Multilayer Security in protecting and hiding data and videos Using Cryptography & Steganography

[1]D. Sowmya, [2]Y. Supriya Reddy, [3]P. Srilakshmi., [4]M. Anand

[1,2,3,4]Assistant Professor,Department of Computer Science and Engineering,G Pulla Reddy Engineering College, Kurnool, India.

ABSTRACT:Data hiding is the process of incorporating information into a source of data without modifying its perceptual quality. Steganography is the art and science of creating concealed communications by blending information with other information so that only the sender and recipient of the message are aware of its presence. Here, the Least Significant Bit (LSB) algorithm is used to implement text steganography, image steganography, audio steganography by LSB Modification using Advanced Encryption Standards, and video steganography by KSA and PRGA algorithms. The secret message is first encrypted using the Cryptography RC4 algorithm before being embedded in the image, text, audio, and video files. Using the proper decoding technique, one can extract the personal text from the stego file and decrypt the hidden message. Steganography uses sophisticated software to conceal the data from a third party. Steganography and cryptography can be used together to securely hide the secret message.

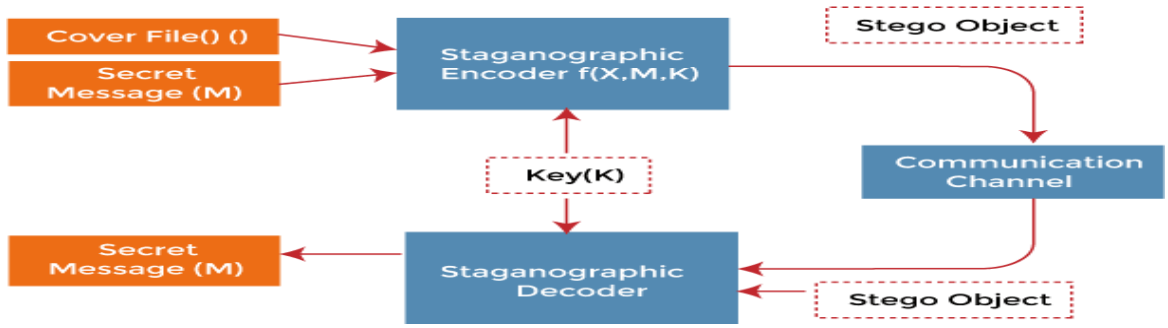
Keywords: Data hiding, Python, Least Significant Bit Algorithm, Text Steganography, Image Steganography, Audio Steganography, Video Steganography.

1. INTRODUCTION

While sending and receiving personal information safe, we must be aware of the rising Internet usage. The data can be transformed using various methods, and the generated data can be comprehended if the original form can be recovered. This technique is referred known as "encryption." A significant disadvantage of this strategy is that the existence of the data is not concealed. If someone gives the encrypted data enough time, it can be decrypted and returned to its original state.By hiding data under a cover material and rendering it unreadable to others via the "steganography" approach, this problem has previously been overcome. The amount of data that can be concealed, how clear the message is, and how sturdy it is all affect the cover media's attributes. The system for data concealment described in this research is based on several image-hiding techniques and algorithms.

A sink file, an image file, and a container image are where we keep the data. The primary objective is to boost security while utilizing less storage using steganography techniques.

Figure 1: Model for Steganography



Greek roots give steganography, which means "covered or hidden writing," its name. Steganography is the art and science of hiding a message inside another message so that only the intended recipient can find it without raising suspicion in the eyes of others. By converting data into a format unwanted users cannot comprehend, information can be kept secure using cryptography. Information is intended to be unreadable by outside parties using data encryption. On the other hand, steganography tries to hide information from a third party. While cryptography scrambles a message to conceal its contents, steganography only conceals the existence of a message. Because criminals can identify and react to the presence of encrypted communications, simply encrypting the transmission is insufficient. However, when information concealing is utilized, the message cannot be guessed because it is done surreptitiously, even if an eavesdropper listens to the communicated object. Because the text is unintelligible, encryption has the disadvantage that a third party can always decipher what is being spoken. This limitation is overcome by steganography, which wraps the message in a visually appealing cover.

Contributions of The Paper

Most systems in use today use cryptography techniques. Something concealed in a file is known to the unauthorized person according to cryptography techniques. As a result, the data could be more secure. Data is kept secret by steganography from everyone save the sender and receiver. The suggested approach combines steganography and encryption to transport data more securely.We encrypt the personal data using the RC4 cryptography technique, and for text files, we utilize ZWC, LSB, and modified LSB; for video files, we employ advanced LSB steganography algorithms. Steganography is a popular and easy technique for hiding data in photographs. The embedding potential of steganography for audio and video is enormous.

The following are some of the suggested system's benefits:

1. Unlike previous methods, steganography successfully masks communications so no one can see them. In countries where encryption is prohibited, sending an easily decipherable encrypted message will raise suspicion and could be harmful.
2. Steganography is an encryption method that protects messages' content and the relationships between sender and recipient.
3. It is advantageous to establish covert communication channels and transfer information surreptitiously using text files due to steganography's security, versatility, and robustness.
4. If you keep an encrypted copy of a file containing sensitive information on the server, you don't have to be concerned about unauthorized individuals accessing the data.

Highlights:

1. In steganography, only the sender and recipient may see or hear secret messages encoded in text, image, video, or audio files.
2. Information is encrypted in cryptography.
3. The data is safer when Steganography and Cryptography are used together.
4. Data transmissions are done more securely and straightforwardly.

Motivation: The development of Steganography and cryptographic techniques is reportedly driven by the communication between its members and between members of the military, intelligence agents, or corporate agents to conceal secret messages or engage in espionage. Combining cryptography and steganography's primary goal is to prevent the detection of the transmission of personal information. If hackers discover any modifications in the delivered message, this goal—planned to achieve the security of the secret messages—will be achieved if suspicion is aroused. This observer will make an effort to decipher the message's

confidential information. Because of this, the project's main motivation is to employ a multimedia file to transmit a hidden message or establish the veracity of some data.

Problemdefinition: The project addresses the problem of internet data transmission security. The basic idea is how to communicate with a recipient covertly. The science of steganography and cryptography answers this question. Using steganography and cryptography, information can be hidden in carriers like photos, audio files, text files, movies, and data transmissions.

Objective of Thepaper: This research primarily focuses on the security challenges of sending data over a network utilizing steganographic and cryptographic approaches. The project's main objective is to develop a security tool based on message-hibernation techniques. stego-media that is intended to be undetectable by humans to avoid concerns about a concealed message.

Limitations of Thepaper: One of the project's drawbacks may be how criminal hackers exploit steganography to damage data files or hide malware in otherwise benign documents. For instance, hackers can use PowerShell and BASH scripts to conduct automated assaults utilizing Word and Excel documents. When a careless, credulous user opens

one of those papers, the secret script is activated, and havoc ensues. The other limitations cover attacks on images, including dilution, nose, contrast change, and more. Caution is advised because the visual distortion may become obvious if many LSB bits in pixels are modified. Care must be exercised since audio noise may become audible if too many LSB bits in frames are altered.

2. LITERATURE SURVEY

Many organizations rely heavily on electronic communication. A lot of the information shared every day needs to be kept private. Information, including financial reports, personnel information, and medical records, must be shared to protect its integrity and confidentiality. This is prudent from a commercial standpoint and might even be covered by laws like the Health Insurance Portability and Accountability Act (HIPAA). Much of this information is transmitted via the open Internet and could be read by third parties, as in an e-mail or instant messaging (IM), which complicates unsecured communication.

In Yuanjin et al.g et al., Luo introduced the idea of a designated cover image for embedding secret information while transmitting it directly through its attributes, such as pixel brightness value, color, texture, edge, contour, and high-level semantics. Enhancing the robustness of steganography and detecting steganalysis[1]. Three innovative approaches to text steganography were presented in the paper by FitraChairil Akbar et al. The number of lines in a text document is directly proportional to the number of characters that can be introduced using the word-shift approach.The word-shift technique's character limit is directly related to the number of lines in a text document, according to key studies. To associatively conceal a few pieces of information, much overhead was required [2].

The proposed method in this work is illustrated in Noor Alhuda, F et al., along with its main parts. It can have good payload, strong protection, and maintain image quality for a reasonable price. This graphic representation of the framework further clarifies the invention of the methodology because readers can better visualise and comprehend our procedure [3].Rohit Kumar Yadav et al. proposed a plan to create a more reliable and secure means of

information exchange. Cryptography and steganography are coupled to achieve the necessary robustness and security. Using a combination of encryption and steganography, the necessary robustness and security is achieved [4].

A novel lossless centralized difference expansion approach is proposed byMadhabanandaDasa et al. Each block's payload is variable and based on its type. Depending on the kind, different amounts of data are embedded in each block as part of the dynamic embedding technique. The proposed method offers excellent concealing potential. Although the distortion of the stego image is less than that of earlier methods, it could yet be improved [5].

Hussein AbdulameerAbdulkadhim and colleagues suggest that the transmitter channel's cover message be used to conceal the secret audio. The selected methodologies are the Least Significant Bits (LSB) algorithm and the 4D grid. GMWH's chaotic system's effective key will assist security, robustness, and difficulty in detecting attackers and hackers. Using a pseudorandom number generator to distribute the message randomly throughout the sound file is a more complicated strategy [6].

The author incorporated the proposed Mid Position Value (MPV) technique in Nisreen I. R. Yassin et al. The idea of the centre position and its associated values for each of the dwelling pixels are used in this process. According to the number of coefficients in the category and the message size, the number of LSBs taken from each category was displayed [7].

[8] To discover edge pixels and hide data in the detected edges, Phalguna Gupta et al. applied the distribution of the proposed data detection algorithm. Due to the anomalies caused by LSB replacement, this approach can withstand visual, structural, and non-structural attacks.
The authors of Nisreen I. R. Yassin et al. suggest a method for concealing data. In order to prevent any eavesdropper from noticing any modifications in the original material, it seeks to conceal data. The LH, HL, and HH high-frequency subbands contain information that improves robustness and guarantees visual quality. According to the quantity of coefficients and the size of the message, the number of LSBs from each category was displayed [9].In Maisa's Abid Ali K et al.'s study, we proposed image steganography using the least significant bit. Secret map techniques are carried out by applying 3D chaotic maps, specifically 3D Chebyshev and 3D logistic maps, to obtain high security. The secret keys for this algorithm are likewise extremely sensitive [10].

Ahmed Sabah Ahmed Al-Jumail et al.'s paper aims to suggest an LSB and Deflate compression method combo for image steganography. Both LZ77 and Huffman coding was used in the proposed Deflate method. After the message text was compressed, LSB was used to embed the reader into the cover image [11].

In Mohammed Majid Msallam et al.'s section, the suggested method involves restoring a byte’s low-order bit (LSB) using an M's bit. This method works well for the steganography of images. The LSB (Least Significant Byte) technique conceals data within the graphics. Since the stego-key relies on the cover image to conceal a secret message, the results show greater robustness in steganography—less capacity and greater complexity [12].

In AbdulkaremAlmawgani et al., an embedding algorithm and an extraction algorithm comprise the suggested solution. The embedding algorithm separates the cover image into nxn pixel blocks that don't overlap. The HDWT makes the stego image more secure by

distributing the secret info among all pixels. LZW's high computational efficiency [13] is a result of this.Min-Allah suggested quantum steganography in Nasro et al., which is essential for encrypting carrier messages with sensitive information utilizing quantum computing techniques. From the standpoint of security, embedding effectiveness and capacity, imperceptibility, and time complexity, the quantum variation of steganography performs better than its classical equivalent [14].

To conceal the secret and the players during the transmission phase, Apurva Sankpall et al. introduced a new palette-grounded steganography technique that employs a texture with LSB and a natural-image-grounded VSS scheme (NVSS scheme). Also suggested were potential strategies for keeping the information secret to lessen the transmission hazard issue for the share [15].

Nitin Arora et al proposed a steganography technique for embedding the data in medically scanned images. Both the patient's data and the diagnosis are classified information. The algorithm saves the diagnosis and patient data, enabling accurate and quick patient treatment [16].

An LSB-based method for image steganography was proposed by Mohsen Rezvani et al. and is called LSB matching revisited. This technique uses a form of coding to enhance steganography. With this technique, a single alteration can conceal two bits of the secret message in each of two pixels. However, this approach needs guidance for concealing a message with several bits [17].

A brand-new method of symmetric key-based picture concealing was put out by S. Rajendran et al.Using a 1D logistic map, pseudo-random keys are created, and those keys are utilised to select at random the pixel position of the cover image to conceal the secret image. The choice of pixel position in the cover image is the primary security component of the projected technique. The suggested approach offers an effective level of security, according to the result analysis, which compares Peak Signal Noise Ratio (PSNR) and Mean Square Error (MSE) measurements [18].

A brand-new challenge of spotting heterogeneous parallel steganography (HPS) on streaming media was put forth by Yuting Hu et al. This job involves using various orthogonal steganographic techniques to identify the confidential messages concealed in streaming media frames [19].

To reliably identify audio steganography techniques in quantum communication networks, Javad Chaharlang et al. suggested a novel quantum steganography-steganalysis system for digital audio signals. The proposed model is divided into two parts: steganography and steganalysis. In the steganography part, the embedding operation is carried out within the Least Significant Fractional Qubit (LSFQ) of the amplitude information of the audio signal samples tominimise the effects of the embedding process and increase the Signal Noise Ratio (SNR) [20].

According to a theory by Ashok et al., steganography can be compared to cryptography. Both have been employed as methods of information protection throughout recorded history. While the two technologies' goals are different, they sometimes appear to merge. To prevent messages from being intercepted and decoded, cryptographic procedures "scramble" the messages. Steganography essentially "camouflages" a message to obscure its content and

make it appear "invisible," so hiding the fact that a message is even being delivered [21].

3. PROPOSED SYSTEM

RC4 Algorithm using Cryptography

When we performed video steganography, we integrated cryptography and steganography. To encrypt the message, we use two components. We encrypt plaintext using the RC4 Encryption Algorithm to create cipher text. RC4 is a stream cipher that uses keys of various lengths. This algorithm encrypts one byte at a time.

StepsInvolvedintheProposed Work

3.1 TextSteganographyviaEngagingUnicodeStandardEncoding: It is necessary to encode the message that must be inserted, embed it, and then extract the secret message from the produced stego file. Consequently, the hidden message's cover file is initially a text file. The secret message is then requested to be hidden from the user. The length of the message determines whetherit may be incorporated in the selected cover file. If specific requirements are satisfied, the concealed message is embedded.

EncodingSecretMessage: Each character whose ASCII value is retrieved is included in this. The ASCII value of the character is increased by 48 if it has an ASCII value between 32 and 64. If the ASCII value is outside of the range of 32 to 64, it is reduced by 48. And binary format is applied to the outcome. This is done to convert every message character to the necessary 8-bit format.

The binary representation that results is then XORed with the binary representation of '10101010', which has a decimal equivalent of 170. the outcome of the XOR operation with padding bits attached If the character's XOR value is between 32 and 64, the prefix '0011' is added; otherwise, the prefix '0110' is added, converting the character to a 12-bit representation format.

Consider the character "4" as an example, whose ASCII value is less than or equal to 64. Its conversion into 8 bits is followed by an XOR operation between the resulting binary and "1010101010," with the padding bits "0011" added at the start. Figure 4 below displays each of these procedures.

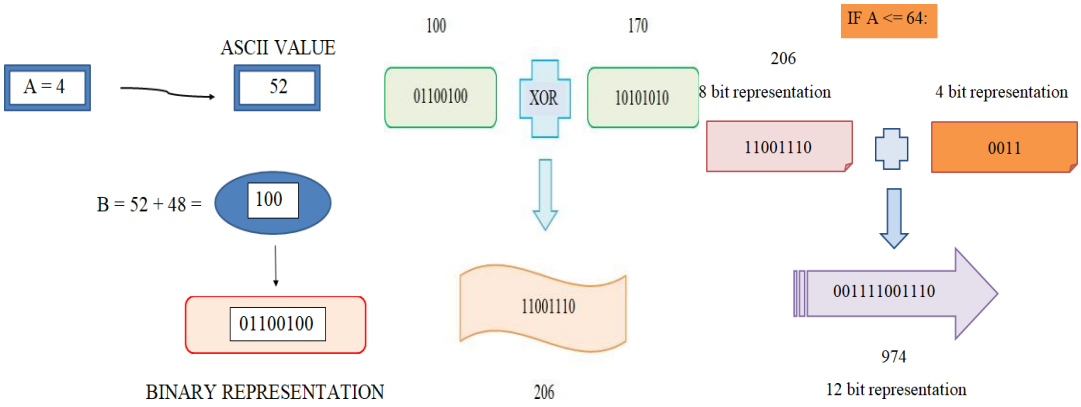


Figure 2:EncodingWhenASCIILess Than64

Another illustration uses the character 'U' with an ASCII value larger than 64. The character's 8-bit binary format is then combined with '10101010', which has a decimal equivalent of 170, via an XOR operation. As illustrated in Figure 5 below, the obtained outcome '0110' will be added at the beginning.

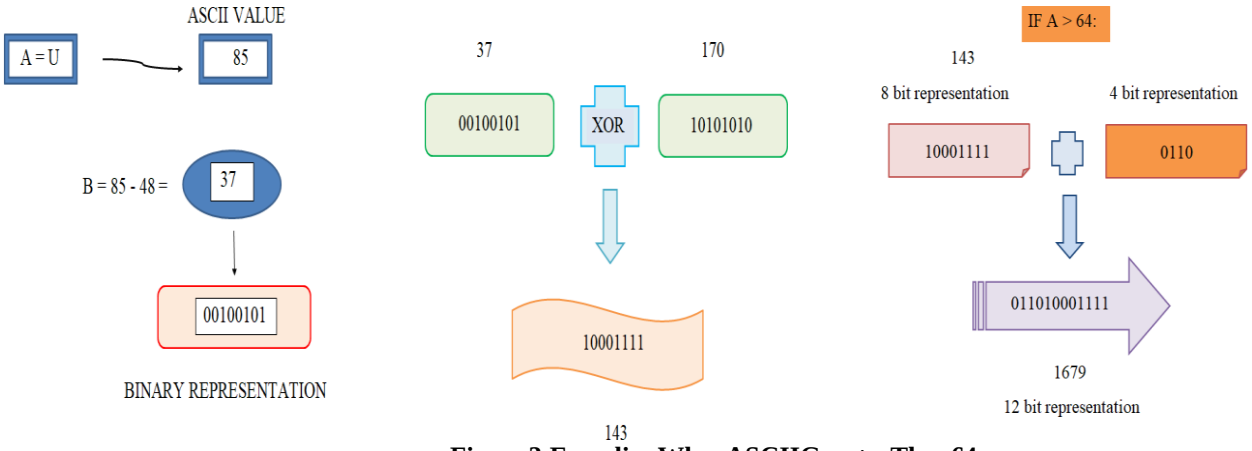


Figure 3:EncodingWhenASCIIGreaterThan64

A delimiter is then inserted to signal the end of the secret message once each character of the secret message to be embedded has been encoded into the necessary 12-bit binary format. The endpoint in this case serves as '111111111111', the delimiter utilized.

EncodingSecretMessage: The 12-bit representation of each character now has an analogous zero-width character in place of every second bit. After a word, every character in the cover text is obscured. So, in this case, we employ mapping the particular 2 bits to the particular Zero width character. So, if the first two bits are 00, we map to a Zero Width Non-Joiner, which is 0x200C. Likewise, the Pop Directional Formatting code 0x202C was assigned to 1. If the bit pair is 11, it will be translated to 0x202D, a Left-To-Right Override ZWC. Finally, if it is 10, the mapping is 0x200E Left-To-Right Mark Zero Width Character.The maximum number of characters that can be embedded equals the total number of words divided by six because it takes six zero-width characters to embed each character. To map these Zero width characters, a dictionary is utilised. After that, the cover file is opened, the required Zero width characters are added to the text following the term, and the required stego file is generated.

Decoding From TextStego File: Read the text stego file in this stage to extract the message. Then, based on how they were mapped in the previous phase, the text file is searched for zero-width characters by decoding them into the proper two bits. Until the delimiter is found, the pertinent bits are stored. After identifying the delimiter, the first four bits are examined to determine whether the character's ASCII value was less than 64 or in any other situation. Based on that, the next 8 characters are then decoded.For instance, ASCII was less than or equal to 64 if the first four bits were 0011. Therefore, between that 8-bit and "10101010," an XOR operation is carried out, and the outcome is reduced by 48. This exposes a character's true nature. Take another example where the first four bits are "0110," signifying that ASCII was more than 64. So, between that 8-bit and "10101010," an XOR operation is carried out, and the outcome is then multiplied by 48. This procedure is repeated until the delimiter is found. This presents the character exactly as is. In this way, the hidden message is recovered.

3.2 Image Steganography Using Least Significant Bit Algorithm (LSB): It is necessary to encode the message that must be inserted, embed it, and then extract the secret message from the produced stego file. As a result, the secret message's cover file begins as an image file. The secret message is then requested to be hidden from the user. The length of the message determines whether it may be incorporated in the selected cover file. A stego file is created and the secret message is incorporated into the cover image if all conditions are satisfied.

EncodingSecretMessage: Suppose the length of the secret message is within the embedding capacity of the user-provided input picture. In that case, the delimiter "***" is appended at the end and the message is then resumed. Here, each secret message character is transformed into an 8-bit binary representation. The ASCII value of the character is retrieved using the ord() method. If necessary, the format() method converts the character to 8 bits by padding the MSB side with zeroes to create an 8-bit binary representation of the character.

EmbeddingSecretMessage: Because each pixel has three channels—red, green, and blue values—it is possible to calculate an image's embedding capacity using its pixel count. So, using the shape() technique, it is possible to locate the height kept at picture index '0'. The image's shape() and width are stored at index '1' of the image. Shape(). The amount of pixels is equal to the height and width of the input image. The embedding capacity is (Number of Pixels * 3 / 8). Therefore, the secret message is encoded and embedded if its length falls within this capacity for embedding; otherwise, a message is presented to the user asking for either a large-size image or a reduced size image.

As a result, we employ the Least Significant Bit Algorithm to transform each pixel's red, green, and blue values into the appropriate 8-bit binary values. The least significant bit of the red value is replaced by the first data binary bit, the least significant bit of the green value is replaced by the second data binary bit, and the least significant bit of the blue value is replaced by the third data binary bit. At least significant positions for the red, green, and blue values can then be added in each of the three data pixels. The stego file generates the user-supplied name, and the cv2.im write () method is used to update the pixel values.

DecodingFromImageStegoFileIn this phase, read the picture stego file to extract the message. This is followed by accessing every pixel in the image. For each pixel, the least significant bits at red, green, and blue values are extracted into a variable and the procedure is repeated. After then, the final eight bits are collected and transformed into characters. This is the original character of the hidden message. Until the delimiter "***" is found, this process is repeated. The covert message is thus made known.

3.3 AudioSteganographyUsingModifiedLSB

The created audio stego file is encoded, embedded, and decoded before the secret message is extracted from it. As a result, the cover file for the concealed message is initially a wave xtension audio file. The secret message is then requested to be hidden from the user.

EncodingSecretMessage

The location where the delimiter "***" should be added is then determined using the user's input to hide the message in the audio cover file. This section transforms each character in the hidden message into an 8-bit binary representation. The ASCII value of the character is retrieved using the ord() method. The format() function is then used to transform the character to an 8-bit value, with any necessary padding zeros being added to the MSB side to convert the binary bits to an 8-bit number.

EmbeddingSecretMessage: Using the user-provided audio cover file and the wave.open() method of the wave library in reading mode. The quantity of audio frames is then obtained using the wave's get nframes() method. All of these frames are also read, converted to lists of frames, and then, with the help of the bytearray() method, converted to byte arrays. The embedding capacity equals the total number of frames / 8, so each character would require 8 frames to be embedded.

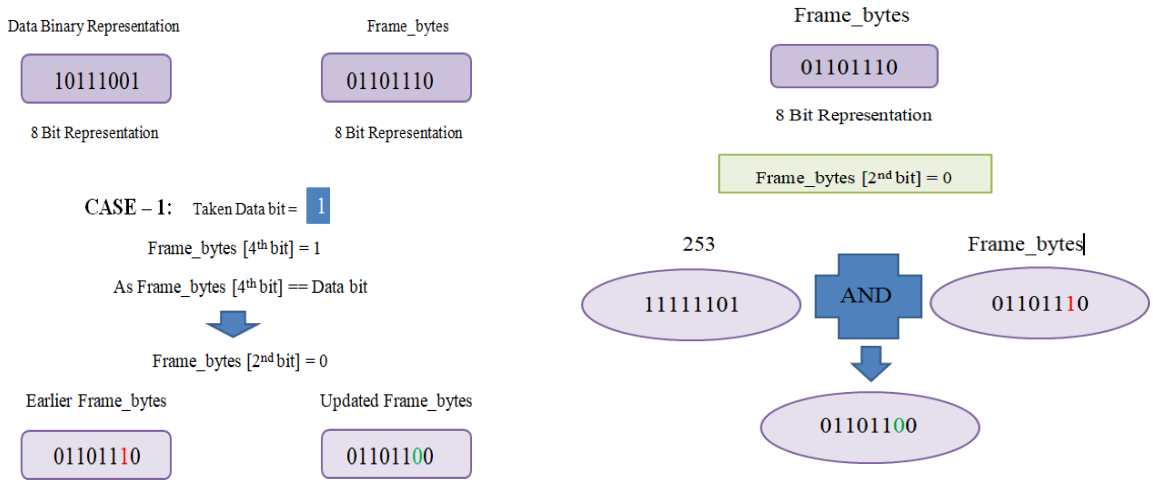


Figure 4: Embedding DataBit Example-1

Currently, a frame can only store one bit. The embedded data bit is compared to the fourth bit of a frame. If the data bit and fourth-bit match, a "0" is added to the frame's second bit. As a result, this AND operation is carried out between the bytes of the current frame and the number "11111101," which has a decimal value of 253. Figure 6 gives a sample of the aforementioned process.

The data bit is embedded at the first bit of the frame byte if it is not the same as the fourth bit, and '1' is inserted at the second bit if it is not. To accomplish this, an AND operation is performed on the current frame of bytes and "11111101," which has a decimal equivalent of 253, and an OR operation is performed on the outcomes of the OR operation and "00000010," which has a decimal equivalent of 2. The adjusted byte frame and "11111110," which has the decimal equivalent of 254 (or the data bit), are combined in an AND operation to place the data bit at the first bit in the frame.The data bit to be encoded is then put between this outcome and the OR operation. This operation is repeated until all of the data bits have been encoded. An illustration of the aforementioned procedure is shown in Figure 7.

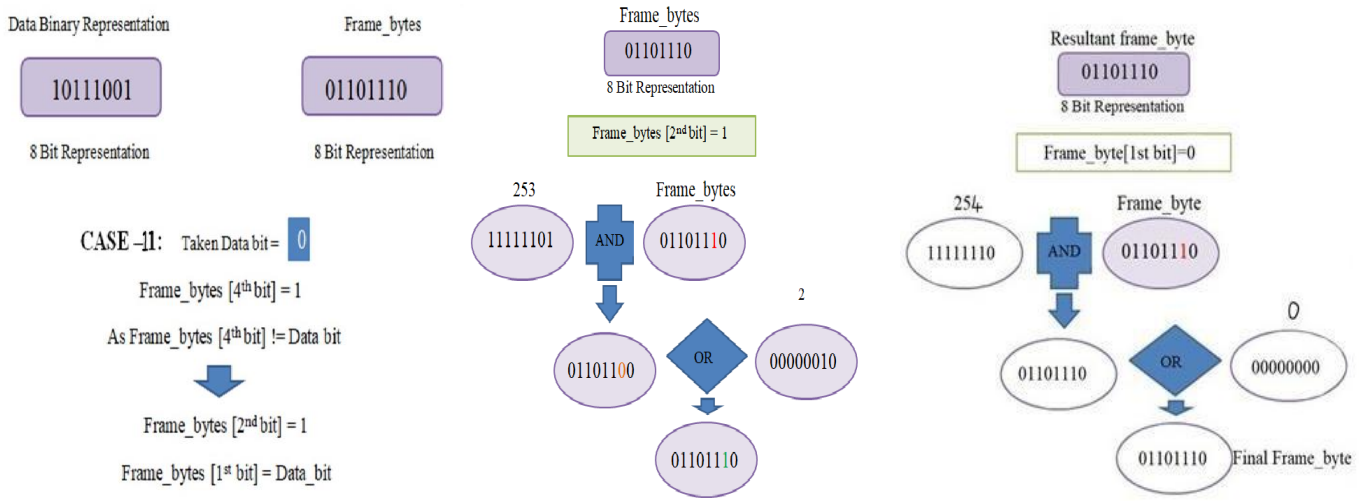


Figure 5:Embedding Data BitExample-2

Decoding From Audio Stego File: Read the audio stego file in this stage to extract the message. Then, in that audio, every frame is read using the read frames() technique, which are transformed into byte arrays using the bytearray() method. These byte frames are then transformed into an 8-bit binary representation using the zfill() function.Next, frame by frame, the second bit of the frame bytes is examined. If the databit is 0, the frame byte's fourth bit is the databit. If the condbit of the frame bytes is 1, the databit is otherwise the first bit of the frame byte. Using the chr() function, for instance, these data bits are removed, grouped as 8, and their ASCII values are then converted into characters. This process is repeated until the delimiter "***" is found. The hidden message is thus disclosed in this way.

3.4 Video SteganographyUsingKSA & PRGA

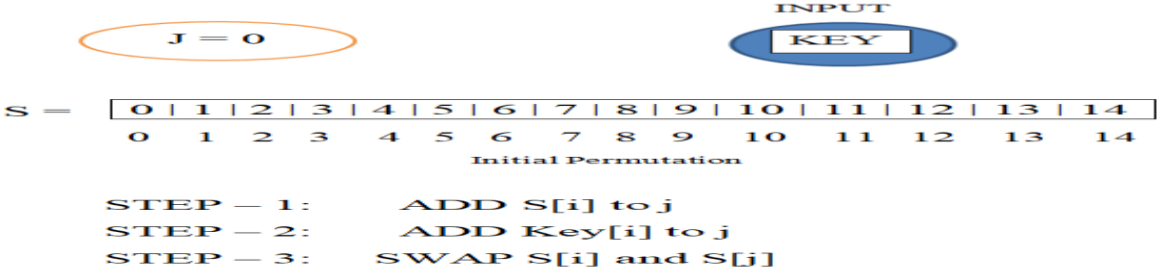
A video file and secret text are the inputs for video steganography.

Encryption:

The secret text is first encrypted using the RC4 cryptography technique, and then the user enters a key to encrypt the data. After that, the data is integrated into the video file. The user is then prompted for the frame number they want to embed the data once the number of frames is calculated during the embedding procedure. After receiving user input, a modified LSB technique embeds the secret data into the video file. The file that is now open is called Stego file.

For encryption and decryption, it consists of two main sections: -

KSA (Key-Scheduling Algorithm)-In ascending order, values between 0 and 255 are assigned to the entries of a list S with 256 items. We convert a key into its corresponding ascii code after requesting it from the user. To create a new permutation for the entire keystream depending on the key, S(i) and S(j) are switched, and the variable j is given the formula j=(j+S[i]+key[i%key length]) mod 256. A permutation of 0, 1, 2,..., 255 is S[].



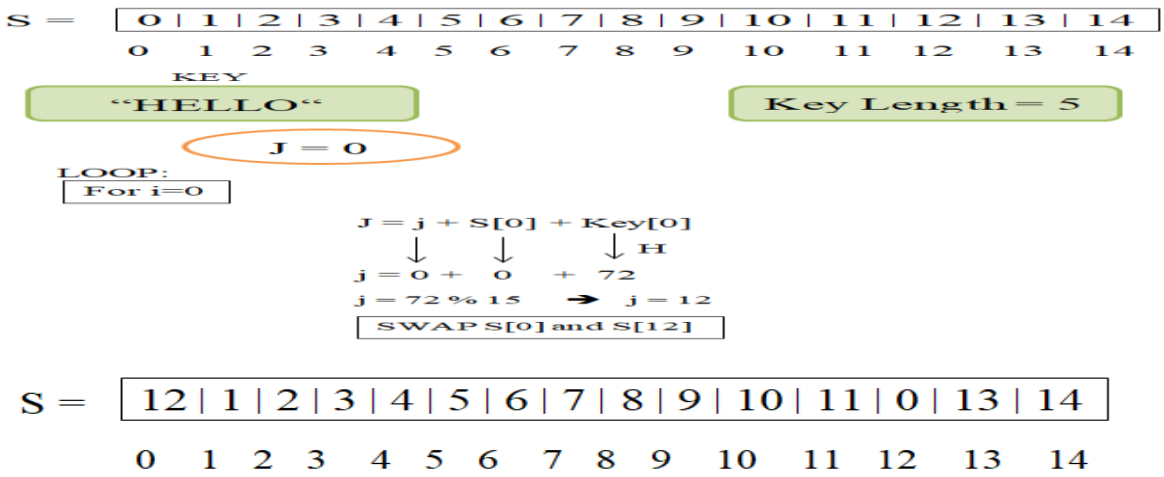


Figure 6: KSA (Key-Scheduling Algorithm)

2. **PRGA(Pseudo-random generation Algorithm (Stream Generation))**- A loop is now initiated to produce a keystream byte that is the same length as the input plaintext using the plaintext's length. We now start with i=0 and j=0, raising I by 1 while increasing mod by 256. We switch the values again, add S[i] to j, and mod j by 256. To get a keystream that is the same length as plaintext, record the bytes in the keystream that match S[(S[i]+S[j] mod 256]. We will now XOR the plaintext and keystream to create the final cipher.

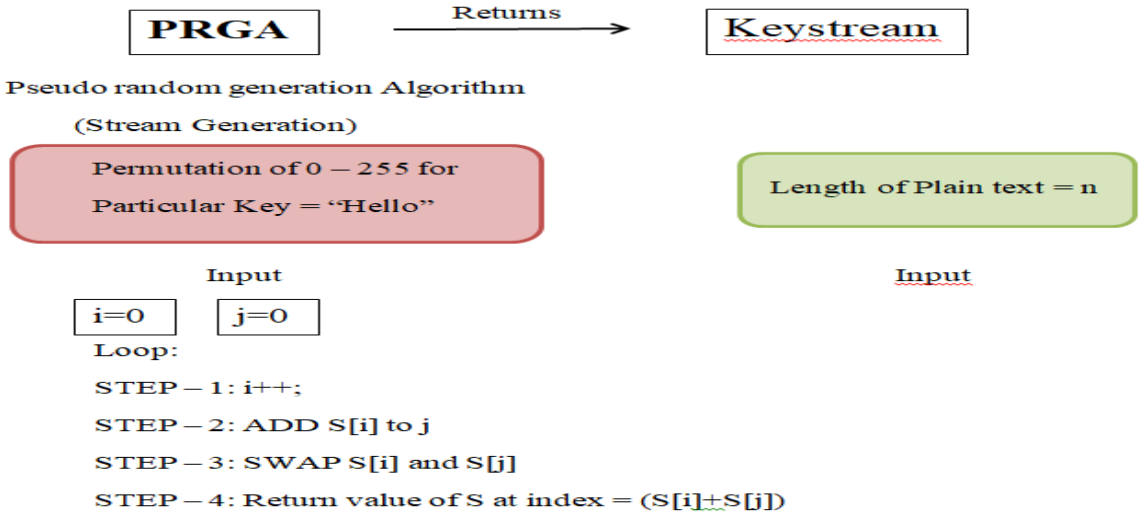


Figure 7: PRGA(Pseudo Random GenerationAlgorithm)

Decryption:

The secret data will be retrieved from the stego file using decryption. The user must provide the frame number they want to obtain data from. We can extract encrypted secret data from that frame number using decryption. Using the RC4 decryption technique and the encryption key, we can decode the encrypted secret data and obtain the standard secret text. The secret text is then delivered to the recipient.

4. CONCLUSION

We conclude that Audio Steganography can incorporate data more effectively than Image and Text Steganography. Image steganography has a greater embedding capacity than text steganography. Image, audio, and video data are more commonly transferred in daily communication than text files. In contrast to text steganography, image and audio

steganography is useful. The message could be included to the work as the video file's cover file. The usage of network steganography is feasible. Additional Network By including new features in work, steganography can be implemented, and the capacity and other factors like imperceptibility, robustness, and security, could be enhanced for future enhancement. To add a further common security layer to the secret text in this case, an encryption algorithm can be a useful addition. Therefore, by combining cryptography with steganography, efficiency can be greatly boosted.

5. REFERENCES

[1]NandiniSubramanian,SomayaAlmadeedandAhmedBouridane"ImageSteganography:AReviewoftherecentadvances"IEEEACCESS,January25th,2021.

[2]Jiaohua,Yuanjingluo,XuyuXiang,YunTanandHuajunHuang,"CoverlessImageSteganography",IEEEACCESS,November25th,2019.

[3]FitraChairilAkbar,TitoWaluyoPurboyoandRoswanLatuconsina," Steganography onText Using Word-Shift Coding and Centroid Methods", Journal of Engineering and AppliedSciencesin2020

[4]NoorAlhudaF.Abbas,Nida Abdulredha1,RaedKhalidIbrahim,AdnanHusseinAli,"Security and imperceptibility improving of image steganography using pixel allocation andrandom function techniques", International Journal of Electrical and Computer Engineering(IJECE),February2022.

[5] Rohit Kumar Yadav, Madan Kushwaha," Message Hiding Using Steganography andCryptography", International Research Journal of Engineering and Technology (IRJET) May2018.

[6] ShreelaDash,Dayal Kumar Behera,SubhraSwetanisha,Madhabananda Das," HighPayloadImageSteganographyusingDNNClassicationandAdaptiveDifferenceExpansion", ResearchSquare,September8th,2022.

[7] Hussein AbdulameerAbdulkadhim, Jinan NsaifShehab"Audio steganography based onleast significant bitsalgorithm with 4D grid multi-wing hyper-chaotic system",InternationalJournalofElectricalandComputerEngineering(IJECE),February2022.

[8] SrilekhaMukherjeea, Subhajit Roya and Goutam Sanyala," Image Steganography UsingMidPositionValueTechnique"InternationalConferenceonComputationalIntelligenceand Data Science(ICCIDS2018).

[9] SaifulIslam,MangatRModiand PhalguniGupta,"Edge-basedimagesteganography",EurasipJournalofInformationSecurity,2019.

[10] NisreenI.R.Yassin,EnasM.F.ElHouby,"ImageSteganographyTechniqueBasedonInteger Wavelet Transform Using Most Significant Bit Categories", International Journal ofIntelligentEngineeringandSystem,October2021.

[11] AshwakALabaichi ,Maisa'a Abid Ali K. Al-Dabbasand Adnan Salih ,"Imagesteganographyusingleastsignificantbitandsecretmaptechniques"InternationalJournalof ElectricalandComputerEngineering(IJECE),February2020.

[12] HudaKadhimTayyehandAhmedSabahAhmedAl-Jumaili,"Acombinationofleastsignificant bit and deflate compression for image steganography",International Journal ofElectricalandComputerEngineering(IJECE),February2022.

[13] Mohammed Majid Msallam," A Development of Least Significant Bit Steganography Technique",Iraqui journal of Computers, Communications, Control and System Engineering, January 2020.

[14] AbdulkaremAlmawgani, Adam Alhawari, WlaedAlarashi, Ali Alshwal ,"Hybrid Image Steganography Method Using LZW and Genetic Algorithm for Hiding Confidential Data ",Research Square,October 15th, 2020.

[15] Nasro Min-Allah , Naya Nagy , Malak Aljabri,Dana Alghamdi, Razan Sabri and Rana Alshaikh ,"Quantum Image Steganography Schemes for Data Hiding: A Survey",Applied Science 2022.
[16] Apurva Sankpal1, Adarsh Singh ,"Data Concealment Using Steganography Technique",May 2022---International Journal for Research in Applied Science & Engineering Technology (IJRASET).
[17] Nitin Arora , Ahatsham , Kamal Preet Singh ,"Achieving Securityin Medical Scanned Images using Extended Image Steganography",July 16, 2018- E ISSN.
[18] Mansoor Fateh , Mohsen Rezvani ,"A New Method of Coding for Steganography Based on LSB Matching Revisited",February 2021----Hindawi Security and Communication Networks.
[19] LingyunXiang ,Guoqing Guo AIMS ,"A convolutional neural network-based linguistic steganalysis for synonym substitution steganography",and 11 November 2019.
[20] MohanadNajmAbdulwahed ," An effective and secure digital image steganography scheme using two random function and chaotic map",15th January 2020 JATIT & LLS.
[21] YutingHua ,YihuaHuangb," Detection of Heterogeneous Parallel Steganography for Low Bit-Rate VoIP Speech Streams",Science Direct & 2 January 2021.
[22] Mustafa Sabah Taha," Combination of Steganography and Cryptography:A Short Survey",ICSET& 2019
[23] Javad Chaharlang, Mohammad Mosleh,"A novel quantum steganography-Steganalysis system for audio signal",SpringerLink& 20 February 2020.
[24]Akash Nag ,"Low -Tech Steganography for Covert Operations",MECS& 2019.
[25] Avinash, Rajendra Kumar Buraniya," Steganography :AnOverview",ISSN& 2019.