IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Framework to Analyse Different Application which is used to Identify Encrypted Media

Shaminaz[1], Dr. Divya .T.L[2]
[1]*Student*, [2]*Assistant Professor*
[1,2]*RV College of Engineering®, Bengaluru, India*

Abstract: Steganography Encryption is a technology which is used to hide any data or information as an embedded one within another file. Steganography was first used in 440BC. Its main purpose is to hide information from any third person. Data are hidden safely and for embedding data different tools are used where each tool uses different approaches to hide an information. This research is focused on how these technologies are misused by black hat hackers in order to make someone compromise his data and it is not a difficult task that any person who is master in hacking only can be done, it is something anyone can do that is why it is very difficult aspect to identify which image or audio or video is corrupted or embedded with malicious code.

Keywords: **Steganography encryption, embedding data, malicious code, technology misused**

1. INTRODUCTION

Steganographic Encryption is the process of concealing one piece of information within another. [1] It is not an inherently dangerous method for integrating text or data into an image. There are many legitimate reasons to hide a message within image. [2] Some of the legitimate reasons include: in social media, data that is very sensitive is encrypted before being sent; photographers, audio producers, and video producers use this to protect themselves from copyright theft; and in corporations, this technique is used to save the company's important documents. [3] Problem is when hackers use this technique to secretly hide and execute malicious code. When an image, audio or video is encrypted with malicious code, on opening those files by victims the malicious code run automatics at backside without the knowledge of victim.[4]. Main intention of this research work is to aware people about different kinds of Cyber-attacks. Everyone should know, how to secure their data, so that they won't be the next target of Black hat hacker.

There are different types of Steganography encryption: video encryption, audio encryption, image encryption etc. [5] The main goal of this research is to raise awareness about how Steganography encryption works, to help people understand how important it is to protect our data and to be aware of how to avoid compromising it.

There is a myth like if any image with a size in megabyte are stegano-object but it is incorrect as size of an images varies from image to image based on number of pixels an image consists of, like wise to video also. [6] One cannot claim that an image that is only a few kilobytes in size cannot be encrypted; any image can be encrypted, so one precaution is to avoid downloading any video or audio that is sent by an unknown source and to refrain from forwarding such images until one is certain that the image does not contain any malicious data. [7] In one or the other way this cycle is to be stopped where a person unknowingly download malicious codes embedded data and same he/she shares across, the person who trust the another person download and shares the same. [8]

There is no specific prevention one can follow as one cannot differentiate image whether it is stegano-object or not, just by following some steps, because there are enormous number of tools where each tool follow different algorithm and even after knowing that any image, video or audio is encrypted, it is difficult task to extract hidden file without knowing the tool used to hide. [9] Image size will be more, like double of a normal file. In those file it's also possible to identify all image files as built out of binary digits and encrypted message will be in text, chances of image reflecting those text is more. [10]

When there is need of identifying any image, audio or video whether it is encrypted or not, in that case these demonstration steps can be followed to identify if any media which one is possessing right now is encrypted with malicious code or not.

2. IMPLEMENTATION AND RESULTS

In this research work, demonstration is done to make people aware about how it is simple to create a stegano object of audio, video, images and also without using any tool, so that everyone should keep their data safe and if any such media one have, they can find if any media is encrypted or not using the below demonstrations. [11]

1. **Demonstration of hiding a text file in image without any tool.**

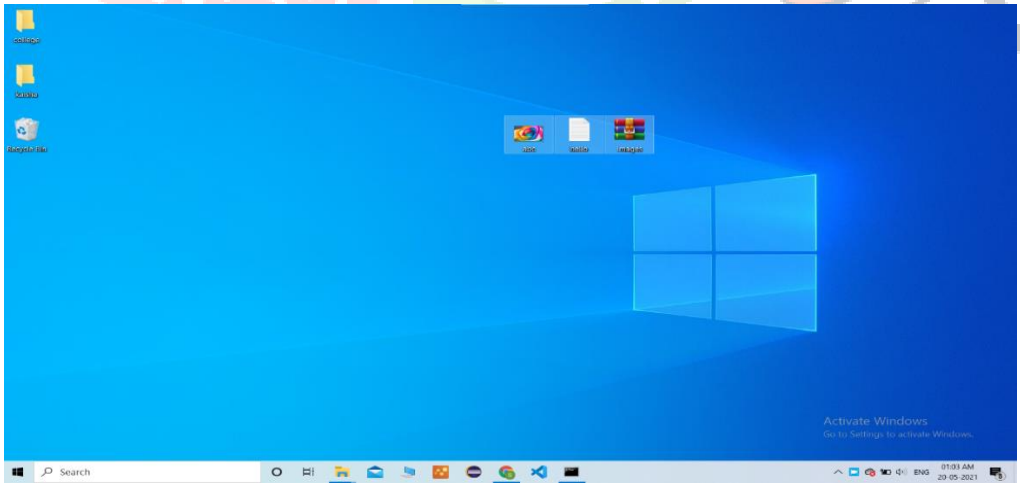

Figure 1 Creating an empty Zip folder

In Figure 1, a text file with a message, a picture of a flower and a zip folder was created, named images.[12]

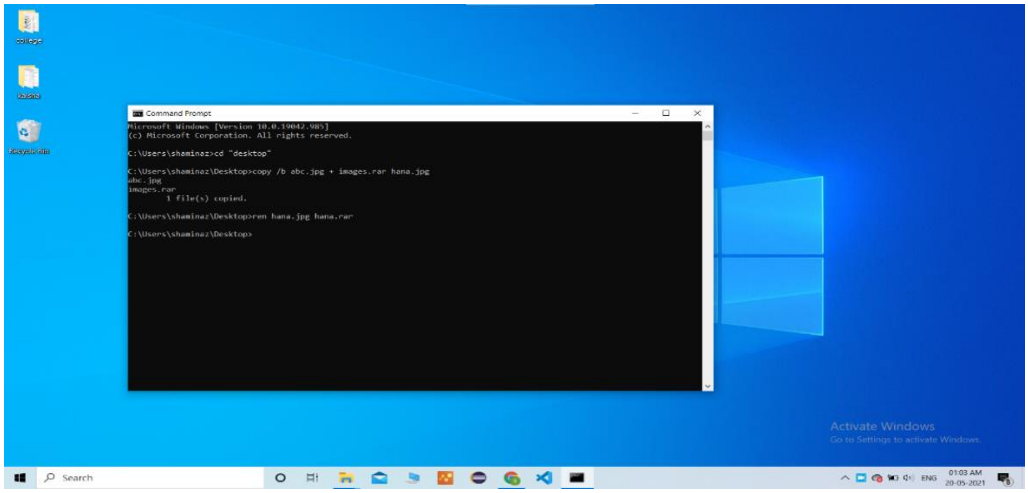

Figure 2 Open cmd prompt

In Figure 2, after opening cmd prompt above commands were executed.

Copy /b abc.jpg + images.zip hana.jpeg

The above command copies the binary values of abc.jpg file and images.zip file and combining them, output of the combined file name is given as hana.jpeg. [12]

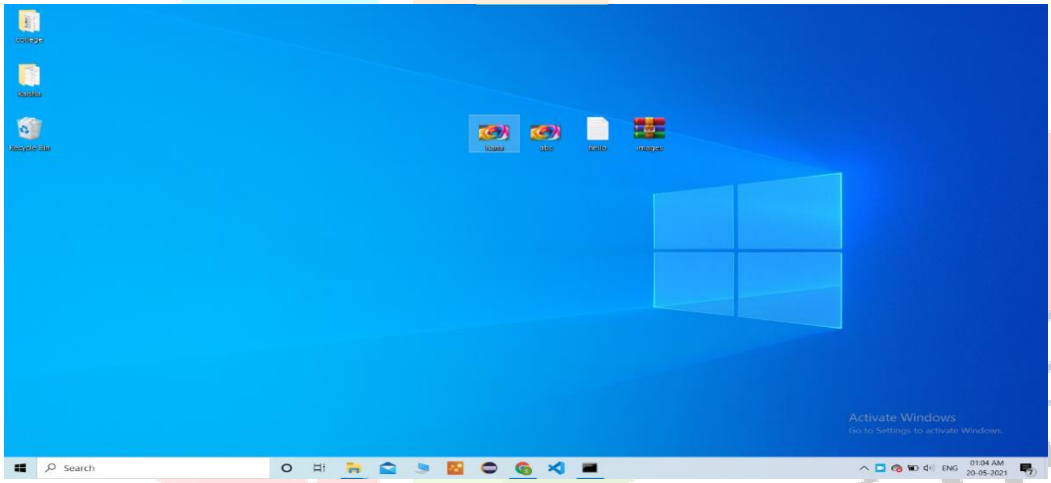

Figure 3 Display output file

In Figure 3, after executing command as mention In Figure 2, the output file will be displayed as above.[12]

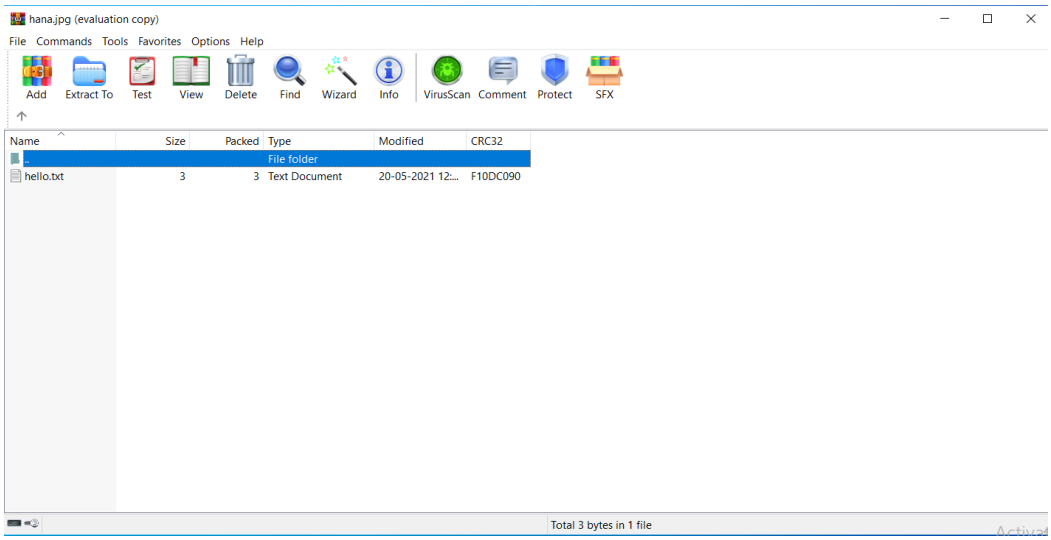

Figure 4 Way of identifying the hidden message

In Figure 4, from Winrar tool if any stegano object, in this case it is an image, if it is opened then the hidden files are visible.

Another option is shown In Figure 2, where another command is executed.[12]

ren <stegano_object file name> <new file name>

The above command converts .jpeg file to .rar file, which is a hidden file.

2. **Demonstration of hiding pdf file in image using a tool called as OpenStego**

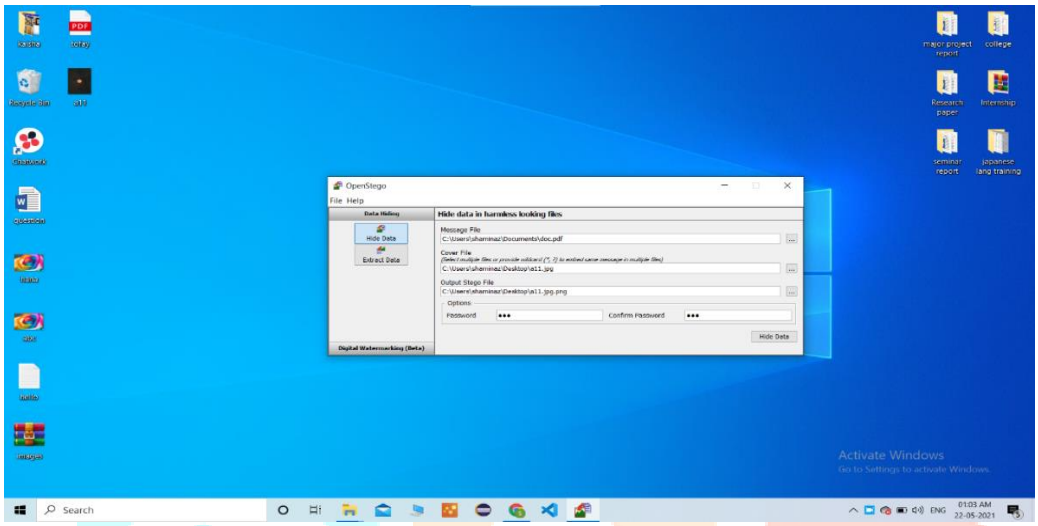

Figure 5 Open stego home screen.

In Figure 5, there are 2 option hide data and extract data, in hide data option, embedding image, output file and embedding document should be added along with password, to give extra security. [13]

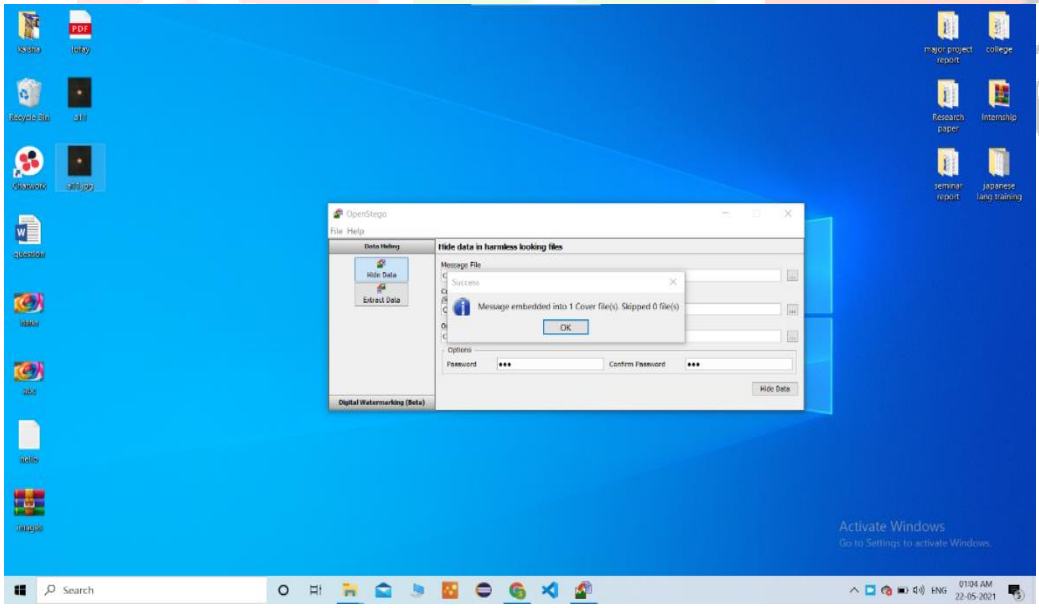

Figure 6 Data embedded with an image

In Figure 6, it is displaying the alert message showing the file embedded and saved in the desktop.

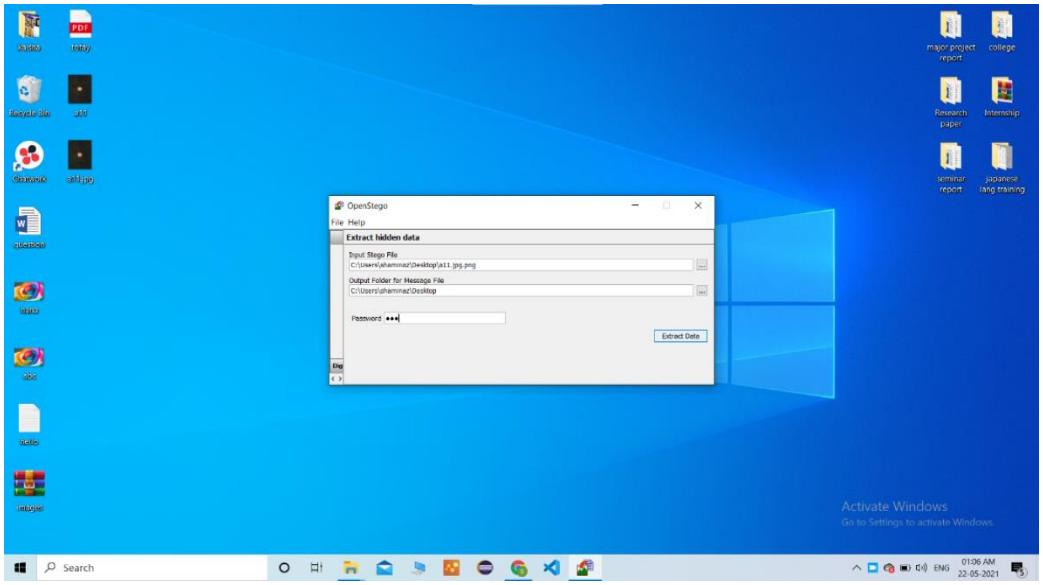

Figure 7 Extract data

In Figure 7, images embedded using Open stego tool can be extracted as shown, where the embedded image, with destination to save that file along with password have to be entered respectively.

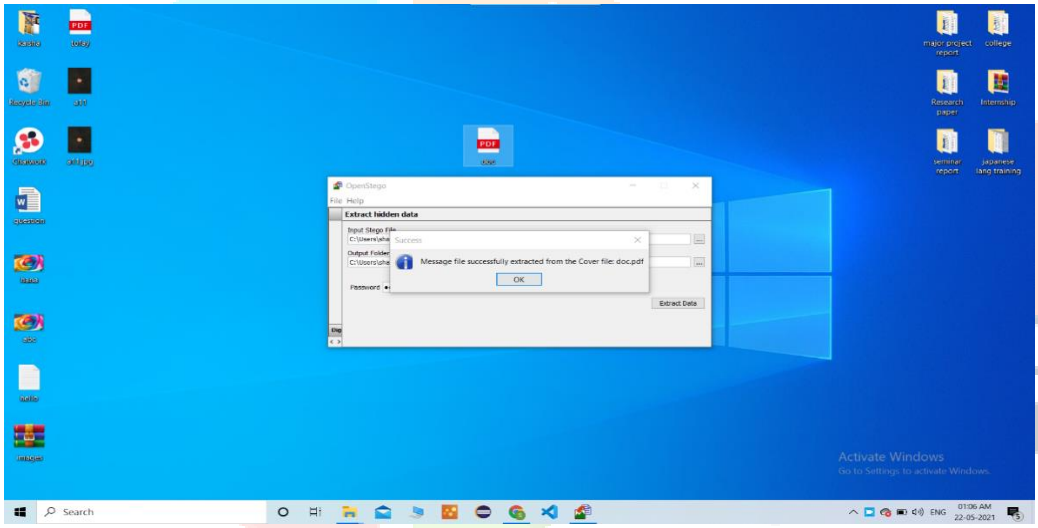

Figure 8 PDF file extraction

In Figure 8, These alert messages can be seen once the data from the image has been extracted.

3. **Demonstration of hiding a ppt file in a video using a tool called as DeEgger Embedder.**

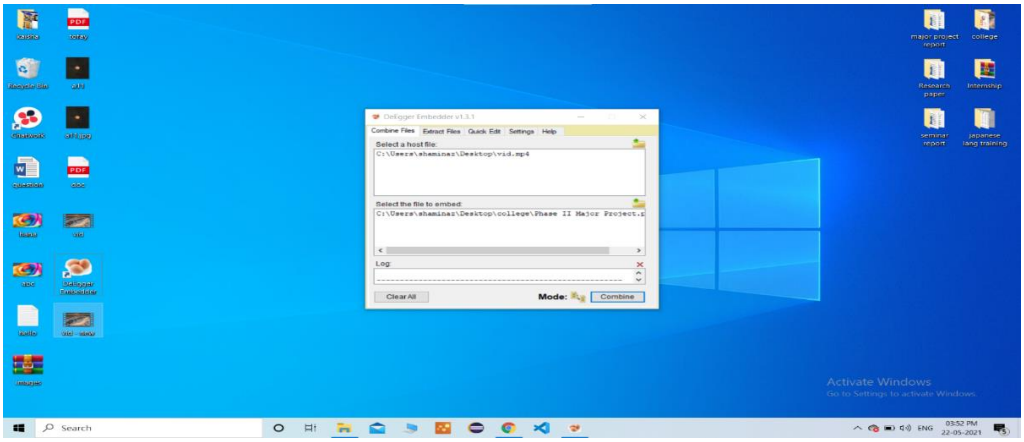

Figure 9 Embedding a data in a video

In Figure 9, using a tool named DeEgger Embedder a ppt presentation is been embedded within a video.[14] Video location along with the embedding file location should be added in this and should click on the button combine.

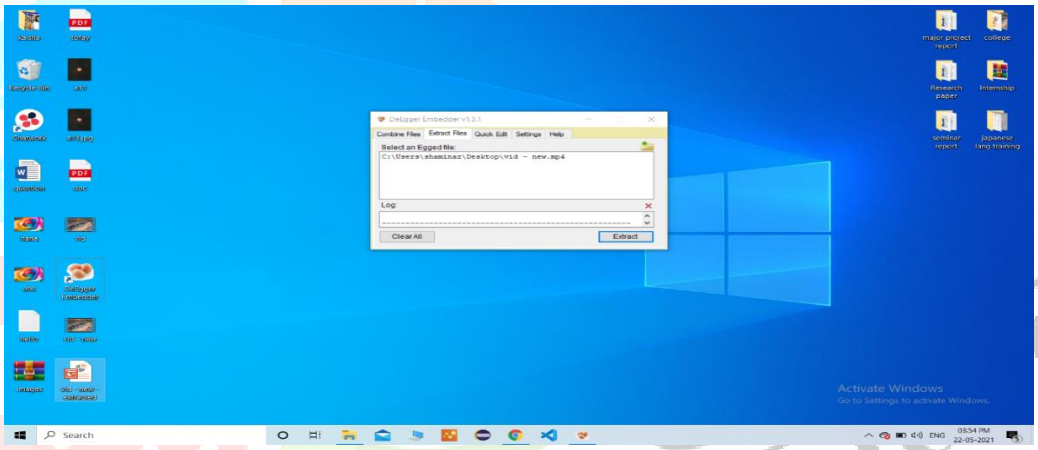

Figure 10 Extracting data from video

In Figure 10, the data file which was embedded within a video can be extracted by just giving the url of the embedded video.

4. **Demonstration of hiding a graphic message in an audio file using a tool called as Coagula and to retrieve a message using a tool called Sonic Visualiser.**

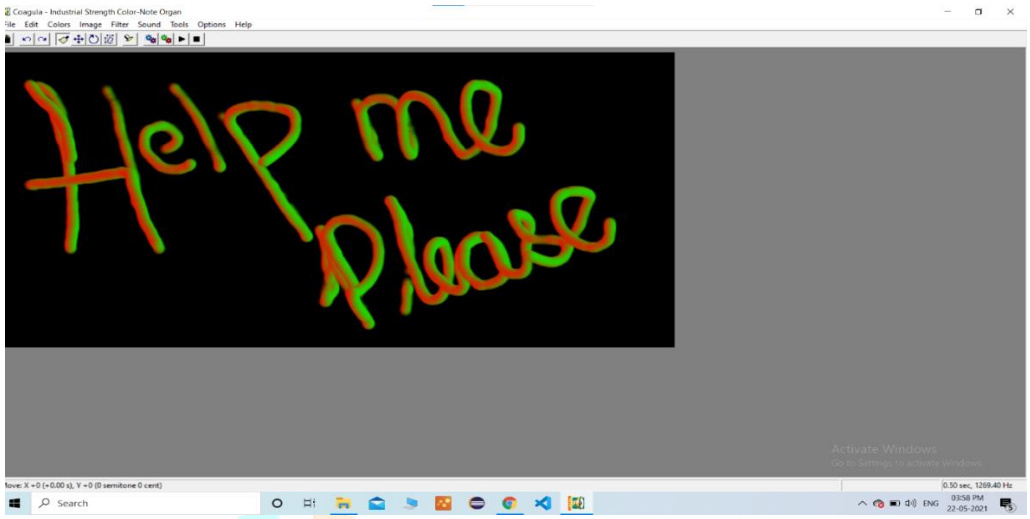

Figure 11 Coagula applications page

In Figure 11, Using Coagula graphic application a message was drawn and converted that message into a wave file.

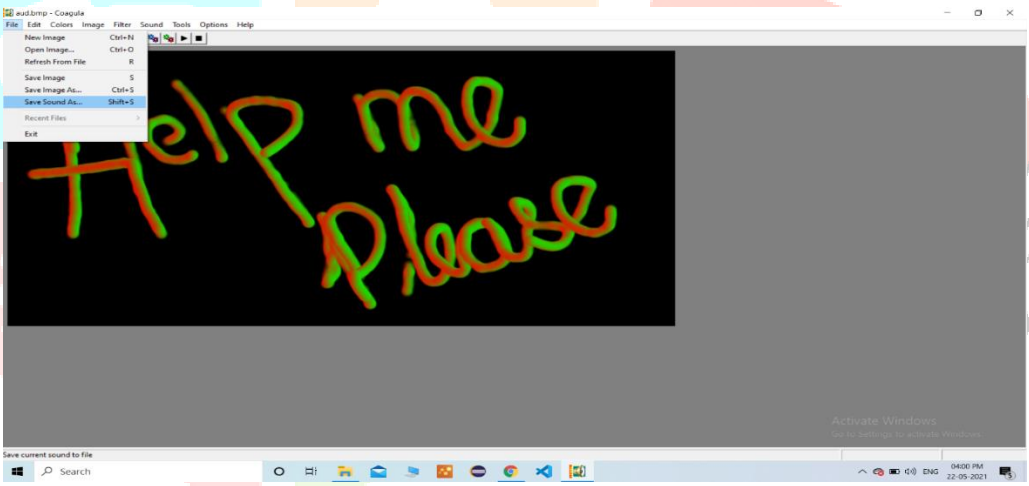

Figure 12 Graphic page

In Figure 12, it shows different option like that graphic image can be converted as image or can be converted as a sound wave file with an extension of .wav.[15]

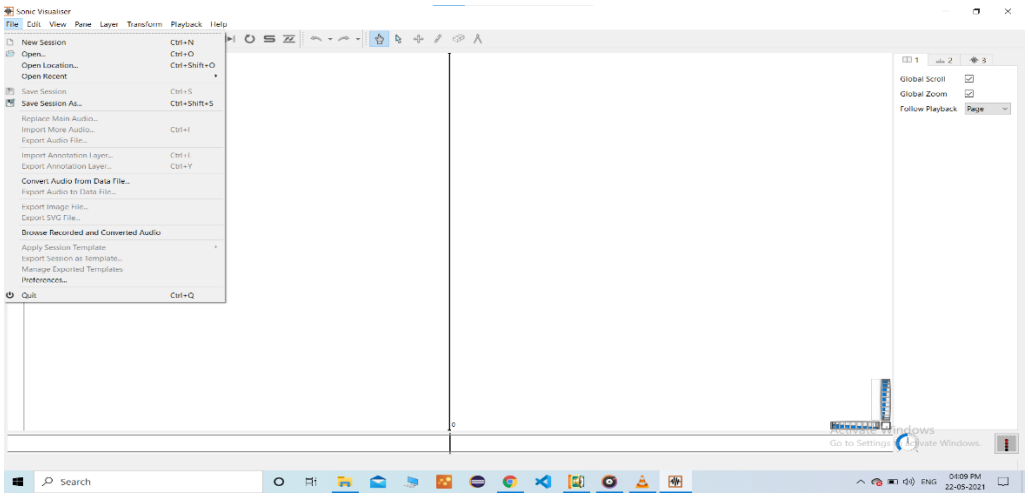

Figure 13 Sonic Visualization screen

In Figure 13, there are many option like one can create a new session or open existing application, here one have to select an audio file which is been created earlier[16]

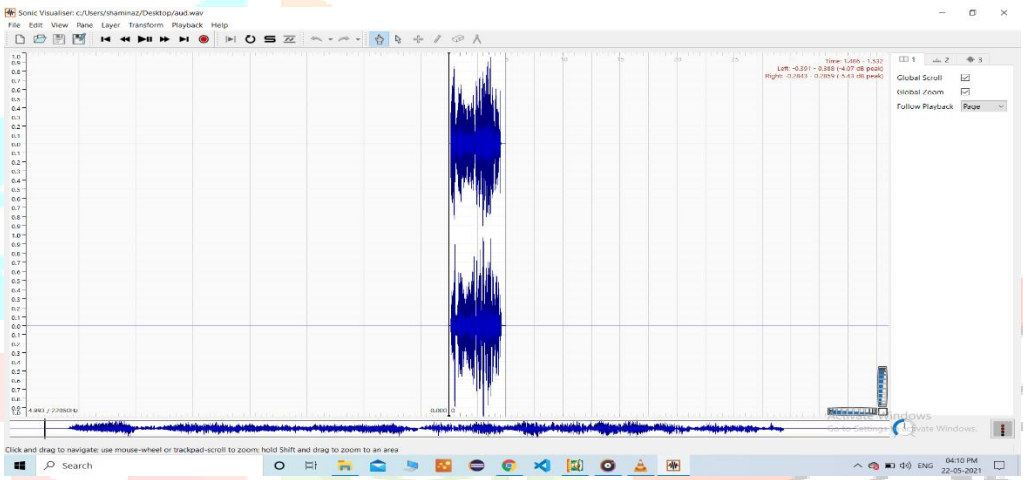

Figure 14 Wave file of an image

In Figure 14 the audio file created earlier using application coagula, will be opened using sonic visualization.

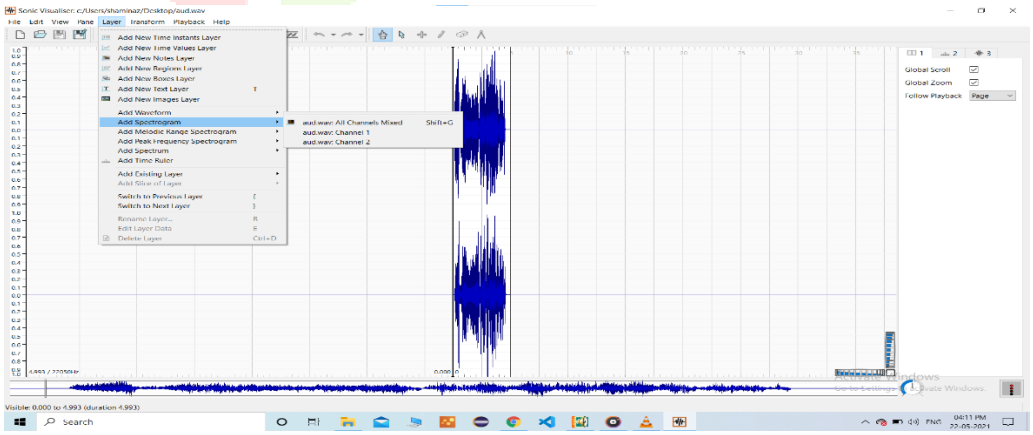

Figure 15 selecting a channel

In Figure 15, for converting audio file into a spectrogram, one should select both channels, as it requires two channels to get back the hidden message in an audio.

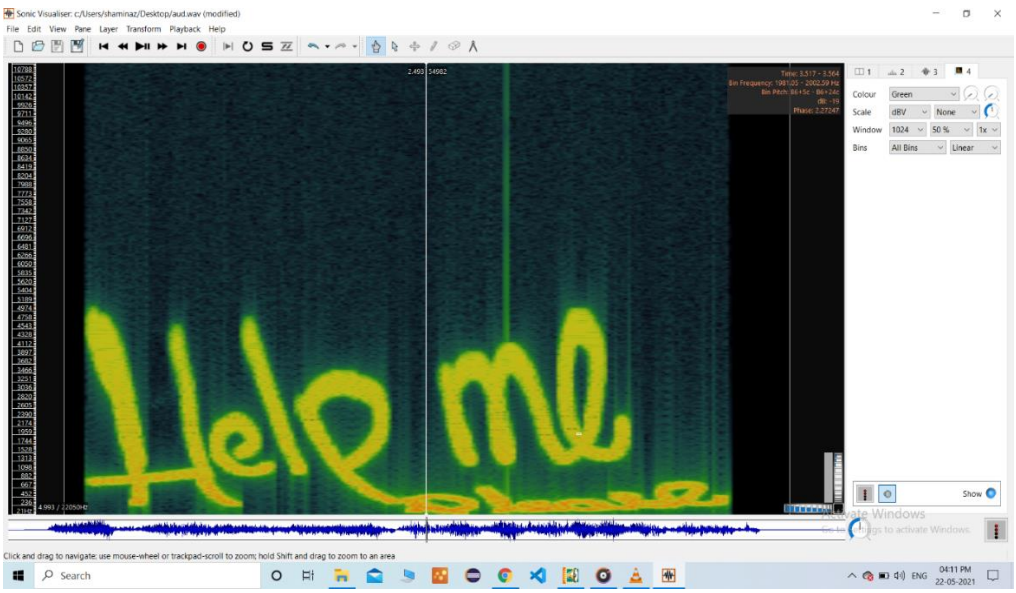

Figure 16 Output of audio

In Figure 16, after selecting the two channels as shown In Figure 4, the output will be as shown here, which displays same message as it was created using the tool coagula.

CONCLUSION

Steganography encryption is a part of privacy of Internet and its security, in an open system like Internet. While steganography may offer valuable solutions to the privacy concerns that plague Internet and its security. It also offers easy way for hackers to plan their crimes and hide their intentions. [18, 19] It is not an inherently dangerous method for integrating text or data into an image. There are many legitimate reasons to hide a message within image. Problem is when hackers use this technique to secretly hide and execute malicious code. Malware is embedded in videos, photos, and graphics so that it can be transmitted undetected. [20] Cyber-crime is never taken into consideration until it is faced by an individual. To prove the security of data is very much required. The main goal of this research work is to raise awareness about steganography encryption and how to protect themself.

REFERENCES

[1]. Meghana.N, Chethan.H, “New Method For Secret Image Transmission using Mosaic Fragments via ECC Key”, IEEE international WIE conference on electrical and computer engineering, 2019.

[2]. Divyansh Singh, “Digital Image Steganography”, International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429 Volume 8 Issue V, 2020.

[3]. Sachin Dhawan, “A Review of Image Compression and Comparison of its Algorithms”, International Journal of Electronics & Communication Technology, Volume 2 Issue 1, 2016.

[4]. Fran¸cois Kassene Gomis , Thierry Bouwmans, Mamadou Samba Camara , and Idy Diop, “Estimation of the Hidden Message Length in Steganography: A Deep Learning Approach”, International Journal of Computer Applications, 2018.

[5]. Khider Nassif Jassim, Ahmed Khudhur Nsaif , Asama Kuder Nseaf , Al Hamidy Hazidar , Bagus Priambodo, Emil Naf'an , Mardhiah Masril,Inge Handriani , And Zico Pratama Putra, “Hybrid cryptography and steganography method to embed encrypted text message within image” , International Conference Computer Science and Engineering,2019.

[6]. Huma Jabeen, Professor Abdul Wahid, “Image Steganography using Pseudo Random Number Generator”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 8, Issue 3, ISSN: 2278 – 1323, 2019 .

[7]. Mahendra Kumar and Richard Newman, “J3: High Payload Histogram Neutral JPEG Steganography”,Department of Computer and Information Sciences and Engineering University of Florida, 2016.

[8]. Mr. Sudhakar A, Purushotham Y , Shankupalle Sree Charan , Syed Sohail Ahemed , V K Praveen Kumar, “Armour for Nebulous Data using Secret Writing”, International Journal for Research in Applied Science & Engineering Technology (IJRASET) . Volume 8 Issue V, 2020.

[9]. M. V. Ramana , N. Likita Rajeswari , M. Syamala , V. L. Aparna , M. S. Susmitha , P. Tulasi, “Secure Record Storing on Cloud using Blend Cryptography”, International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429 Volume 8 Issue V , 2020.

[11]. Steganography Dr. Saleh A. Khawatreh, Dr. Jihad Nader, Dr. Mohammad S. Khrisat, Prof. Yousif Eltous, Prof. Ziad Alqadi, “Securing LSB2 Message”, International Journal of Computer Science and Mobile Computing, Vol.9 Issue.6, pg. 156-164, 2020.

[12]. Mishra , Ms. Deepica S. Dominic, “Steganography Data Hiding Technique Satyam”, International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429 Volume 8 Issue VI June 2020.

[13]. Hardikkumar, D. Apurva, "Steganography of Messages using Mandelbrot Fractal", VNSGU Journal of Science and Technology – Vol. 5 No. 1, 2016.

[14]. Hetal N. Patel , Dipanjali R. Khant , Darshana Prajapati "Design of a color palette based image steganography algorithm for fractal images", International Conference on Wireless Communications, Signal Processing and Networking, 2017.

[15]. sharingJens Saenger b , Wojciech Mazurczyk a , Jörg Keller b , Luca Caviglione c, “VoIP network covert channels to enhance privacy and information”, Future generation computer system 111 , 2020, 96-106.

[16]. Mohammed Abbas Fadhil, “A Novel Steganography-Cryptography System”, Proceedings of the World Congress on Engineering and Computer Science 2015 Vol I WCECS 2015, October 20-22, 2015, San Francisco, USA.

[17]. Amritpal Singh, “An Improved LSB based Image Steganography Technique for RGB Images”, Electrical, Computer and Communication Technologies (ICECCT), 2017 IEEE International Conference on. IEEE, 2017, pp 1-4 .

[18]. Mehdi Hussain, “A Survey of Image Steganography Techniques”, International Journal of Advanced Science and Technology Vol. 54, May, 2018, pp 113-124

[19]. T. Morkel, “AN OVERVIEW OF IMAGE STEGANOGRAPHY”, ISSA. 2015, pp 1-11.

[20]. R.Poornima, “AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY”, (IJCSES) Vol.4, No.1,February 2017, pp 23-31.