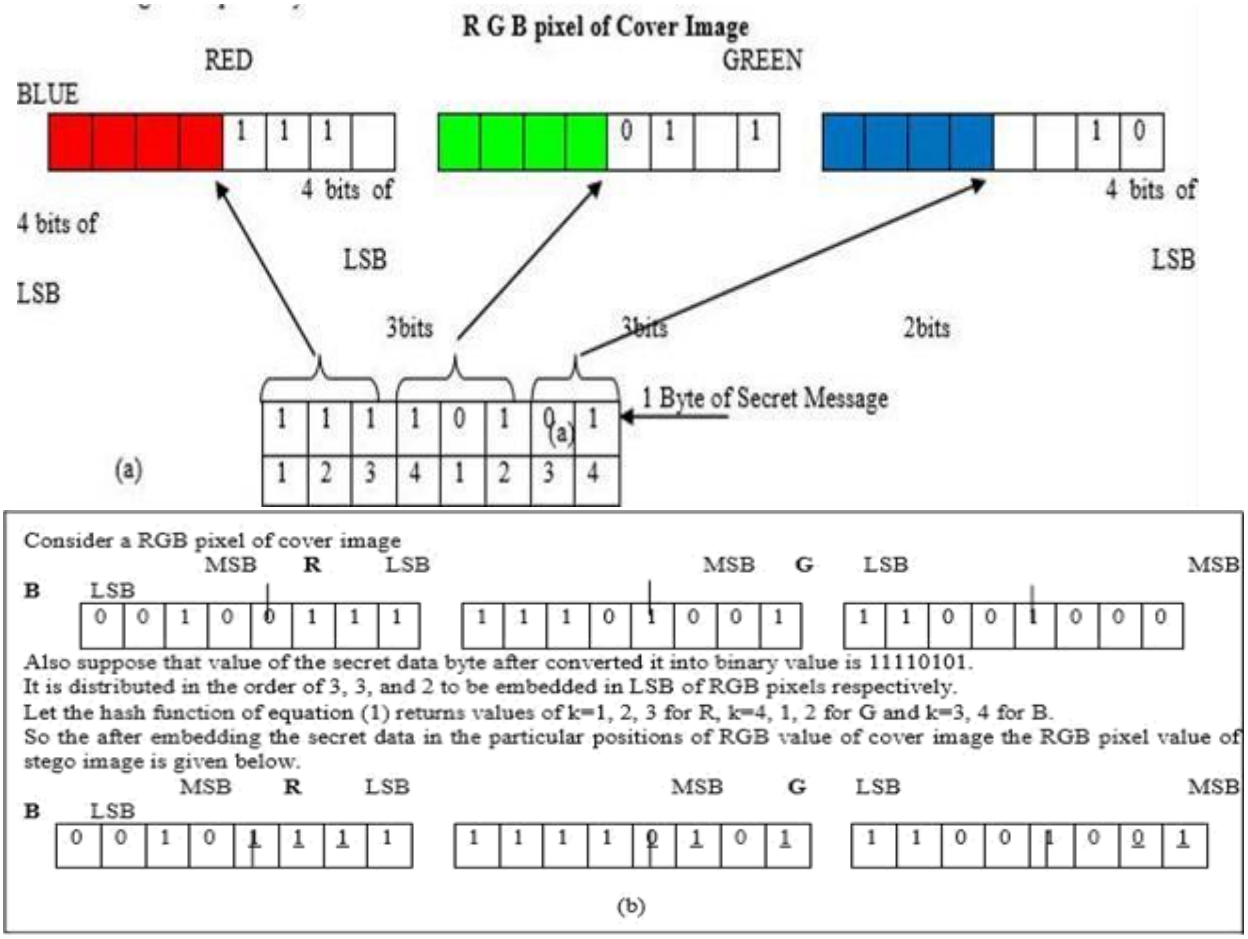


Figure (a) & (b): To find LSB of RGB pixels value

4. Testing, Analysis, and Evaluation

4.1 Image Steganography

While running the MATLAB code with the help of graphical user interphase it will take you to a module based on LSB steganography. Where you can command to encrypt or decrypt the data.

First of all we have to encode the data. For this we have to click the encode button then the following interface will appear with the help of which we can encrypt our data.

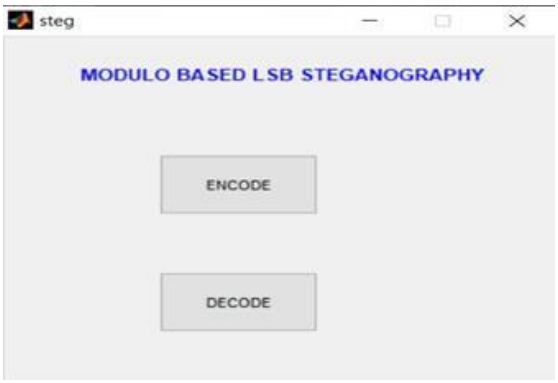


Fig-1: Module based LSB Steganography

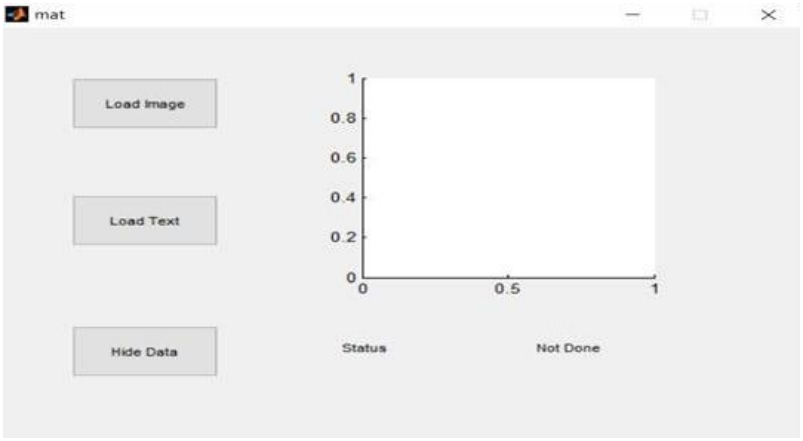


Fig-2: Command to load image

For encryption we have to load a image by clicking the load button. After that we have to choose a picture from our gallery in which we have to encrypt the data. As we are choosing the f15sm.bmp file.

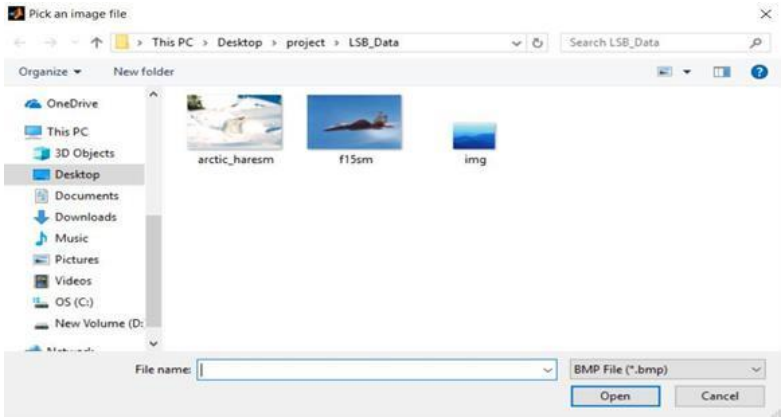


Fig-3: Shows which picture to choose

After the picture is loaded, we have to load the text whatever you want to send to an another party. For that we have to choose the file from our pc in which the text message are written.

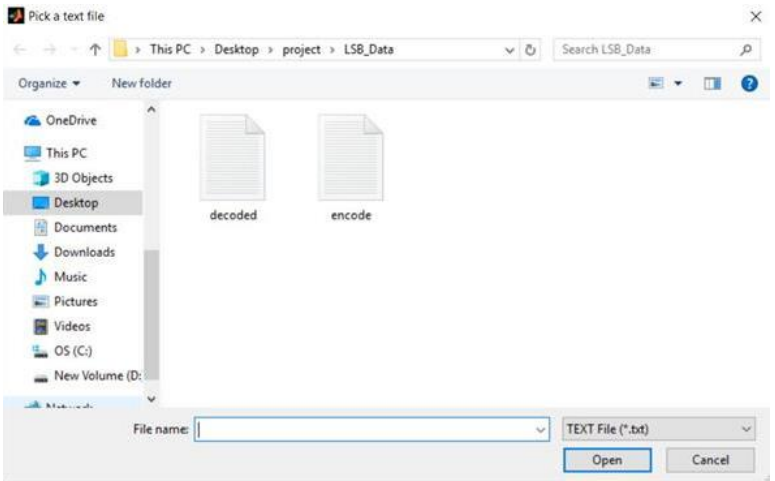


Fig-4: To select the encode file

The text are loaded. After that we have to click the hide button given in the graphical user interface to encrypt the data inside the picture. Following figure shows that the Image with encrypted data. Hence the encryption process is done successfully.

Fig-5: Shows the data is encrypted in the picture

After the encryption process we can send that picture through any Social networking sites to the other party. To see what the text are encrypted in that picture the party should decrypt the picture by running the code. Then the following graphical user interface will appear again.

Fig-6: Module based LSB steganography to decode

After pressing the decode button, Then interface will ask you to choose which picture you want to decrypt as can be seen by the following figure.

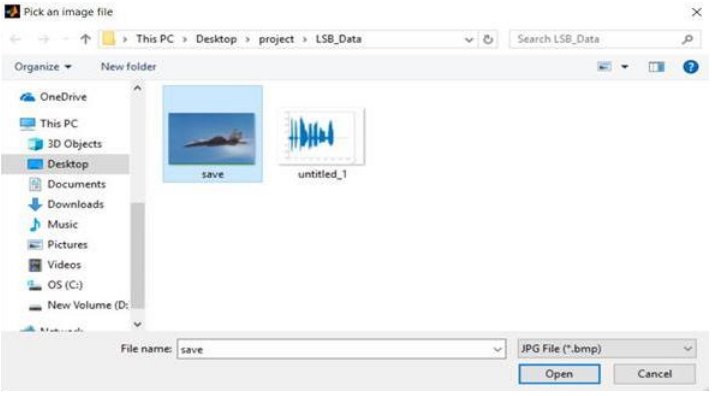


Fig-7: Shows which picture to decrypt

After the picture is chosen the interface will automatically decode it and will say decoded successfully and will show that the process is completed as shown in then following figure.

After clicking the OK button the details of embedded bytes will be shown in the command window and will also show the text whatever you had encrypted in the picture.

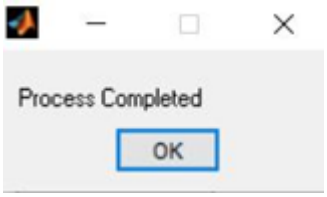


Fig-8: Shows the data decrypted

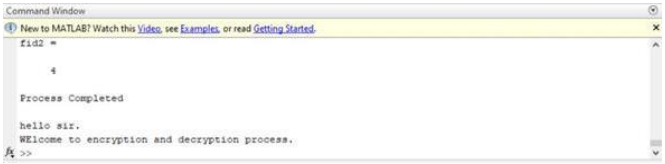


Fig-9: Show the output shown in command window

AFTER ENCRYPTION

Here the following figure shows the text what we want to encrypt inside a picture.

Fig-10: Shows the encode part

While the encryption process was going the decode file is empty as you can see in the following figure.

Both Fig- A & B Shows the comparison

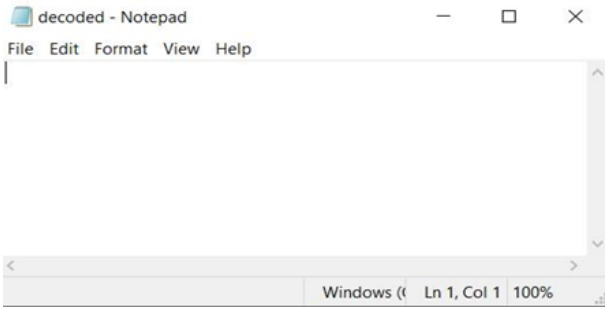


Fig-11: Shows decode part before decryption

AFTER DECRYPTION

After completion of decryption process we got the following message.

4.2 Audio Steganography

In this process after running the audio steganography program the below graphical user interference figure will appear asking for your command to proceed.

To hide the written data you have first choose the audio file which is in .wav form to encrypt the data inside. After choosing the file we have to click the button „Hide the Text" so that the text data can be hidden in the .wav audio format.

Fig-12: Shows decode part after decryption

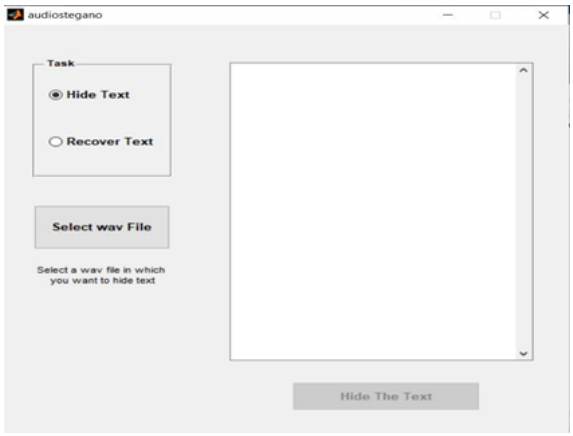


Fig-13: Shows the audio steganography graphical user interference format

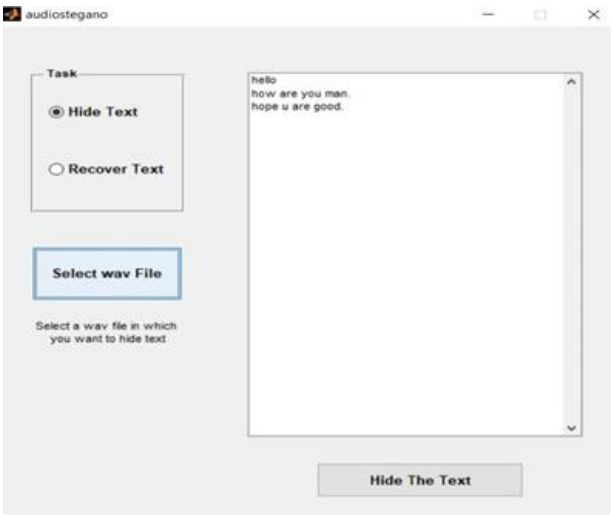


Fig-14: Data is written to hide

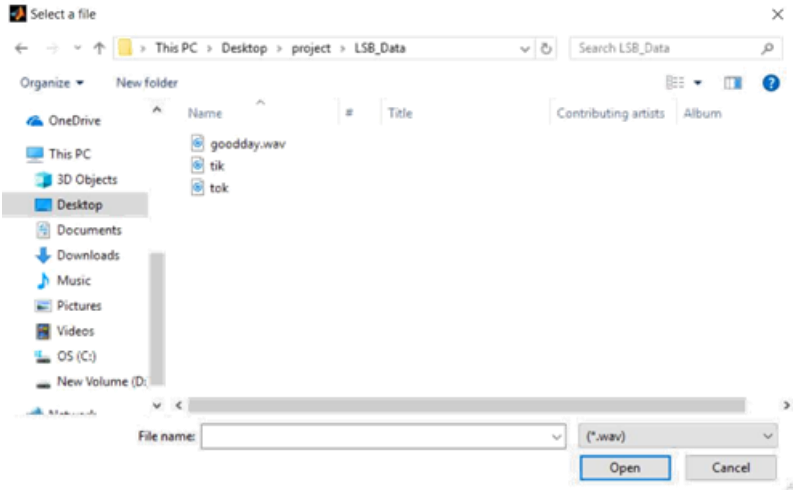


Fig-15: Shows which audio file to choose for hiding the data

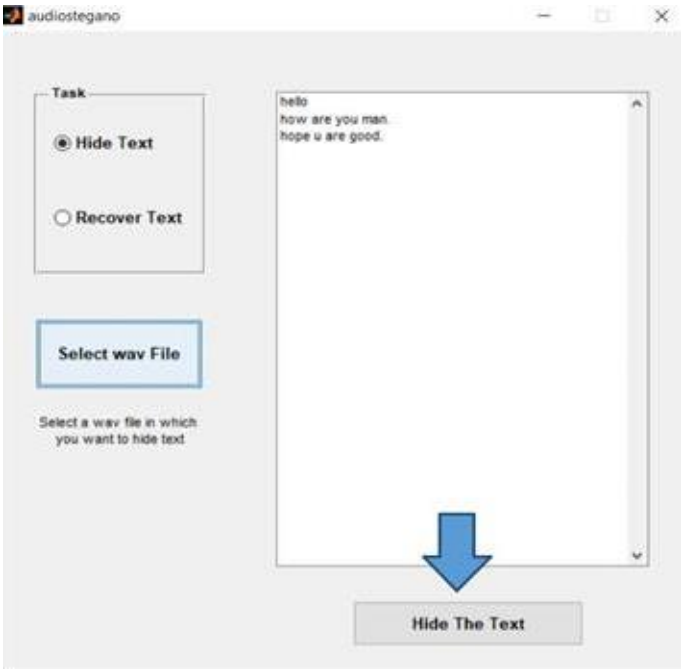


Fig-16: Shows the option to hide the data

After clicking the „Hide the Text" data a new copy of the same audio format will create with the encrypted data. As shown below.

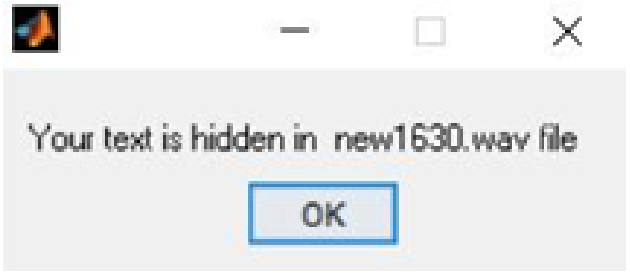


Fig-17: Shows the new .wav clip with the encrypted data

To know what inside the file the receiver have to recover the file by clicking „Recover Text" option which will lead you to the new .wav audio format to which you have to decrypt.

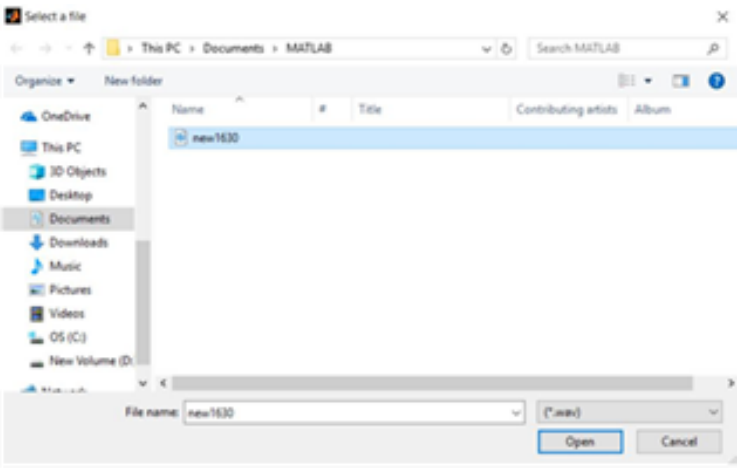


Fig-18: Shows the file chosen for decryption process

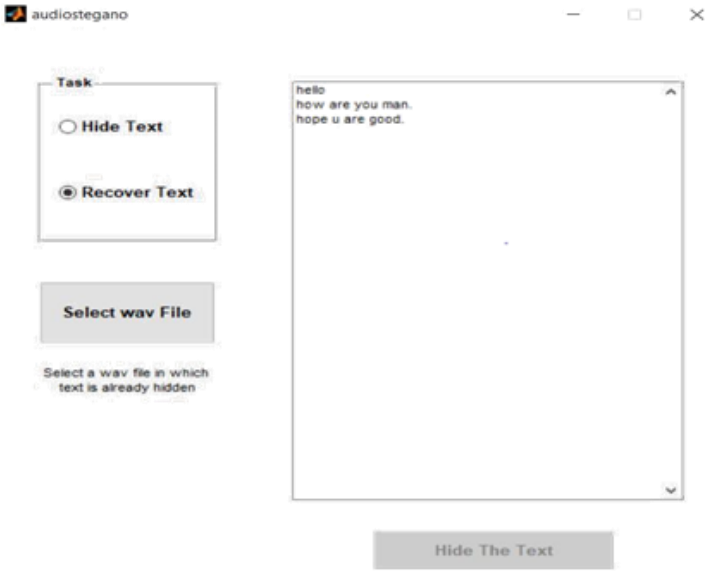


Fig-19: Shows the result of the file 'new 1630' after decryption

5. Challenges

While making the project we have encountered several challenges and difficulties. Some of them we have tried to overcome but some we were unable to rectify. Second challenge is, it does not support JPEG image for the encryption process. The most challenging task was transferring the embedded information to the destination without being detected.

6. CONCLUSION

A steganography technique has been put out in this research to provide greater information security in system settings. Information can be transmitted between sender and recipient using the system we have provided in an unbound system scenario. This system is undoubtedly one of the best ways to keep the secret of the message hidden from intrusions in the system domain.

The paper's main goal is to develop a system with additional security features. The secret message was scrambled using the Least Bit Algorithm, converted to ASCII code, and then inserted into the image to make the encryption code impossible to decipher without the secret key and keys. Furthermore, Least Significant Bit method has been executed for inserting scramble message into spread pictures. To assess this system we tried various pictures with different sizes of information to be covered up with the proposed calculations.

There is continually a space for improvement in any software package, however efficient the system may be. The system is flexible enough for future modifications. The system has been factored into totally different modules to form the system adapt to any changes.

This system is user friendly as any new user can use it and easily understand its functionality. Security is enabled as sure options and functionalities area unit restricted to the registered users solely and additionally at different levels security is enforced. Our aim is to

build user friendly secure data encryption and decryption system which can work as fast as possible.

REFERENCES

- Cachin, C. (1998). "An Information-Theoretic Model for Steganography", Proceedings of 2nd Workshop on Information Hiding, MIT Laboratory for Computer Science.
- Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). "Information Hiding - A Survey", Proceedings of the IEEE, 87(7), pp. 1062-1078.
- Amritpal, S. (2015). "An Improved LSB based Image Steganography Technique for RGB Images", Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on. IEEE, pp 1-4
- Mehdi, H. (2013). "A Survey of Image Steganography Techniques", *International Journal of Advanced Science and Technology*, 54, pp 113-124.
- Morkel, T. (2005). "An Overview Of Image Steganography", *ISSA*, pp 1-11.
- Poornima, R. (2013). "An Overview of Digital Image Steganography", *(IJCSES)*, 4(1), pp 23-31.
- Anil, K. (2013). A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique, *IJARCSSE*, 3(7), pp 363-372.
- Mahajan, S., & Singh, A. (2012). A Review of Methods and Approach for Secure Stegnography. *International Journal of Advanced Research in Computer Science and Software Engineering*, *2*(10), 67-70.
- Kour, J., & Verma, D. (2014). Steganography techniques–A review paper. *International Journal of Emerging Research in Management & Technology*, *3*(5), 132-135.
- Al-Shatnawi, A. M. (2012). A new method in image steganography with improved image quality. *Applied Mathematical Sciences*, *6*(79), 3907-3915.
- Sumathi, C. P. (2013). "A Study of Various Steganographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey (IJCSES), 4(6), 9-25.
- Rashi, S. (2014). "A Review on Image Steganography", *IJARCSSE*, 4(5), pp 686-689.
- Gunjan, C. (2013). "Image Steganography Techniques: A Review Article". Fascicule 3 [July–September], pp 97-104
- Shikha, S. (2013). "Image Steganography: A Review", *IJETAE*, 3(1).
- Stuti, G. (2013). "A Review of Comparison Techniques of Image Steganography", *Global Journal of Computer Science and Technology Graphics & Vision*, 13(4), pp 8-14.
- Rakhi. (2013). "A Review on Steganography Methods", *IJAREEIE*, 2(10), pp 4635-4638.
- Anjali, T. (2014). "A Review on Different Image Steganography Techniques", *IJEIT*, 3(7), 121-124.
- Kamble, S. V. "A Review on Novel Image Steganography Techniques", *IOSR-JCE*, PP: 1-4. ISSN: 2278-0661, ISBN: 2278-8727.
- Devasis Pradhan. "Invisible Digital Audio Watermarking using DWT-DCT based Transform." IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), vol. 12, no. 5, 2017, pp. 14–19 DOI: 10.9790/2834-1205021419