JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Secure Communication using Steganography and Machine Learning

[1]Vishwas P, [2]Dr.Shamshekhar S. Patil,

[1]Student, MTech, [2]Associate Professor,
[1,2]Department of Computer Science,
[1,2]Dr. Ambedkar Institute of Technology, Bangalore, Karnataka, India

Abstract: Machine learning techniques have advanced in our modern world and have improved the ease, efficiency, and security of a much of our lives. The main priority is always security. We have to provide a protection for the private data to be able to ensure the safe transmission of any existing confidential information. However, hackers will always find a technique to breach the security barrier. Therefore, it is going to be safe to employ additional security measures to safeguard the system. The more security measures in place, the harder it will be for hackers or other intruders to breach the perimeter. Here we provide a system called steganography. Through the utilization of a secret key, users of the program can insert a concealed information into a chosen media. Here the chosen media acts as a carrier media. Steganography is divided into three categories, image, audio and video steganography. An existing secret information can be encrypted and decrypted by the user. Bit slicing technique used to transform the carrier material into bit planes. The least significant bit of the carrier media is replaced with transformed bit format of text utilizing the LSB (Least significant bit) algorithm following bit plane conversion. By uploading the stego media that has been received and inputting the right secret key, the recipient is able to decode the information that has been encrypted. Our design meets any of the given operational criteria, is user friendly, and is straight forwardly directed.

***Index Terms* - Encrypt, Decrypt, Steganography, Security, LSB (Least Significant Bit)**

I. INTRODUCTION

In our habitat, sharing the confidential data to other user is a complex process. The user can share the data to another user on some social platforms like WhatsApp, Facebook, Mail and so on. But the main issue is the safe keeping of the confidential data. To provide the security to the confidential information from the unauthorized user. we have to conceal the confidential data in other files. Steganography method is to encrypt the confidential information inn a file like image, audio, video containing a secret key.
In order to accommodate the secret message, steganography converts the cover file in to binary data. Binary data has two segment, namely most significant bit and least significant bit. User replaces the least significant bit in cover file by binary message. Those who have acquaintance about the method and have secret key to the necessary resource, may extract and decode the encrypted message from the cover file which still appears to the untrained eye to be the original cover file.
There are three types of steganography, namely-
1.Image steganography: Image steganography hide the Existing confidential information in an image file where image file acts as cover file. The format of the image is in jpg, jpeg.
2.Audio Steganography: Audio steganography hide the confidential information in an audio file where audio file acts as cover file. The format of the audio is wave format.
3.Video Steganography: Video steganography hiding the confidential information in a video file. The format of the video is in mp4.
The process of steganography involves mainly on two components
1.Cover file: It is a file that user can encrypt a message into it.
2.Secret message: It is the information that user wants to encrypt in cover file
Though steganography is less popular than cryptography, it has more benefits as outsiders cannot notice the secret data. According to the cover media steganography has different names such as audio steganography, image steganography and video steganography. Basically, steganography none other than cover writing while cryptography relies on secret writing and is used only for data protection. Cryptography is the study and practice of methods for communication in the occurrence of third parties called adversaries. It deals with evolving and assessing the procedure that restrict spiteful third parties from getting their hands on the information that is being exchanged between the two parties thereby following the various outlook of the information safety. secure communication refers to the scenario where the message or data shared between the two parties can't be accessed by an adversary.
Machine learning is an extent of artificial intelligence. The objective of machine learning is to allow the structure of data and adopt that data into models that can be recognized and utilized by people. It is intriguing technologies that one would ever come across. Machine learning is the field of study that gives computer ability to learn without being explicitly programmed. As it is evident from the name, it gives the computer that makes it more relatable to human's "the ability to learn". Machine learning is being used very often in these days, yet it is expected to be used in many more places. Although machine learning is a filed within a computer science, it differs from conventional computational approaches. In conventional computing, algorithms are collection of distinctly programmed rules used by computer to resolve a problem. We need to be very persuasive in at least any one programming language, preferably python. Python language has made coding effortless. It contains a lot inbuilt libraries which can be made use to model the system automatically. One more significant factor is domain language. If we choose machine learning as our domain, we should be acknowledged regarding that particular domain like what are the different applications available is the domain or how they work

is very significant. The third essential thing is mathematics and algorithms. Only coding knowledge alone is not enough to solve complex set of issue. We also need to have knowledge about the mathematical equation and steps, mathematical procedure along with machine learning algorithm can be blended in order to generate a useful model. Basically, the data scientist has too very inquisitive regarding everything around them. Why and what questions has to pop in their thoughts in order to understand the topic more evidently. Through investigation will help to resolve a complicated issue smoothly.

II. LITERATURE SURVEY

Junqui Wu, Bolin Chen, Weiqi Luo and Yanmei Fang [1] Illustrate steganography, which uses audio files as the carrier file and data as the encrypting information. It might challenge to share private information publicly. Thus, they suggest using audio steganography. Here, audio steganography is being implemented utilizing the CNN algorithm for security. digital multimedia steganalysis has shown that convolution neural networks (CNNs) perform better. With the use of secret key, a user may both encrypt existing information and decrypt the encrypted file. This implementation's primary goals are to secure the transport of existing information via encryption and a secret key.

Yunzhao Yang, Xianfeng Zhao, Xiaowei Yi, and Haibo Yu [2] they propose an adaptive double-layered embedding system for mp3 steganography in this implementation. The encoded region is made up of Lin bits in accordance with the audio encoding specifications. The proposed technique has two levels, and binary STCs that are employed for storing the data in every layer. In order to attain the best imperceptibility, the cost function employed in the initial layer was created through the use of masking effect. The cost function for the second layer is changed in accordance with the first layer's embedding findings in order to reduce the modification of coefficients. Experiments show that this method is effective in achieving higher embedding modification efficiency and improved sound concealment.

Songbin Li, Yizhen Jia and C.C.Jay Kuo [3] describes about structural analysis of a voice source encrypted with tiny bits using quantization index modulation (QIM) steganography is carried out. We first find out that the significance qualities of divided vector quantization VQ code phrases of linear predictive coding filter coefficient are altered during QIM steganography. In accordance with the principles of speech production concept and sound dispersal features in conversation. They build a model known as the quantization codeword correlation network (QCCN) based on splitting VQ codeword from neighbouring sound frames in response to this discovery.

Houngguo Zhao, Yunxia Liu, Yonghao wang, SI Liu and Cong Feng [4] describes about the video steganography, secret information embedded in a video file. The use of video in high-definition has created an abundance of discussion in both academia and business. H.265/HEVC, the most recent and significant video coding technique, represents an exciting opportunity for video steganography. In this article, they describe a brand new, effective solution for H.265 format video steganography that depends on transformation block choice. They alter the splitting parameters in CB, PB and TB, assess the encoding errors of data hiding, alter the transformation block choice for integrating secret message, and updates relevant residuals concurrently with the goal to improve the clarity of carrier video. The recommended strategy can provide higher appearance quality, a greater embedded capability, and a smaller bit-rate increases than innovative research, according to data from experiments.

Jie Wang,Xiaoqing Jia, Xiangui Kang and Yun-qing [5] describes the video steganography, text can be encoded in high efficiency video. Based on intra-prediction mode (IPM), this research suggests a brand-new HEVC video steganography. Initially the probability distributions of 4*4 IPMs is examined in this work. The safety and functionality of a stego streaming video may then be enhanced by combining a cover selection strategy with programming information from the coding unit (CU) and prediction unit (PU). Additionally, the steganography on HEVC video streams is implemented using matrix coding as an example of coding. Experimental findings demonstrate that the suggested technique is not only simple to use but also capable of maintaining both security and video quality. Likewise additional HEVC IPM-based steganography can incorporate the suggested cover selection criterion.

Richa Khare [6] describes about the video steganography to embed and decode the existing information. Video steganography is a technique of concealing a secret message within a video. The addition of this information to the footage is not visible to the naked eye because there is barely any change in pixel color. The addition of neural network techniques, such as back propagation neutral networks (BPNN) and artificial neural networks approach adoption (ANN), might enhance the techniques effectiveness even more. In the suggested way, they implemented steganography in the video file using a back propagation neural network technique.

Lindawati [7] propose an image steganography application to android. This approach performs modifying or changing the LSB, which is the part of the media package with the bits of data that need to be concealed. Message that was successfully encrypted earlier will be concealed uniformly on every region in mp3 or wav that has been separated. The java programming language eclipse is used by the author to create the steganographic application because it is simple to use and compatible with the android mobile operating system.

Fauzi Adi Rafrastara and Raka Prahasini [8**]** describes about the image steganography method how the message embedded and decoding using the LSB patterns. This study suggests using a three-bit LSB pattern, where the design is made up of the second, third- and fourth-bit s of LSB. To reduce LSB alteration in each pixel of the cover picture is the goal. It has been demonstrated through testing that the inverted LSB approach, which employs three LSB patterns, yields superior result to the two-bit LSB pattern. In eight out of ten cover images that were evaluated, the stego image quality had improved. To improve communication security, chaotic map-based message encryption techniques are also used and integrated with the LSB inverted approach.

Omar Elharrouss, Noor Almaadeed, Somaya Al-maadeed **[9]** describes, The LSB (Least significant bit) method is modified and used in this instance. The bit- inversion approach improves the appearance of the stego- image. This method lowers the quantity of changed LSBs by inverting any of the cover image's least significant bits after LSB steganography when they occur together with a pattern of other bits. Thus, fewer least significant bits of the cover image are changed than with the standard LSB technique, increasing the stego image's PSNR. The right message picture may be produced by saving the bit patterns for which the LSBs are inverted. The RC4 technique has been utilized to achieve the randomization in concealing message image bits into cover image pixels rather of storing them subsequentially, which increases the resilience of steganography.

III. PROBLEM STATEMENT

The main purpose of the steganography is to improve safety and potential by employing LSB (least significant bit) substitution, data encryption and randomized insertion. In addition, numerous other LSB planes are utilized for data masking and the chunking with interleaving is put in for huge payloads. In audio steganography multi-channel inserting is employed, while video steganography selectively chooses frames with little motions. For image steganography, inserting exist in regions with invariable pixels values and texture. The recommended type draws attention to adaptability, improve imperceptibility and defiance to steganalysis methods providing a comprehensive solution for safe and efficient steganographic communication in various media type.

IV. METHODOLOGY

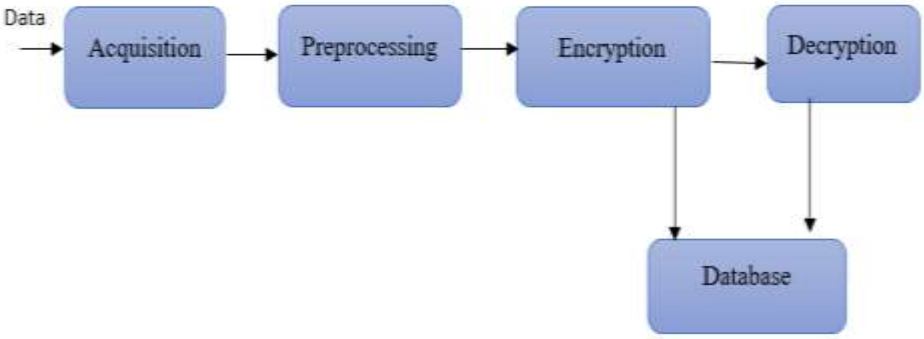


Figure 1.Steganography Modules

A. Data acquisition: The first step in the procedure is to gather the essential data elements for image, audio, video steganography. This involves deciding on a suitable wave audio file to serve as the secret message’s carrier for audio steganography, jpg image file to serve as the secret message’s carrier for image steganography and mp4 video file to serve as the secret message’s carrier for video steganography. A graphical user I interface (GUI) program that the user uses offers a file browser so they may select the appropriate audio file from their device storage by interacting with it.

B. Pre-processing: The user is requested to input the secret message they want to hide in the carrier media. The carrier media file needs to contain this hidden message in order to be embedded. After that, the input text is ready for further processing.

C. Bit-slicing and data embed: bit slicing generally the primary mechanism employed for data embedding in wave audio files. The secret message is transformed into its binary equivalent after the user enters it. The secret message is encoded using every character’s 8-bit binary equivalent. After that, the wave audio file is examined, and its samples are converted to a binary format. The least significant bits (LSBs) in audio samples are swapped out for the appropriate bits of the private messages in order to incorporate the secret message within an audio file. The LSBs are selected for encrypting because they have the smallest influence on audio quality and are least possible to be detected by humans. This technique makes sure that the concealed data blends in with the audio file without producing audible errors.

D. Encryption and key management: the GUI program invites the user to input a secret key before embedding procedure in order to improve the protection of the concealed data. The secret key serves as an encryption and decryption password. It makes guarantee that only those having right key may access the secret information. The user provided secret key will remain private and only accessible by those with permission by being saved in a separate file. Bit slicing is utilized to merge the certain media file with the secret message during encryption, and the resultant audio file is then stored with the given output file name.in order to be used subsequently during the decryption process, the key file is also saved together with the encrypted media file.

E. Decryption and secret message retrieval: The user is providing a choice to decrypt the earlier encrypted media file at the decryption stage. The software asks the user to input the secret key before continuing. The decryption procedure starts if the given key matches the one that was saved during encryption. The software examines the encrypted media file and extracts the LSBs from each sample during the decryption process. The binary representation of the concealed secret message is made up of these extracted LSB’s. The application then changes this binary representation back into text, displaying the user with the secret message.

F. Database: Database module is most important module for storing the necessary information. The database could store information on encrypted file and their accompanying data, including file names, keys, and secret data.

V. IMPLEMENTATION

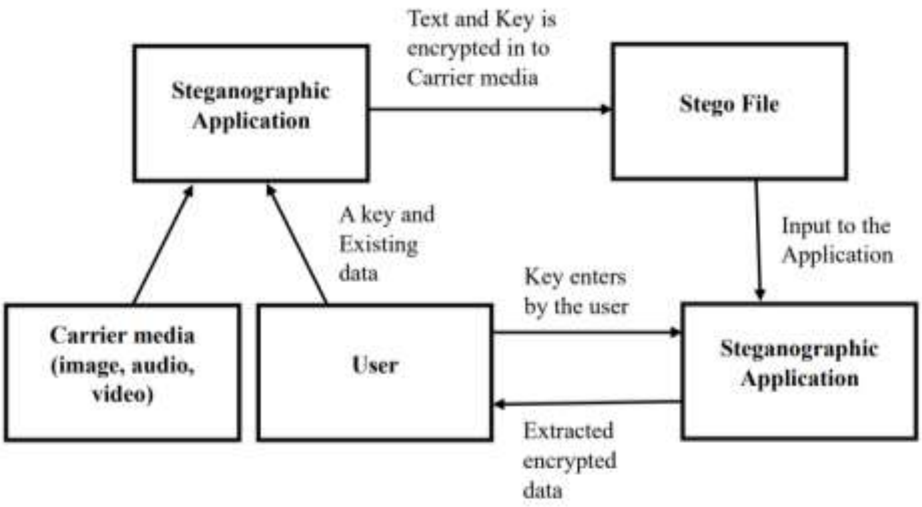

Steganographic Application
Text and Key is encrypted in to Carrier media
Stego File
Input to the Application
A key and Existing data
Key enters by the user
Carrier media (image, audio, video)
User
Steganographic Application
Extracted encrypted data

Figure 2: Architecture Diagram

4.1 Bit slicing

Bit slicing is a type of data manipulation method used in computer graphics and image processing to conceal information inside a picture. The procedure entails segmenting a picture into several bit planes, each of which stands for a certain bit position of the pixel values. This accomplished by first converting the image's pixel values into the matching 8-bit binary representation. The ith bit from each byte of the pixel values is taken once the picture has been converted to binary form, and it is then utilized to build the ith bit-plane image. To put it another way, each bit-plane picture will only show the contribution of the appropriate bit from each pixel in the original image. The approach allows for the subtle embedding of concealed data without considerably affecting the visual quality of the image by modifying the least significant bit (LSBs) of the pixel values, which have less of an effect on the overall look of the image. As a result, bit slicing is a well linked technique for steganography in which secret information may be hide inside seemingly innocent visuals to prevent discovery.

The concept of "bit plane" corresponds to the several layers that make up the image in the context of bit slicing with each bit plane serving as a binary representation of a particular bit position over all the pixels. We can express a large range of pixel intensity values by splitting the image into 8 separate bit-planes since 8 bits may represent 256 distinct levels. Real time applications are possible because the extraction and arrangement the bits into these bit-planes are computationally efficient. The higher order bit-plane values should not be significantly changed by the concealed data, though, as this might result in obvious artifacts in the final image.

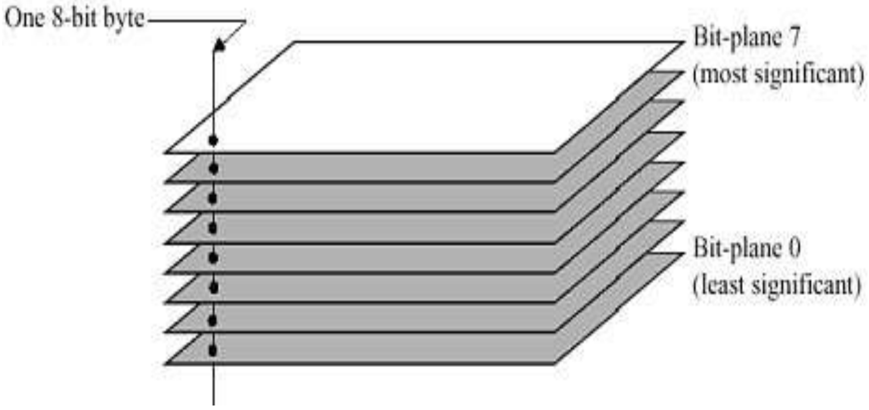


Figure 3.Converted frames

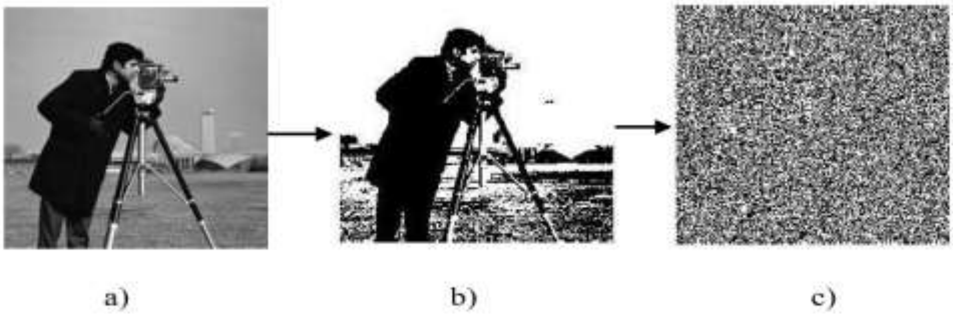


Figure 4. Image conversion (From original image to LSB image) a) Original image, b) Grey scale image, c) LSB image

4.2 Least significant bit

A traditional steganography technique user to hide data behind a "public" cover is the LSB algorithm. In computation, the least significant bit" (LSB) refers to the bit that sits at the unit's position in the binary representation.

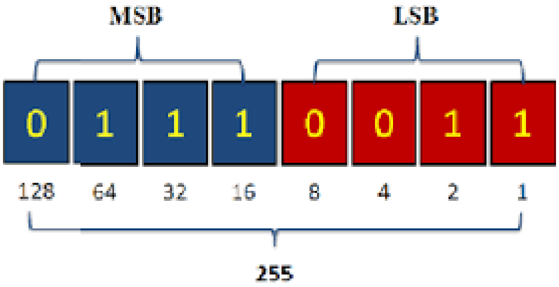


Figure 5. Representation of MSB and LSB

These bits in the binary code are of the lowest order. They have the least bearing on the binary number's total value. The LSBs of the file samples are changed in this implementation to correspond to the secret message's bits. As human perception is less sensitive to changes in the LSBs, this adjustment is modest and has little impact on the file quality.

The video file is first turned into frames. Often in a little video. At least 20-25 frames per second may be created for mp4 video. A frame in video is essentially a picture composed of a group of pixels values (color and intensity) organized in a matrix or list. Each pixel in the 24-bit map RGB picture contains 24bits of values, and each of the three-color channels has 8 bits. The RGB since it has a large amount of data and only requires on bit change per byte to conceal hidden messages. Each component consists of one byte, or eight bits, with the first bit being the most important. The least bit of each byte in a component is altered when secret information is concealed using the LSB method. Human imperceptibility is produced by replacing the least significant bit. We are all aware that the cover frame modification must be invisible in order for steganography to go undetected by the human eye is its main strength. We utilized a 24-bit picture to conceal bits of data in each pixel's color.

In its most basic version, the LSB algorithm substitutes one bit from the "secret" message for each LSB of each byte in the "carrier" data. In the diagram below, this idea is shown.

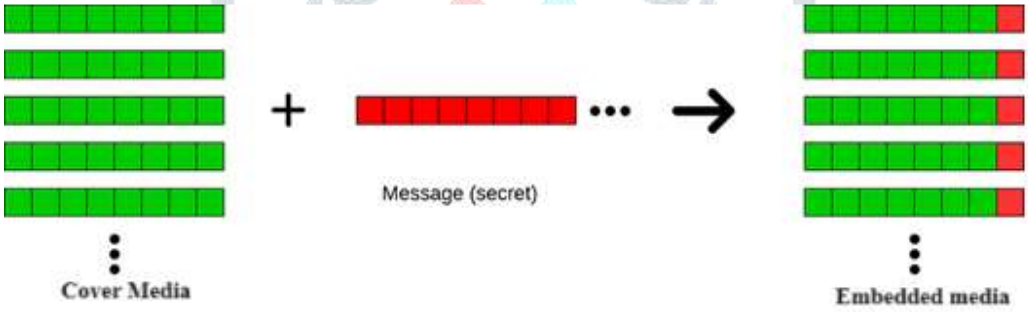


Figure 6. Encryption

Byte by byte, the transmitter 'embeds" the secret message bits onto the carrier data. While the receiver executes the "extraction" process by reading the LSB bits of each byte of incoming data, the receiver constructs the secret message in this way.

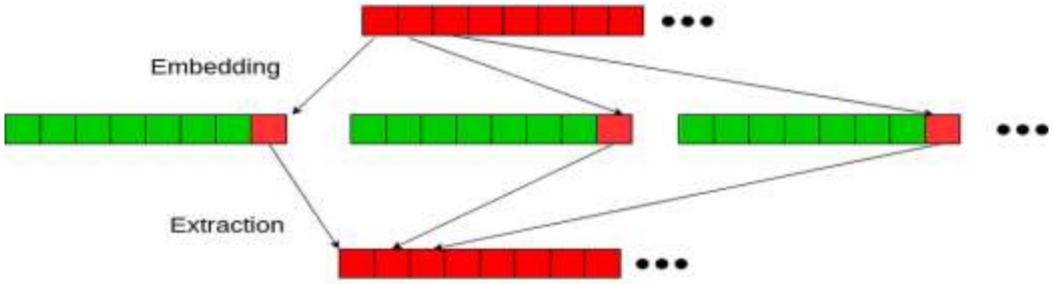


Figure 7. Encryption and Decryption

VI. RESULTS AND DISCUSSION

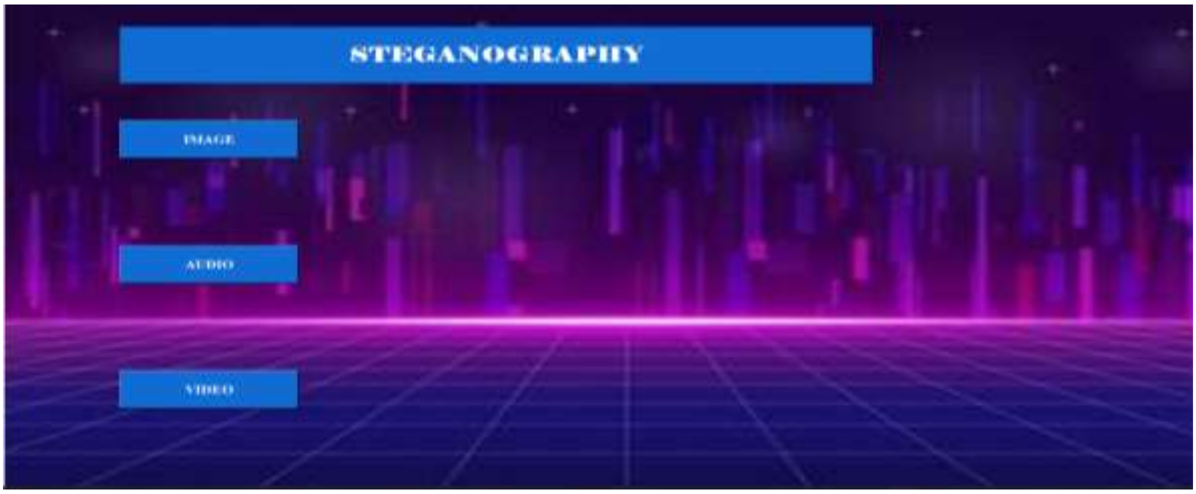
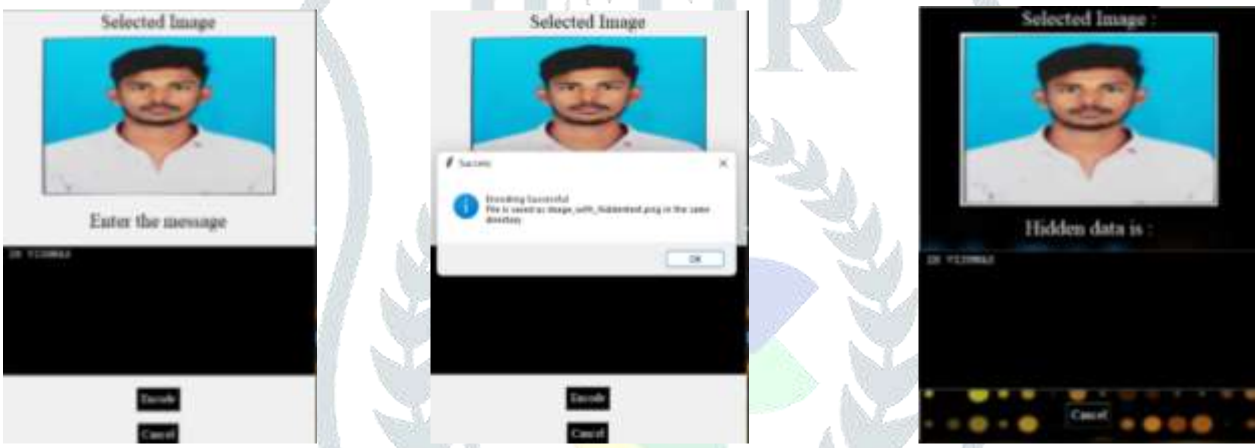


Figure 8. Home page

Figure 8 shows that home page of this project. There are three buttons on this home page. To encrypt secret data onto a cover media, the user has three choices to make. Depending on the cover media, the user can choose a certain option



IM VISHWAS

Success

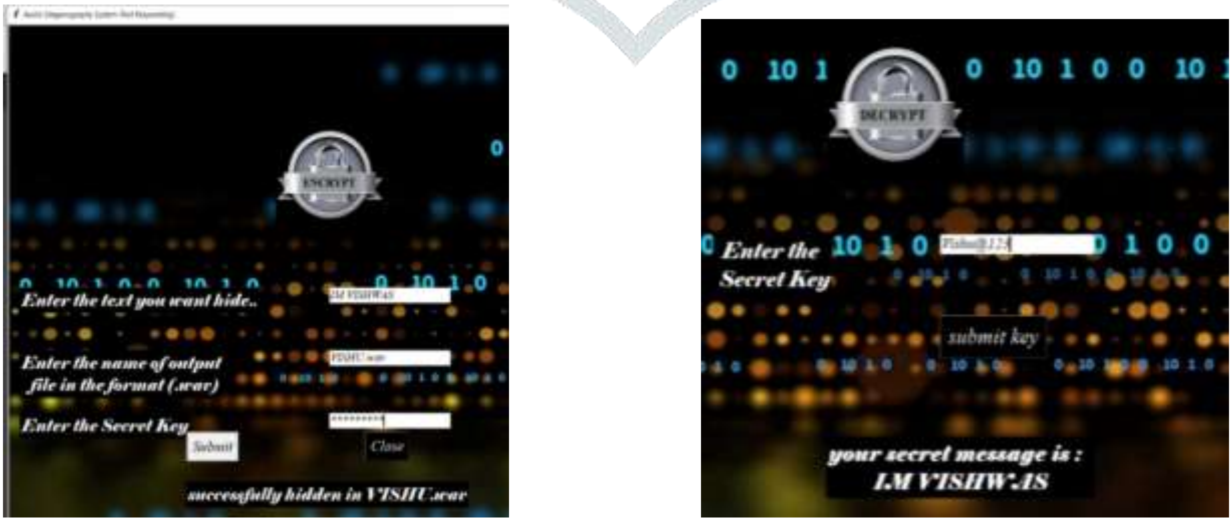
Encoding Successful
File is saved as image_with_hiddentext.png in the same directory

OK

IM VISHWAS

Figure 9: Encryption and decryption image as a carrier madia

The first step in image steganography is encryption, which involves selecting an image as a cover media. A data can be successfully encrypted and saved to the file directory by using the encryption button. After the encryption is completed, user proceeds to the next step. Decryption, which allows user to extract the hidden data by selecting the encrypted media.



Enter the text you want hide.. IM VISHWAS

Enter the name of output file in the format (.wav) VISHU.wav

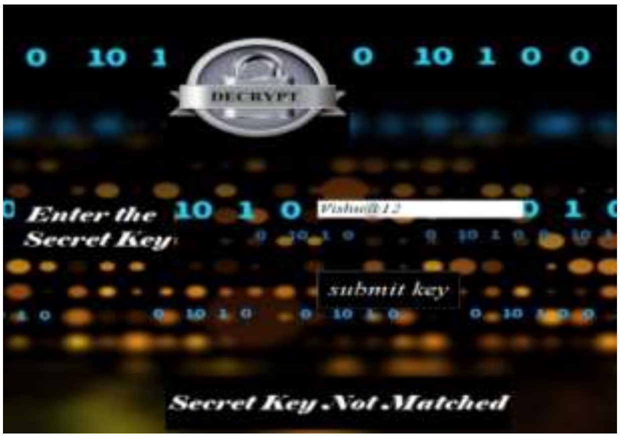
Enter the Secret Key *********

successfully hidden in VISHU.wav

Enter the Secret Key Vishu@123

your secret message is :
I.M VISHWAS

Figure 10. Encryption and decryption audio as a carrier madia

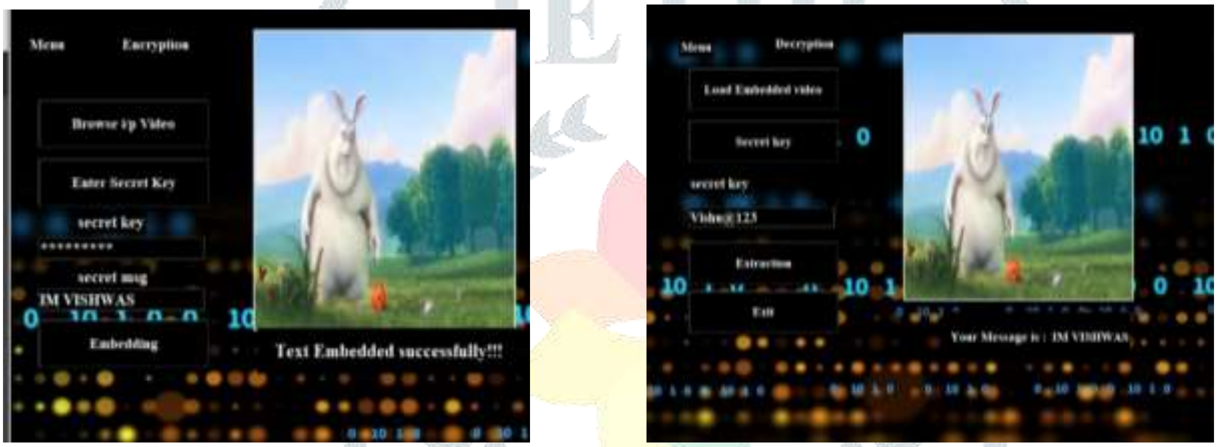


Vishu@12

Secret Key Not Matched

Figure 11. Wrong secret key

When choosing audio steganography, the user has the choice between encryption and decryption. The user must choose an audio clip that acts as cover media, enter any secret information they wish to keep private, enter a secret key, and then enter the encrypted file name they wish to save. A user can encrypt data by providing all the necessary information. Encrypting data can be decrypted by selecting the encrypted media and entering the correct secret key, user can successfully decrypt. User cannot decrypt without having the secret key. Secret key not matched when user entered a wrong secret key.



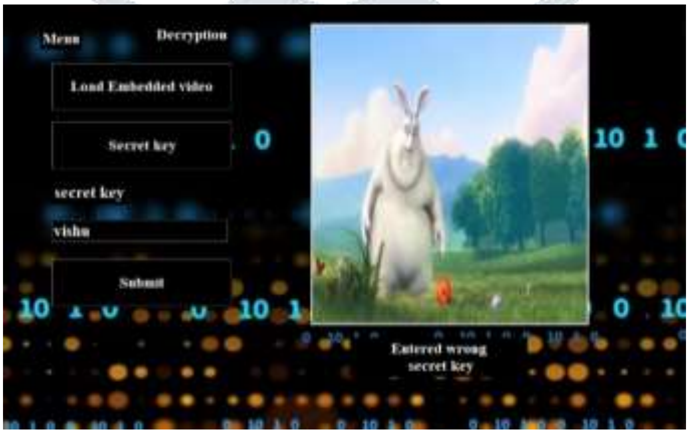
secret key
****
secret msg
IM VISHWAS

Text Embedded successfully!!!

secret key
Vishu@123

Your Message is : IM VISHWAS

Figure 12. Encryption and decryption video as a carrier madia



secret key
vishu

Entered wrong secret key

Figure 13. Wrong secret key

A video is used as the cover media in video steganography. Submit a secret key along with the data that the user wants to hide. User can encrypt a data on to video fiel by entering all the required information. By entering the secret key, the user may successfully decode from encrypted media. User cannot decrypt without having the secret key. Secret key not matched when user entered a wrong secret key.

VII. CONCLUSION

A cover file can be used to hide existing hidden information using the steganography technique. Here, we implemented a steganograophy technique for existing information in an cover file such as, aduio, video, image. Steganography is a technique covert communication. We have looked at the theroretical and practical boundaries of steaganography. In order to create a way of secure communication, we printed out the improvement of the audio, video, image steganography system employing LSB technique. When the message was embedded into the cover file, a stego-key was applied to the system. This project provides an secure communication through public channel using the steganography software. For a variety of application that demand adequate security, our technology is simple to use and very effective. As steganography- based authentication is handled by our system, unauthorized acces is effectively prevented. The over all goal of our project is to improve the securoty of user and reciever authentication. With several technologies advancements and a dedication to user ecurity and privacy, this system has the capacity to give a smooth and safe user experience.

References

[1] Junqui Wu, Bolin Chen, Weiqi Luo and Yanmei Fang, “Audio Steganography Based on Iterative Adversarial Attacks against Convolutional Neural Networks”, IEEE,2019.

[2] Yunzhao Yang, Xianfeng Zhao, Xiaowei Yi, and Haibo Yu, “An Adaptive Double-layered Embedding Scheme for MP3 Steganography”, IEEE, 2020.

[3] Songbin Li, Yizhen Jia and C.-C. Jay Kuo, “Steganalysis of QIM Steganography in Low-Bit-Rate Speech Signals”, IEEE,2017.

[4] Houngguo Zhao, Yunxia Liu, Yonghao wang, SI Liu and Cong Feng, “A Video Steganography Method Based on Transform Block Decision for H.265/HEVC”, IEEE, VOL.9, pp.55506-55521,2021.

[5] Jie Wang, Xiaoqing Jia, Xiangui Kang and Yun-qing, “A Cover Selection HEVC Video Steganography Based on Intra Prediction Mode”, IEEE, vol.7, pp.119393-119402,2019.

[6] Richa Khare, “Video Steganography by LSB Technique using Neural Network”, 2014 Sixth International Conference on Computational Intelligence and Communication Networks, 2014.

[7] Lindawati, “Steganography Implementation on Android Smartphone Using the LSB (Least Significant Bit) to MP3 and WAV Audio” IEEE,2017

[8] Fauzi Adi Rafrastara and Raka Prahasini, “Image Steganography using Inverted LSB based on 2nd, 3rd and 4th LSB pattern”, 2019 International Conference on Information and Communications Technology (ICOIACT),2019.

[9] Omar Elharrouss, Noor Almaadeed, Somaya Al-maadeed, “An image steganography approach based on k-least significant bits (k-LSB)”, IEEE, 2020.

[10] S. M. Alwahbani and H. T. Elshoush, ‘‘Hybrid audio steganography and cryptography method based on high least significant bit (LSB) layers and one-time pad—A novel approach,’’ in Dr. Yaxin Bi Editor. Studies in Computational Studies, vol. 751. Cham, Switzerland: Springer, Jan. 2018, pp. 431–453.

[11] D. R. I. M. Setiadi and J. Jumanto, "An Enhanced LSB-Image Steganography Using the Hybrid Canny-Sobel Edge Detection," Cybernetics and Information Technologies, vol. 18, no. 2, pp. 74-88, 2018.

[12] D. R. I. M. Setiadi, "Payload Enhancement on Least Significant Bit Image Steganography Using Edge Area Dilation," International Journal of Electronics and Telecommunications, vol. 65, no. 2, pp. 295-255, 2019.

[13] A. Kumar and K. K. KM, ‘‘Enhanced LSB algorithm for stegano communication,’’ J. Web Develop. Web Designing, vol. 1, no. 3, 2016.

[14] S. M. Alwahbani and H. T. Elshoush, ‘‘Chaos-based audio steganography and cryptography using LSB method and one-time pad,’’ in Proc. SAI Intell. Syst. Conf., Cham, Switzerland: Springer. Sep. 2016, pp. 755–768.

[15] T. K. Hazra, M. Haldar, and M. K. Mukherjee and A Chakraborty, ‘‘A survey on different techniques for covert communication using steganography,’’ IOSR J. Comput. Eng. (IOSR-JCE), vol. 20, no. 2, pp. 42–52, Apr. 2018.

[16] Application Guide for Objective Quality Measurement Based on Recommendation, document Recommendation P ITUt ITUt 862.3:862, 2005.

[17] R. D. Ra and D. Pugazhenthi, ‘‘Ideal sampling rate to reduce distortion in audio steganography,’’ Proc. Comput. Sci., vol. 85, pp. 418–424, Jul. 2016.

[18] F. Djebbar, B. Ayad, K. A. Meraim, and H. Hamam, ‘‘Comparative study of digital audio steganography techniques,’’ EURASIP J. Audio, Speech, Music Process., vol. 2012, no. 1, p. 25, Dec. 2012.

[19] J. Chaharlang, M. Mosleh, and S. Rasouli-Heikalabad, ‘‘A novel quantum steganography-steganalysis system for audio signals,’’ Multimedia Tools Appl., vol. 79, nos. 25–26, pp. 17551–17577, Feb. 2020.

[20] J. Chaharlang, M. Mosleh, and S. R. Heikalabad, ‘‘A novel quantum audio steganography–steganalysis approach using LSFQ-based embedding and QKNN-based classifier,’’ Circuits, Syst., Signal Process., vol. 39, no. 8, pp. 3925–3957, Jan. 2020.

[21] Jiang, G. Yang, and W. Chen, ‘‘A cabac based hevc video steganography algorithm without bitrate increase,’’ J. Comput. Inf. Syst., vol. 11, no. 6, pp. 2121–2130, Mar. 2015.

[22] M. M. Sadek, A. S. Khalifa, and M. G. Mostafa, ‘‘Video steganography: A comprehensive review,’’ Multimedia Tools Appl., vol. 74, no. 17, pp. 7063–7094, 2015.