ISSN XXXX XXXX © 2019 IJESC

Research Article Volume 9 Issue No.3

Robust Audio Steganography Enhanced with Spy Analysis for Unassailable Data Transmission

Divya. R[1], Sangeetha. R[2], Jane Juliana. A. B[3]
UG Student[1, 2, 3]
Meenakshi Sundararajan Engineering College, Kodambakkam, Chennai, India

Abstract:
The project presents the privacy data protection during transmission via common network through audio signals based on Steganography with RC7 and Chaos encryption standard. The proposed encryption technique is used to encrypt the confidential data into unreadable form and not only enhances the safety of secret carrier information by making the information inaccessible to any intruder having a random method. After data encryption, the data hider will conceal the secret data into the audio signal coefficients. Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural or meaningless. This system is still enhanced with encrypt messages using RC7 crypto system. This is the reason a new security approach called data hiding arises. It is the art of hiding the existence of data in another transmission medium to achieve secret communication. It does not replace cryptography but rather boosts the security using its obscurity features. The data hiding technique uses the LSB replacement algorithm for concealing the secret message bits into the high frequency coefficients. In the data extraction module, the secret data will be extracted by using relevant key for choosing the relevant data to extract the data. By using the decryption keys, extracted text data will be decrypted from encryption to get the original information. Here the performance metrics such as Signal to noise ratio and Mean Square Error will be evaluated.

Keywords: Audio steganography, RC7 and Chaos encryption , LSB algorithm , Signal to noise ratio,Mean square error

1.INTRODUCTION

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphein meaning "to write". The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

1.1 Research Motivation

We live in a world were data is considered as the most precious aspect. A lot of organisations holding important databases have been hacked. Data insecurity and hacking of crucial data can lead to a huge crisis that can lead to the downfall of an era itself. From “Target” being targeted to telemedical documents being hacked, we have seen the problem growing bigger and bigger. In order to provide data security and to divert the hackers, we have come up with a new solution that proves to be useful.

1.2 Project Objective

The major objective of this project lies on audio steganography to divert the hacker’s mindset by providing them with a false/dummy data at the user interface that too by using a robust technique for unassailable data transmission. Apart from providing a false message to confuse the hacker, we want to make the encryption even more stronger and hence a double encryption is being preferred and used. The major objective withholds transmission of data without being tampered by intruders apart from providing an accurate transmittal.

2. PROPOSED METHOD

The proposed system consists of

1.Encryption
2.Decryption

2.1,Encryption

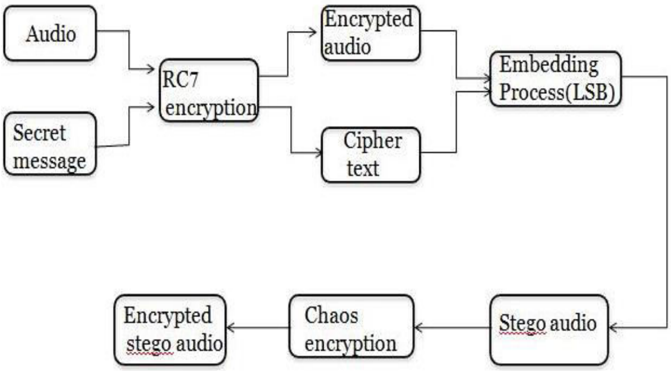


Figure.1. Encryption

1. The normal input audio is taken and allowed to be read at the MATLAB.
2. The secret text is converted to cipher text by using RC7 encryption.
3. Using the LSB algorithm, the audio signal and cipher text is embedded together.
4. The output obtained after the embedding process is a stego audio, which has to be encrypted once again using chaos encryption, which leads double encryption which in turn increases the security feature.
5. Hence the encrypted audio is obtained.

2.2.Decryption

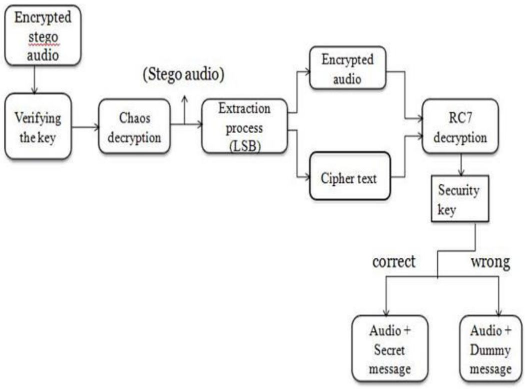


Figure.2. Decryption

1. The obtained encrypted audio is first verified with a key and passed on to the chaos decryption unit where the fitrst level of encryption is removed.
2. The encrypted audio and the cipher text is separated by the LSB Extraction process.
3. After the audio is separated from the text, the RC7 Decryption takes place and two case studies can be seen.
a. If the correct key is given, the correct message and the audio will be provided to the hacker.
b. If the wrong key is given, the false/dummy message and the audio will be provided to the hacker.

3.METHODOLOGIES

This section presents some common methods used in audio Steganography

- RC Encryption
- LSB Embedding and Extraction
- Chaos crypto system

3.1 RC Encryption:

Based on the type of key being used, the algorithms could be classified into Symmetric key algorithms and Asymmetric key algorithms. The Symmetric key algorithms are those in which encryption and decryption are performed using the same key. Asymmetric key algorithms are the ones in which encryption and decryption are performed using different keys. The RC7 algorithms are a set of symmetric-key encryption algorithms invented by Ron Rivest. The "RC" may stand for either Rivest's Cipher or, more informally, Ron's code.

RC7 encryption:

To improve the encryption efficiency of the already existing RC6 algorithm , RC7 has been proposed which takes relatively less time to encrypt data and is comparatively more flexible.In RC7 encryption , the intended information or message, referred to as plaintext is encrypted into cipher generating ciphertext that can be read only if decrypted using correct security key. It provides that only authorized parties can access it and those who are not authorized cannot . Both the audio and secret message is encrypted into secure audio and cipher text so that the non-authorised cannot access it easily.

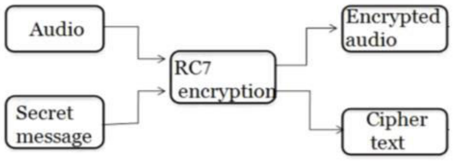


Figure.3.RC7 algorithm

3.2 LSB CODING:

Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. The following diagram illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method:

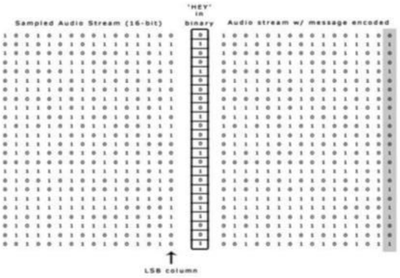

Sampled Audio Stream (16-bit)
'HEY' in binary
Audio stream w/ message encoded
LSB column

Figure.4.LSB coding

Standard LSB Algorithm:

It performs bit level manipulation to encode the message. The following steps are

a. Receives the audio file in the form of bytes and converted in to bit pattern.

b. Each character in the message is converted in bit pattern.

c. Replaces the LSB bit from audio with LSB bit from character in the message.

3.3 CHAOS ENCRYPTION:

Chaotic cryptology includes two integral opposite parts:

- Chaotic cryptography
- Chaotic cryptanalysis.

Chaotic cryptography is the application of the mathematical chaos theory to the practice of the cryptography, the study or techniques used to privately and securely transmit information with the presence of a third-party or adversary. Since first being investigated by Robert Matthews in 1989, the use of chaos in cryptography has attracted much interest; however, long-standing concerns about its security and implementation speed continue to limit its implementation. In order to use chaos theory efficiently in cryptography, the chaotic maps should be implemented such that the entropy generated by the map can produce required Confusion and diffusion. Properties in chaotic systems and cryptographic primitives share unique characteristics that allow for the chaotic systems to be applied to cryptography. If chaotic parameters, as well as cryptographic keys, can be mapped symmetrically or mapped to produce acceptable and functional outputs, it will make it next to impossible for an adversary to find the outputs without any knowledge of the initial values. One of the most important issues for any cryptographic primitive is the security of the system. However, in numerous cases, chaos-based cryptography algorithms are proved unsecure. The main issue in many of the cryptanalyzed algorithms is the inadequacy of the chaotic maps implemented in the system.

4.EVALUATION OF AUDIO STEGANOGRAPHY

4.1 Advantages:

Audio based Steganography has the potential to conceal more information:
▪ Audio files are generally larger than images
▪ Our hearing can be easily fooled

- Slight changes in amplitude can store vast amounts of information.
- The methods discussed provide users with a large amount of choice and makes the technology more accessible to everyone.
- Many attacks that are malicious against image Steganography algorithms (e.g. geometrical distortions, spatial scaling,etc.) cannot be implemented against audio Steganography schemes.
- As emphasis placed on the areas of copyright protection, privacy protection, and surveillance increases, Steganography will continue to grow in importance as a protection mechanism.
- Audio Steganography in particular addresses key issues brought about by the MP3 format, P2P software, and the need for a secure broadcasting scheme that can maintain the secrecy of the transmitted information, even when passing through insecure channels.

4.2 Disadvantages:

- Embedding additional information into audio sequences is a more tedious task than that of images, due to dynamic supremacy of the HAS over human visual system.
- Robustness: Copyright marks hidden in audio samples using substitution could be easily manipulated or destroyed if a miscreant comes to know that information is hidden this way.
- Commercialized audio Steganography have disadvantages that the existence of hidden messages can be easily recognized visually and only certain sized data can be hidden.

5.RESULTS

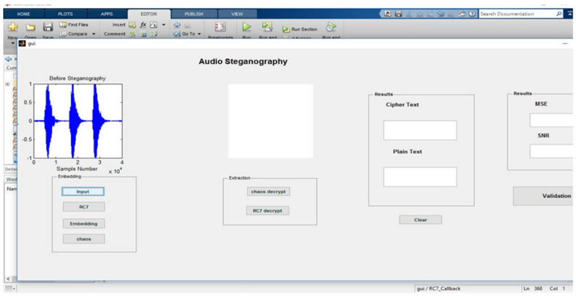


Figure. 5. Before steganography

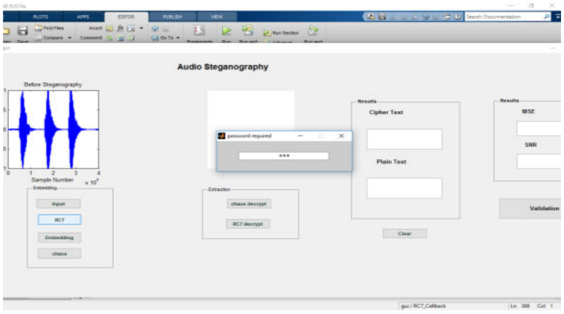


Figure.6. RC7 encryption password

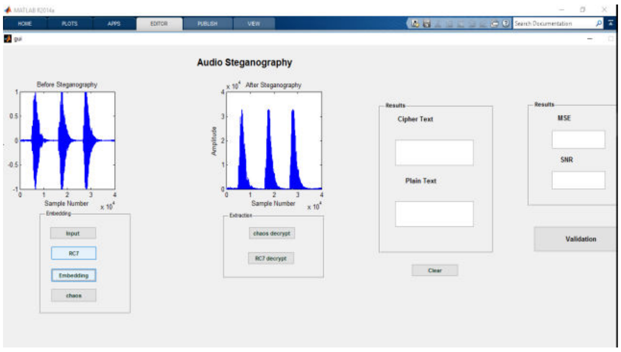


Figure.7:Chaos encryption password

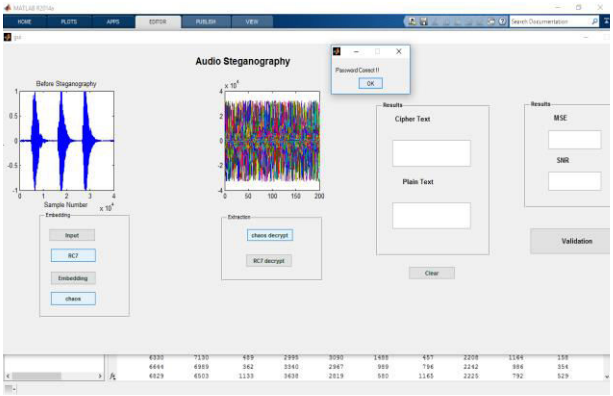
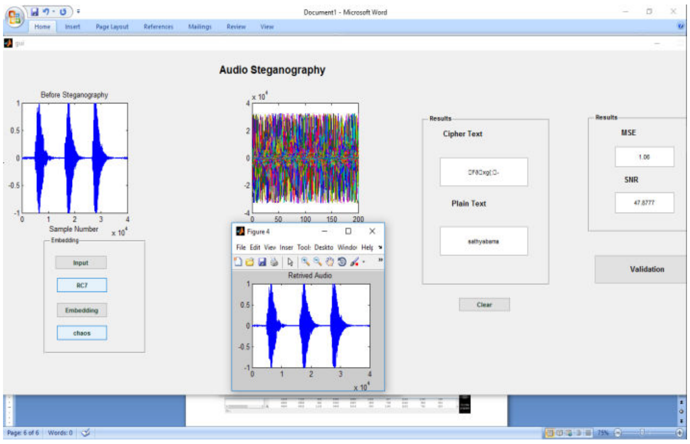

Password Correct !!

Figure .8.Chaos decryption with correct password

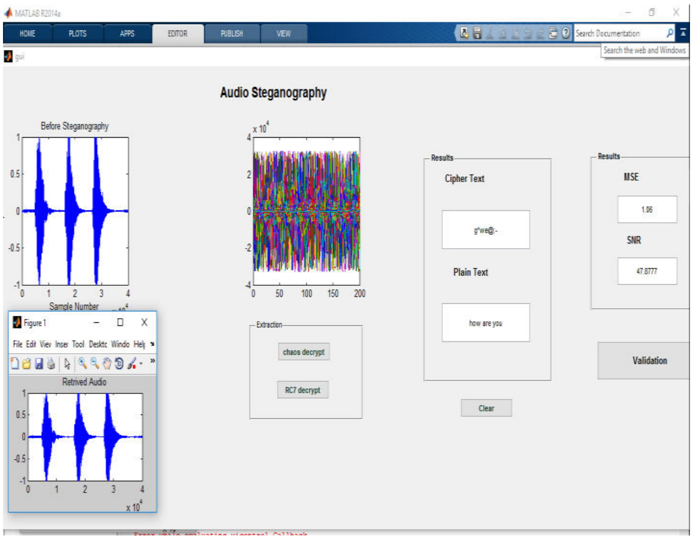

Cipher Text: DF8Zxg(D-

Plain Text: sathyabama

MSE: 1.06

SNR: 47.8777

Figure .9.RC7 decryption with correct password


Cipher Text: g*we@:-

Plain Text: how are you

MSE: 1.06

SNR: 47.8777

Figure .10.RC7 decryption with incorrect password

6.CONCLUSION

The entire project concentrates on the ways to divert the hacking concept and not letting the system be prone to hackers. The system is very rigid as the complication of decryption increases for every other level of decoding. The data security can be kept highly confidential by using robust audio steganography.

ACKNOWLEDGEMENT

We feel elated in manifesting a deep sense of gratitude and thankfulness to the management of Meenakshi Sundararajan Engineering College,our beloved Head of the Department and all our staffs for being extremely supportive in every step of our way.

7. REFERENCES

[1]. S.S.Agaian, D.Akopian, O.Caglayan, S. A. D' Souza , "Lossless Adaptive Digital Audio Steganography," In Proc. IEEE Int. Conf. Signals, Systems and Computers, pp. 903-906, November 2005.

[2]. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", IBM Systems Journal, vol. 35, Issues 3&4, 1996, pp. 313-336.

[3].C. C. Chang, T. S. Chen and H. S. Hsia, "An Effective Image Steganographic Scheme Based on Wavelet Transform and Pattern- Based Modification", IEEE Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing, 2003.

[4].K. Gopalan, "Audio steganography using bit modification , Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Vol. 2, pp. 421- 424, April 2003.

[5].N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," Computer, vol. 31, no. 2, pp. 26-34, IEEE, Feb. 1998.