

Audio Steganography by Cryptography Algorithm

Rushikesh S. Kulkarni
department of Computer Science and
Engineering
Prof. Ram Meghe College of
Engineering and Management Amravati,
India

Mohnish J. Khobragade
department of Computer Science and
Engineering
Prof. Ram Meghe College of
Engineering and Management
Amravati, India

Shrutika S. Gelewar
department of Computer Science and
Engineering
Prof. Ram Meghe College of
Engineering and Management
Amravati, India
Mrs. Shreya Gangane department
of Computer Science and Engineering
Prof. Ram Meghe College of
Engineering and Management
Amravati, India

Shruti R. Deshmukh
department of Computer Science and
Engineering
Prof. Ram Meghe College of
Engineering and Management
Amravati, India

Abstract— Steganographic methods conceal confidential information within seemingly innocuous media like music files without alerting potential interceptors. This suggested framework employs the Data Encryption Standard's cryptography method to secure information prior to incorporating it within an outer shell for enhanced protection measures. The least significant bit (LSB) coding technique is employed for converting digital information into audible signals through audio sample manipulation. A comprehensive framework ensures an inherently protected communication channel; this security comes about due to both steganographic techniques for concealing messages within non-obvious data structures and cryptographic methods used in conjunction with these hidden elements to safeguard information transmission over open networks.

Keywords—Steganography, Cryptographic, Data Encryption Standard (DES), Least Significant Bit (LSB), Cover File.

I. INTRODUCTION

The technique involves embedding hidden data within an audio track without altering its audible content. Stealth encryption conceals information within an innocuous carrier without changing its fundamental nature. An encoded message could raise doubts among recipients whereas a hidden message achieved through steganography remains undetected by its audience. To conceal information without arousing suspicion is what steganography accomplishes. Furthermore, the robustness of traditional steganographic methods depends crucially upon confidentiality in how information is encoded. With knowledge of the encodation method, the steganalysis technique falls apart. The basic model of Audio steganography consists of Carrier (Audio file), Message and Password. Carrier is also known as a cover-file,

which conceals the secret information ([Jayaram P. Ranganatha H. R. and Anupama H. S., 2011](#)). Message is the data that the sender wishes to remain it confidential. Message can be plain text, image, audio or any type of file. Password is known as a stego-key, which ensures that only the recipient who knows the corresponding

decoding key will be able to extract the message from a coverfile. The cover-file with the secret information is known as a stego-file

A. Related Work

Numerous scholars investigated various techniques for encoding digital audio data in hidden formats. Bimbi Koduru Summer introduced an audio file-based app in 2011. Stealth encryption constitutes an area within cryptography focused on concealing data in plain sight. The skill lies in crafting hidden messages whose decipherment requires knowledge beyond mere reading comprehension. Stealth communication techniques have been utilized for centuries without being considered scientific innovations. To be precise, steganography stems from the ancient Greek term "steganos," signifying concealed or secretive nature, combined with "graphein" for 'writing' or 'drawing'. Therefore, steganography refers to hidden writing techniques. Today's context reveals that steganography now functions primarily by embedding data within various types of media like images, sound files, or videos for covert transmission purposes (Bimbi Koduru, 2009). R. Udayakumar, K. P. Kaliyammurthi, Khanna, and A. V. Allin Geo introduced in 2015 their research on steganographic techniques utilizing audio files within MATLAB programming environment.

Their primary goal in this endeavor is to facilitate safe transmission and reception of confidential information free from interception by an intermediary entity. The researchers concealed information within an audio waveform by embedding it into another digital sound file. Prior to applying this method, there was no variation in the audio's fidelity compared to subsequent applications of it. A stealth audio message is transmitted discreetly to its final location undetected by all outside parties. Should detection occur, the concealed information intended for the recipient remains unreadable due to its encryption mechanism employed by the system developers (Bhavana et al., 2015).

II. BACKGROUND ON STEGANOGRAPHY

The developing possibilities of modern communications want the unique means of safety. The community safety is turning into extra vital as the amount of records being exchanged on the net is growing. protection necessities are vital in both at the very last user stage and at the enterprise degree, especially since the massive usage of personal computer systems, networks, and the net with its global availability. in the course of time, computational protection desires have been centered on exclusive functions: secrecy or confidentiality,

identity, verification, non-repudiation, integrity control and availability. This has led to an explosive growth of the field of information hiding. In addition, the speedy increase of publishing and broadcasting era also requires an opportunity solution in hiding records (Bendalam Vijay, and Jallu Swathi, 2014). There are some of methods for securing records. One is cryptography, in which the sender makes use of an encryption key to scramble the message.

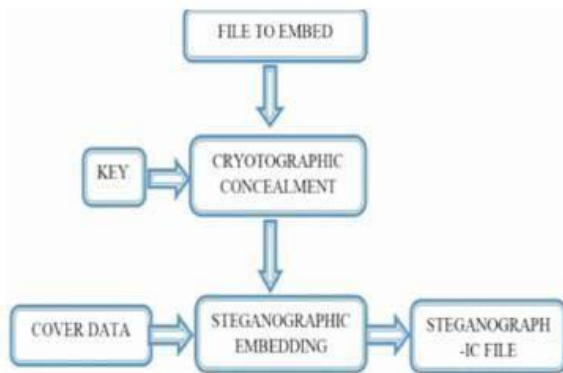


Figure 1. Steganography System Architecture

1. Cryptography

Cryptography is an important detail of any approach to cope with message transmission security necessities. Cryptography is the study of techniques of sending messages in disguised shape in order that simplest the meant recipients can take away the conceal and study the message. It's far the sensible art of converting messages or records into a distinctive form, such that no-one possibly can examine them without getting access to the 'key'. The message can be converted the use of a 'code' (in which case every person or group of characters is substituted through an opportunity one), or a 'cypher' or 'cipher' (in which case the message as an entire is transformed, as opposed to man or woman characters). Cryptology is the science underlying cryptography (Z. V. Patel, and S. A. Gadhiya, 2015).

2. Steganography

The word steganography is derived from the Greek words "stegos" that means "cover" and "grafia" which means "writing" defining it as "blanketed writing". Steganography is one such pro-protection innovation in which mystery data is embedded in a cover. The belief of information hiding or steganography become first brought with the example of prisoners' mystery message by way of Simmons in 1983. Steganography and cryptography are intently related. Cryptography scrambles messages, so they can't be understood. Steganography alternatively, will hide the message so there's no understanding of the lifestyles of the message in the first area. In some situations, sending an encrypted message will arouse suspicion at the same time as an "invisible" message will now not accomplish that.

both sciences may be mixed to produce better protection of the message. In this situation, when the steganography fails and the message can be detected, it's far nevertheless of little need as it's far encrypted the usage of cryptography techniques.

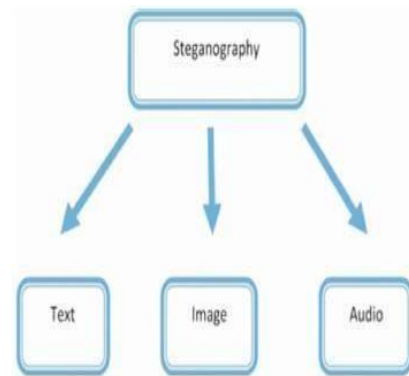


Figure 2. Different Categories of File Formats

III. AUDIO STEGANOGRAPHY SYSTEMS

The primary goal of steganography is to reliably send hidden records secretly, not merely to difficult to understand its presence. Steganography in modern pc era is taken into consideration a subfield of statistics conversation protection domain. currently, new directions primarily based on steganographic methods started to emerge to make certain facts secrecy. as opposed to as a substitute to current solutions, those approaches ought to gain higher records secrecy if mixed with conventional protection techniques. contemporary techniques of steganography make the most the characteristics of virtual media by using using them as vendors (covers) to hold hidden statistics. Covers may be of various sorts together with photograph, audio, video, text, and IP datagram. An instance of audio steganography is depicted in discern five, in which the quilt report in use is a digital audio report (Fatiha Djebbar, Beghdad Ayad, Karim Abed Meraim, and Habib Hamam).

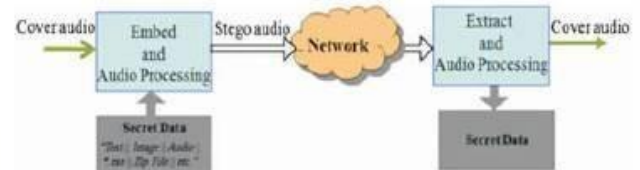


Figure 3. Example of Digital Audio Cover Object

The sender embeds information of any type in a virtual cover record the usage of a key to provide a stego-record, in any such way that an observer can't discover the lifestyles of the hidden message. At the alternative quit, the receiver procedures the acquired stegoreport to extract the hidden message. An apparent software of such steganographic machine is a covert communication using risk free cover audio sign, such as smartphone or video convention conversations

IV. DATA ENCRYPTION STANDARD ALGORITHM

The algorithm's overall structure is shown in Figure 6. There are 16 identical stages of processing, termed rounds. There is also an initial and final permutation, termed IP and FP (Wang Tianfu, and K. Ramesh Babu 2011).

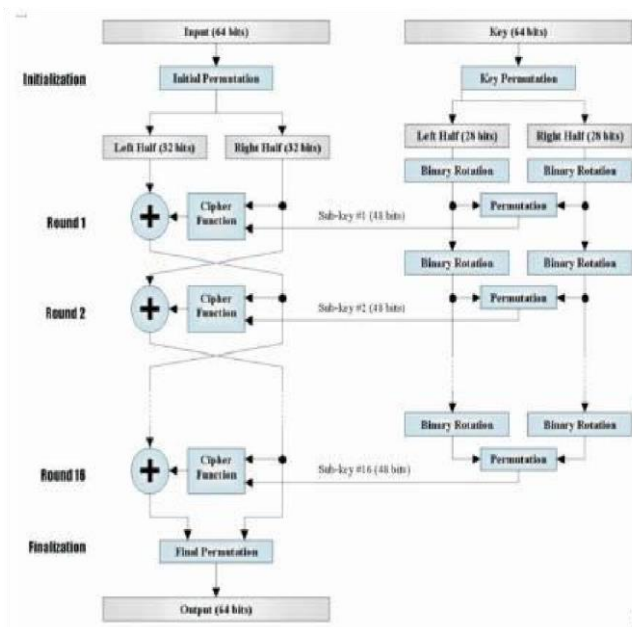


Figure 4. DES Structure

The Feistel (F) function operates on half a block (32 bits) at a time

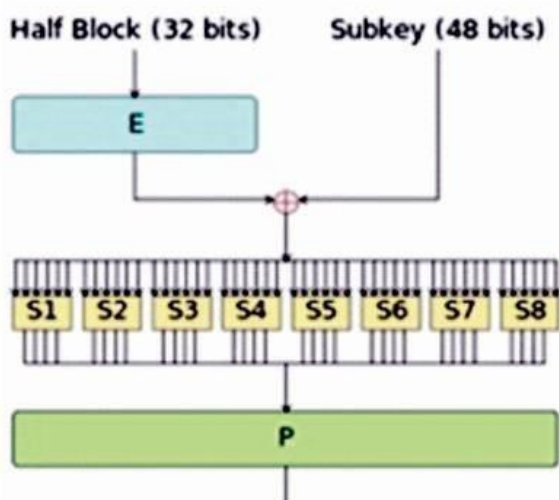


Figure 5. Feistel(F) Function Structure

and consists of four stages, as shown in Figure 5.

3. Permutation: -

eventually, the 32 outputs from the S-boxes are rearranged consistent with a fixed permutation, the P-field. that is designed so that, after permutation, each S-box's output bits are unfolded across 4 exclusive S boxes within the next spherical.

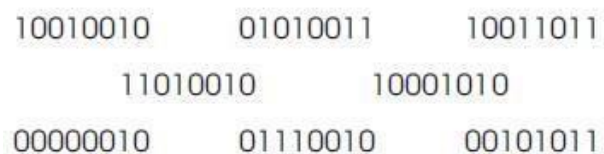
V. LIST SIGNIFICANT BIT ALGORITHM

A completely popular method is the LSB (Least significant Bit) algorithm, which replaces the least big bit in some bytes of the duvet report to hide a sequence of bytes containing the hidden facts. this is generally an powerful method in instances where the LSB substitution would not cause considerable fine degradation, together with in 24-bit bit maps. In computing, the Least sizable Bit (LSB) is the bit role in a binary integer giving the units value, that is, determining whether or not the variety is even or ordinary. The LSB is on occasion called the proper-maximum bit, due to the convention in positional notation of writing much less massive digit similarly to duplicating half of the bits. The output includes eight 6- bit (eight * 6 = 48 bits) portions, each containing a replica of four corresponding enter bits, plus a copy of the right away adjoining bit from each of the input pieces to both side



Figure 6. LSB of a Byte

The binary representation of decimal 149, with the LSB highlighted. The MSB in an 8-bit binary variety represents a fee of 128 decimal. The LSB represents a price of 1. as an example, to cover the letter "a" (ASCII code ninety seven, that is 01100001) interrior 8 bytes of a cowl, you can set the LSB of each byte like this:



1. Key mixing: -

The end result is combined with a sub key the use of an XOR operation. sixteen forty-eight-bit sub keys — one for each spherical — are derived from the main key.

2. Substitution: -

After mixing in the sub key, the block is divided into eight 6-bit portions earlier than processing by the S-boxes, or substitution boxes. every of the eight S-boxes replaces its six enter bits with four output bits according to a non-linear transformation, supplied in the form of a research desk. The S-bins provide the middle of the safety of DES — without them, the cipher could be linear, and trivially breakable

the proper as proven in figure 8. it is analogous to the least vast digit of a decimal integer, that is the digit inside the ones (propermaximum) position (Jayaram P, Ranganatha H R, and Anupama H S, 2011)..

The 32-bit 1/2-block is accelerated to forty-eight bits using the expansion permutation, denoted E in the diagram, by way of

The application decoding the cover reads the eight Least Significant Bits of those bytes to recreate the hidden byte—that is 0110001—the letter "a", as we realize, using this technique it lets you to a byte every eight bytes of the cover.

among special data hiding strategies proposed to embed mystery records within audio record, Least tremendous Bit (LSB) coding method is the most effective way to embed secret information in a virtual audio record by changing the least good sized bit of audio sample with a binary message. on this technique, LSB of binary sequence of every sample of digitized audio document is replaced with binary equal of mystery message. as an example, if we want to hide the letter 'A' (binary equal 01100101) to an digitized audio file in which every sample is represented with sixteen bits, then LSB of eight consecutive samples (each of sixteen bit size) is changed with every little bit of binary equivalent of the letter 'A' as proven in figure 7.

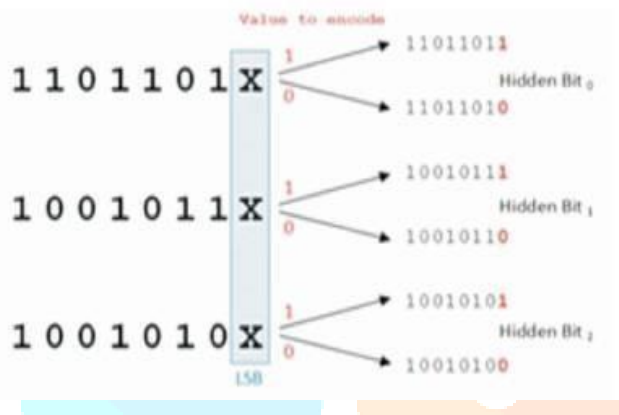


Figure 7. Example of LSB Coding

VI. OVERVIEW OF PROPOSED SYSTEM

In this proposed system, a secure system of hiding information by Steganography is implemented, and for additional security, cryptography is used beside steganography.

An audio report is used as a cowl item, in which the records might be hidden. Hiding process is done using LSB algorithm, with the aid of which, every bit from records to be hidden replaces the LSB of one sample from the audio cover item. As it is discussed, a cryptographic encryption set of rules is used to encrypt statistics before being conceal into the quilt item. The set of rules used in proposed gadget is DES that is a symmetric algorithm of 64 bit key period. with a purpose to compute the minimum range of samples needed to cowl the encrypted report, and therefore the minimum duration of the duvet audio, we ought to first calculate the period of the text record for the reason that it's miles the constrain of the complete procedure. First four bytes of the report is reserved for its length.

This step is vital inside the context of two issues, first, to alarm the system about the decrease restriction of the cover sign length, and second, is for the facts extraction, to notice the receiver to which pattern of the cover item it need to extract statistics.

Data Hiding: These steps are done as shown in Figure 10 in following sequence for data hiding

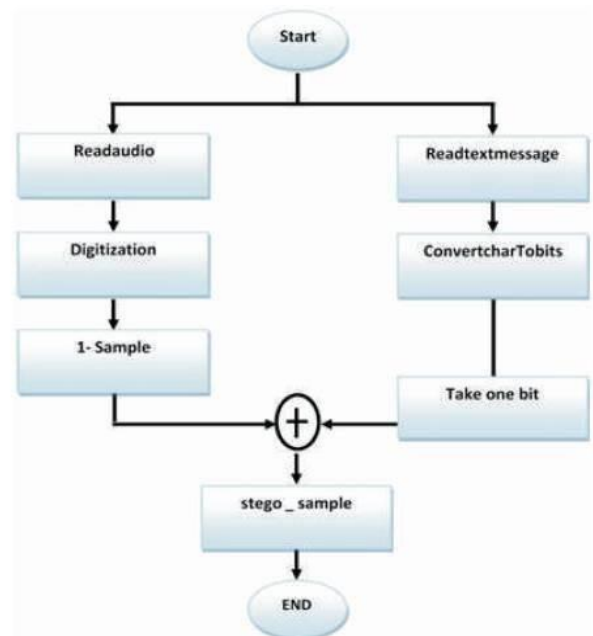


Figure 8. Data Embedding

- Text file to be embedded is opened using open() MATLAB function, and its content is obtained by fread() function.
- Calculating text file length by using length() function and computing the minimum number of seconds needed to cover it.
- Reading audio file using audio read() with length specified in previous step, including conversion from analog format to digital format.
- Applying DES encryption algorithm, with key input from user, to data blocks of 8 bytes, and regrouping all encrypted blocks together to form the whole encrypted file. Concatenating file length with encrypted text.
- Dividing each character from encrypted text to 8 bits using bitand() and bitshift() functions. Embedding of these bits into cover object using bitor() and bitand() functions

By completing these steps, stego object is ready to be transmitted to the receiver side.

Data Extracting: The following steps are done as shown in Figure 9 for data extracting in sequence:

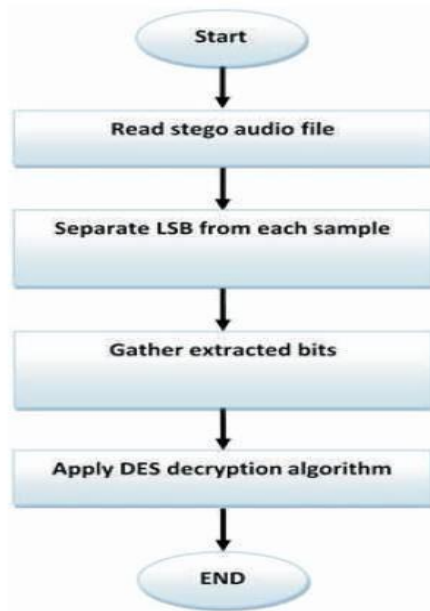


Figure 9. Data Extracting

- Extracting of the first four bytes of text file length.
- Extracting encrypted data bits, begins with the first bit from the fifth byte, and gathering these bits to form the whole extracted encrypted file.
- Applying DES decryption algorithm with the same key used in encryption process.

VII. CONCLUSION

A comfortable transmission machine is produced with the aid of pure Steganography, with out the use of stego key in the embedded facts distribution. The kind of steganography used is Audio Steganography because of this that the cover object is an audio record that would deliver data bits in LSBs of its samples. for extra security, a symmetric cryptographic algorithm, DES, is used to encrypt the records earlier than embedding it into the cover object

Inspiration For Destiny Work the following are hints for destiny paintings in this proposed gadget to improve its implementation and outcomes:

- Applying stego key to randomize the distribution of information bits in cowl object samples which offers more protection to the gadget
- Using triple des algorithm in statistics encryption as opposed to des set of rules which become fairly insecure.
- Concatenating the important thing used for encryption with the message and then encrypting the complete message with a public key encryption set of rules. This is important to avoid protection troubles in key changing.

REFERENCES

- [1]. Bendalam Vijay, and Jallu Swathi, (2014). "Implementation of digital Steganography using image files-a Computational approach", International Journal of Engineering Research and Development, Vol. 10, No.5.
- [2]. Bimbi Koduru Summer (2009). "Steganographic Application Using Audio Files", Graduate Project Technical Report.
- [3]. Fatiha Djebbar, Beghdad Ayad, Karim Abed Meraim, and Habib Hamam, (2012). Comparative Study of Digital Audio Steganography Techniques, EURASIP Journal on Audio Speech and Music Processing.
- [4]. Jayaram P, Ranganatha H R, and Anupama H S, (2011). "Information Hiding Using Audio Steganography – A Survey". The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3.
- [5]. K.P. Kaliyamurthie, Khanaa and A.V. Allin Geo, (2014). "Modeling of Steganography with Audio Files Using Matlabby R. Udayakumar", World Applied Sciences Journal 29 (Computer Sciences, Engineeringand Its Applications.
- [6]. Varsha, and Rajender Singh Chhillar, (2015). "Data Hiding Using Steganography and Cryptography ", International Journal of Computer Science and Mobile Computing, Vol.4, No. 4.
- [7]. Wang Tianfu, and K. Ramesh Babu, (2011). "Design of a Hybrid Cryptographic Algorithm". International Journal of Computer Science & Communication Networks, Vol 2, No. 2, pp. 277-283.
- [8]. Z. V. Patel, and S. A. Gadhiya, (2015). "A Survey Paper on Steganography and Cryptography", RESEARCH HUB – International Multidisciplinary Research Journal (RHIMRJ), Vol. 2, No. 5.