# Audio based Secure Encryption and Decryption

Priyanka Pitale
Asst. Prof., Dept of CSE
RSRRCET, Kohka, Bhilai

Anisha Pateria
Student, Dept of CSE
RSRRCET, Kohka, Bhilai

Priya Singh
Student, Dept of CSE
RSRRCET,Kohka,Bhilai

Nidhi Golchha
Student, Dept of CSE
RSRRCET, Kohka, Bhilai

## ABSTRACT

Steganography is a craft of sending shrouded information or mystery messages over an open channel so that an outsider can't identify the vicinity of the mystery messages. We propose methodologies of substitution method of sound steganography that enhances the limit of spread sound for inserting extra information. For more secure correspondence we are giving security by utilizing the RSA calculation which is focused around cryptography. By utilizing these techniques outsiders can't percept the presence of message implanted in the sound record. The properties of the sound document continue as before in the wake of concealing the mystery message..

**KEYWORDS**
STEGANOGRAPHY,RSA,LSB

## 1. INTRODUCTION

The goal of steganography is to conceal a mystery message inside a spread media in such a path, to the point that others can't observe the vicinity of the shrouded message. Actually in basic words steganograpy means concealing one bit of information inside an alternate. Advanced steganography utilizes the chance of concealing data into computerized media records furthermore Hiding data into a media presupposes emulating components. The cover media that will hold the hidden data

- The secret message may be plaintext or cipher text
- A key or password may be used to hide and unhide the message

**1.1 Audio Steganography:** The essential model of Audio steganography comprises of Carrier (Audio document), Message and Password. Transporter is otherwise called a spread record, which hides the mystery data. Essentially, the model for steganography is demonstrated. Message is the information that the sender wishes to remain it private. Message can be plain content, picture, sound or any sort of record. Secret key is known as a stego-key, which guarantees that just the beneficiary who knows the relating interpreting key will have the capacity to concentrate the message from a spread document. The spread record with the mystery data is known as a stego-document.

Cover Message (image, audio, and video)

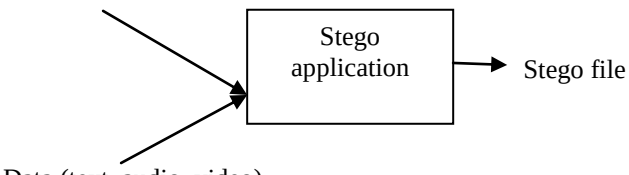
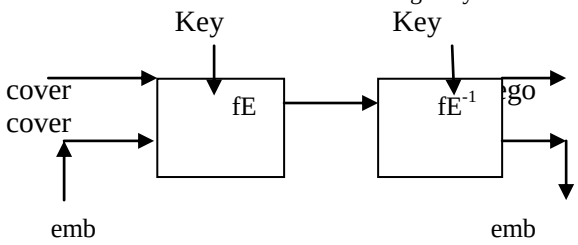



**Fig No: 1**

The steganography application shrouds distinctive sorts of information inside a spread document. The ensuing stego additionally contains shrouded data, in spite of the fact that it is for all intents and purposes indistinguishable to the spread document. What Steganography basically does is adventure human observation; human faculties are not prepared to search for records that have data covered up within them, albeit there are projects accessible that can do what is called Steganalysis.




**FigNo:2**

Fig.2 shows the block diagram of a secure steganographic system. Input messages can be images, texts, video, etc. the components of steganographic system are:

**emb**: the message to be embedded.

**cover**: the data in which emb will be embedded.

**stego**: a modified version of cover that contains the embedded message emb.

**Key**: Additional secret data that is needed for the embedding and extracting processes and must be known to both the sender and the recipient.

$\mathbf{f_E}$: A steganographic function that has cover, emb and key as parameters and produces stego as output.

$\mathbf{F_E}$**-1**: A steganographic function that has stego and key as parameters and produces emb as output.

The embedding process $f_E$ embeds the secret message E in the cover data C. The exact position where E will be embedded is dependence on the key K. The result of the embedding function is slightly modified version of C: the stego data C. After the recipient has received C he starts the extracting process fE-1 with the stego data C and the key K as parameters. If the key that is supplied by the recipient is the same as the key used by the sender to embed the secret message and if the stego data the recipient uses as input is the same data the sender has produces then the extracting function will produce the original secret message E.

# 2. IMPLEMENTATION

## 2.1 RSAAlgorithm

RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. It's also part of Lotus Notes, Intuit's Quicken, and many other products. The encryption system is owned by RSASecurity.

The mathematical details of the algorithm used in obtaining the public and private keys are available at the RSA Website. Briefly, the algorithm involves multiplying two large prime numbers (a prime number is a number divisible only by that number and 1) and through additional operations deriving a set of two numbers that constitutes the public key and another set that is the private key

Using an encryption key (e, n), the algorithm is as follows:

1.Represent the message as an integer between 0 and (n-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range**.**

2.Encrypt the message by raising it to the eth power modulo n. The result is a cipher text message C.

3.To decrypt cipher text message C, raise it to another power d modulo n

4.The encryption key (e, n) is made public. The decryption key (d, n) is kept private by the user.

**Determining Appropriate Values for e, d, and n**

1. Choose two very large (100+ digit) prime numbers. Denote these numbers as p and q.
2. Set n equal to p * q.
3. Choose any large integer, d, such that GCD(d, ((p-1) * (q-1))) = 1
4. Find *e* such that e * d = 1 (**mod** ((p-1) * (q-1)))

## 2.2 LSB Coding

A very popular methodology for audio steganography is the LSB (Least Significant Bit) algorithm, which replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data. That's usually an effective technique in cases where the

LSB substitution doesn't cause significant quality degradation, such as in 24-bit bitmaps. In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |

The binary representation of decimal 149, with the LSB highlighted. The MSB in an 8-bit binary number represents a value of 128 decimal. The LSB represents a value of 1. For example, to hide the letter "a" (ASCII code 97, which is 01100001) inside eight bytes of a cover, you can set the LSB of each byte like this:

10010010
01010011
10011011
11010010
10001010
00000010
01110010
00101011

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 you may realize, using this technique let you hide a byte every eight bytes of the cover. Note that there's a fifty percent chance that the bit you're replacing is the same as its replacement, in other words, half the time, the bit doesn't change, which helps to minimize quality degradation.

# 3. PROPOSED SYSTEM

The larger part of today's steganographic frameworks utilizes mixed media items like picture, sound, feature and so on as spread media in light of the fact that individuals frequently transmit advanced pictures over email and other Internet correspondence. In a machine based sound steganography framework, mystery messages are installed in advanced sound. The mystery message is implanted by marginally modifying the twofold grouping of a sound document. Existing sound steganography programming can implant messages in WAV, AU, and even Mp3 sound records. In future we can likewise actualize feature steganography. Proposed Image and Audio Steganography framework is a strategy for information stowing away is the methodology of concealing data behind the wave record that is transporter document. The message is initially scrambled and after that installed in the transporter. The framework has emulating four layersEncryption

- Encoding
- Decoding
- Decryption

Encoding: The process of hiding the message in the image and audio file.

Decoding: Decoding is a process of retrieving the message from the Image and audio file.

# 4. ADVANTAGES

- Procurement for encryption of message before encoding it into the sound document to upgrade the security.
- Procurement of encryption key and complex encryption calculation.
- The encryption key is altered by the calculation to get another key which is utilized for encoding the message. So regardless of the fact that the key is known for a gatecrasher, he can't break the code.
- Time to encode and decipher is less.

# 5. APPLICATIONS

Stegnography can be utilized whenever you need to conceal information. There are numerous motivations to shroud information however they all come down to the fancied to keep unapproved persons from getting to be mindful of the presence of a message. With these new procedures, a concealed message

is unclear from repetitive sound. Regardless of the fact that the message is suspected, there is no evidence of its presence. In the business world steganography can be utilized to shroud a mystery concoction recipe or arrangements for another development. Number references independently in superscripts. Place the genuine reference at the base of the segment in which it was referred to. Don't place references in the reference list. Utilization letters for table references.

Steganography can likewise be utilized for corporate surveillance by conveying exchange discharge without anybody at the organization being any the savvier.

## 6. CONCLUSION

This paper has presented a hearty technique for impalpable sound information covering up. This framework is to give a decent, effective system for concealing the information from programmers and sent to the objective in a safe way. This proposed framework won't change the measure of the record considerably in the wake of encoding furthermore suitable for any kind of sound document position. Consequently we presume that sound information concealing procedures can be utilized for various purposes other than incognito correspondence, data are following and finger printing. As the sky is not restrain so is not for the advancement. Man is currently pushing without end its own particular limits to make each thought conceivable. So correspondingly these operations portrayed above can be further adjusted as it is in the realm of Information Technology.

Hiding information may introduce enough visible noise to raise suspicion. Therefore the carrier or cover audio must be carefully selected. A cover audio should contain some randomness. It should contain some natural uncertainty or noise. Once it has been used, the audio should be used again and should be destroyed. A familiar audio should be used. It is better for the steganographer to create own audios. This proposed system is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. This proposed system will not change the size of the file even after encoding and also suitable for any type of audio file format. Encryption and Decryption techniques have been used to make the security system robust.

## 7. FUTURE SCOPE

- Steganography though is still a fairly new idea. There are constant advancements in the computer field, suggesting advancements in the field of steganography as well. It is likely that there will soon be more efficient and more advanced techniques for steganalysis. A hopeful advancement is the improved sensitivity to small messages knowing how difficult it is to detect the presence of a fairly large text file within an image, imagine how difficult it is to detect even one or two sentences embedded in an image. It is like finding a microscopic needle in the ultimate haystack.
- We can further develop our project by using video files instead of audio files, hence establishing a video steganography system.
- We are encrypting an audio file of smaller size at present. This can be improved to encrypt audio files of larger size.
- Though it is a well built system, it has been limited to some restrictions. Quality of the sound depends upon the size of the audio file selected by the user and the length of the message to be hidden. There are a number of ways that this project can be extended. Its performance can be upgraded to higher levels by using a better algorithm for encoding and decoding. Instead of having a common secret key for encryption and decryption, a Public-private key pairs can be used.

## 7. ACKNOWLEDGEMENT

We would like to thank our guide Asst.Prof. Priyanka Pitale, for her guidance and feedback during the course of the project. We would also like to thank our department for giving us the resources and the freedom to pursue this project.

## 8. REFFERENCES

[1] July 2013 Encryption of an Audio File on Lower Frequency Band for Secure Communication. Sheetal Sharma, Lucknesh Kumar, HimanshuSharma Dep. Of CSE GCET, Dep. Of ECE, M.U. Greater Noida India Aligarh, India.

[2] **www.informit.com** Cryptography with JAVA.

[3] B. Schneier, Applied Cryptography**,** John Wiley & Sons, New York, 1994.

[4] B. Schneier, Description of a New Variable-Length Key, 64-Bit Block ciphers software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204.

[5] www.arachnoid.com/signal_processing

[6] Meyer, J. and Gadegast, F., "Security Mechanisms for Multimedia Data with the Example MPEG-1 Video,"Project Description of SECMPEG, Technical University of Berlin, Germany, May 1995.

[7] Spanos, G. A. and Maples, T. B., "Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-time Video," Proceedings of 4th International Conference on Computer Communications and Networks, Las Vegas, NV, September 20-23, 1995.

[8] Kriti Saroha SOIT CDAC U.P., INDIA Pradeep Kumar Singh, A Variant of LSB Steganography for Hiding Images in Audio, International Journal of Computer Applications (0975 – 8887) Volume 11– No.6, December 2010

[9] Budda Lavanya, 2 Yangala Smruthi, 3 Srinivasa Rao Elisala. Data hiding in audio by using image steganography technique, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Web Site: www.ijettcs.org Volume 2, Issue 6, November – December 2013

[10] Jayaram, Ranganatha H R2, Anupama H Department of Computer Science and Engineering, R V College of Engineering, INFORMATION HIDING USING AUDIO

[11] STEGANOGRAPHY – A SURVEY The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011

[12] Kamalpreet Kaur DeepankarVerma, Multi-Level Steganographic Algorithm for Audio Steganography using LSB, Parity Coding and Phase Coding Technique,International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014

[13] Tanmaiy G. Verma, Zohaib Hasan, Dr. Girish Verma, A Unique Approach for Data Hiding Using Audio Steganography, International Journal of Modern

Engineering Research (IJMER) www.ijmer.com Vol. 3, Issue. 4, Jul - Aug. 2013 pp-2098-2101

[14] Linu Babu, Jais John S, Parameshachari B D,Muruganantham , HS DivakaraMurthy, Steganographic Method for Data Hiding inAudio Signals with LSB & DCT, International Journal of Computer Science and Mobile Computing A Monthly Journal of Computer Science and Information TechnologyISSN 2320–088X IJCSMC, Vol. 2, Issue. 8, August 2013.

[15] Ashwini Mane., Gajanan Galshetwar., Amutha Jeyakumar, DATA HIDING TECHNIQUE: AUDIO STEGANOGRAPHYUSING LSB TECHNIQUE, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.1123-1125 1123