Academic City University College, Accra, Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Nigeria Chapter

33rd ECOWAS iSTEAMS ETech Multidisciplinary Conference (ECOWAS-ETech)

Hidden Text Into Audio Files

Felicity Elorm Babanawo
School of Technology
Ghana Institute of Management & Public Administration
GreenHill, Accra Ghana
felbabsforu@gmail.com

ABSTRACT

In this digital era, transmitting data through a computer network has become common. Moreover, some applications have also been developed to do it. Nevertheless, users may not be aware of the security aspect of this data transmission, which can lead to disclosing this private message. In a case when a sensitive message is the object to transmit, a security mechanism should be applied. Data hiding is one of the methods introduced to work for this issue. So the attractive solution for this problem is Steganography, which is the art and science of writing hidden messages in such a way that no one, apart from the sender and intend recipient, suspects the existence of the message, a form of security through obscurity. Audio steganography is the scheme of hiding the existence of secret information by concealing it into another medium such as audio file. This paper features a new technique suggests that the text message is encoded through the use of Huffman coding method and entrenched into audio file when applying the LSB algorithm. The result is put into a novel audio file.

Keywords: Steganography, Data security, Data hiding, LSB algorithm, Huffman coding,

Proceedings Citation Format
Felicity Elorm Babanawo (2022): Hidden Text Into Audio Files. Proceedings of the 33rd ECOWAS iSTEAMS Emerging Technologies, Scientific, Business, Social Innovations & Cyber Space Ecosystem Multidisciplinary Conference. University of Ghana/Academic City University College, Ghana. 29th Sept – 1st Oct, 2022. Pp 45-49. www.isteams.net/ecowasetech2022. dx.doi.org/10.22624/AIMS-/ECOWASETECH2022P6

1. INTRODUCTION

The structure of the secret message is not altered in Steganography but hides it inside a cover image so that it cannot be seen. A message in a cipher text, for instance, might arouse suspicion on the part of the recipient while an “invisible” message created with stenographic methods will not. In other word, steganography prevents an unintended recipient from suspecting that the data exists. In addition, the security of classical steganography system relies on secrecy of the data encoding system. Once the encoding system is known, the steganography system is defeated [1}.

Steganography can be classified into three types: pure steganography, secret key steganography, public key steganography [2].All data-hiding applications require hiding algorithms on the sender side and a detector mechanism or algorithm on the receiver side. The hidden message or data can be retrieved by authorized people only. The most crucial parameters of the data-hiding applications are: security, reliability, invisibility, complexity, and data-hiding capacity, these parameters are mostly related to each other [3].In recent years; various techniques for steganography in digital audio with various purposes have been developed. Basically, hiding information in audio files is a type of steganography that hides digital data into digital audio files as a carrier such WAV, MP3, and WMA files without damaging the contained of this uninteresting audio file, so that it cannot be seen by eavesdroppers [4,5,6].

2. RELATED LITERATURE

In [7] present an approach for resolving the problem related to the substitution technique of audio steganography. In first level of security, we use RSA algorithm to encrypt message, in the next level, encrypted message is to be encoded in to audio data for this we used genetic algorithm-based substitution method. The basic idea behind this paper is to enhance the security and robustness.

K.U. Singh [9] highlighted various audio steganography methods like temporal domain method and Transform Domain Technique (e.g, Discrete Wavelet transform, Spread Spectrum, Tone insertion, Phase coding) and then compared between these methods from strength and weakness. T. Sandhya[10] suggested technique based on integration of audio steganography and cryptography that is based on dual density double tree complex wavelet Transform with blowfish encryption. It implements most influential procedure in the initial level of security which is very intricate to disrupt. In the subsequent level, it applies a changed LSB procedure to encrypt the message into audio thus ensures superior security.

3. FINDINGS.

Government ban on digital cryptography:

i. Individuals and companies who seek confidentiality look to steganography as an important complementary since combining cryptography and steganography can help in avoiding suspicion and protect privacy.
ii. The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 201187
iii. The increased need to protect intellectual property rights by digital content owners, using efficient watermarking.
iv. The trend towards electronic communications and humans desire to conceal messages from curious eyes. With rapid advancement in technology, stenographic software is becoming effective in hiding information in image, video, audio or text files [11,14].

4. RESEARCH GAPS

There are some secret data that are hidden in a predictable manner, making them easy to recover by attackers, and to bypass this weak point, encryption of the secret file to be hidden is resorted to by one of the encryption methods before the completion of the hiding process, or by using the proposed method . Even though the steganography method has different applications

that are useful, it can at times be applied for other illegal activities. For instance, drug dealers, terrorists and other criminals can use the technique in order to ensure that their communication is not accessed by third parties thus implying that it can help enhance the activities that are carried out by the criminals.

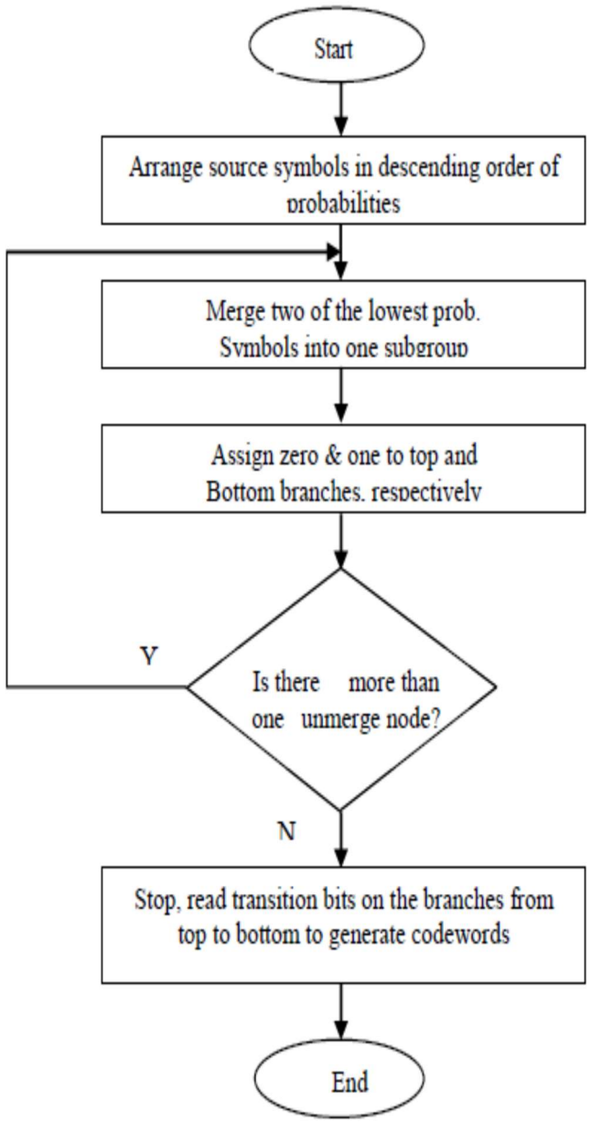
5. RECOMMENDATIONS FOR PRACTICES

The suggested method integrates the cryptography and steganography to acquire a high level security and avert attackers from establishing the existence of the undisclosed message. In the initial level, the confidential message is encoded using Huffman coding Algorithm. In the succeeding level the encoded text is concealed in the audio file using slightest significant bit.

The subsequent steps exemplify the entrenched process:

- Evaluate the audio file(.wav) , establish the length of file, find out the number of samples Compute the key for keeping the data by
- Adel A. Sewisy et al.
- key=number of samplessample rate
- Transform the cover audio file to binary, read undisclosed message and change it to binary.
- Encode the entered undisclosed message using Huffman coding algorithm.
- Substitute the least important bit of each cover position by the bit of encoded undisclosed message.
- Generate a new audio file that comprises of embedded text into audio file
- To obtain the encoded message from the cover audio file at the recipient's side, the succeeding steps should be used:
- Read the entrenched audio file(stego), establish the length of file, number of sample
- Transform stego file into Binary, Compute the key for keeping data into audio file
- key=$number\ of\ samplssample\ rate$
- Apply Key to obtain the value that has frequency of letters and symbol of text
- Decrypt the undisclosed message using Huffman code to get the initial text. Save the symbols in new text file

6. POLICIES AND DESIGN



7. CONCLUSION

This paper features a new technique that is suggested. To begin with, the text message is encoded using Huffman coding method and entrenched into audio file using LSB algorithm. The result is then put into a new audio file and thereafter contrasted through the use of various values that include; PSNR (peak signal to noise ratio), and SNR (signal to noise ratio). The frequency of audio file prior and after entrenched text message is schemed. Trials indicate that the suggested method is comparatively effective in Embedded Encrypted Text into Audio files.

8. DIRECTIONS FOR FUTURE WORKS

The authors recommend more secure encryption algorithms to be utilized for text encryption, so that data is not easily stolen by an unauthorized party. In [11] give an overview of two primitive techniques to get an idea of how steganography in audio file works. LSB modification and phase encoding technique are very primitive in steganography. An effective audio stenographic scheme should possess the following three characteristics: Inaudibility of distortion, Data Rate and Robustness. These characteristics are called the magic triangle for data hiding.

REFERENCES

1. Nedeljko Cvejic, Tapio Seppben "Increasing the capacity of LSB-based audio steganography " FIN-90014 University of Oulu, Finland ,2002.
2. Cheng-Te Wang, Tung-Shou Chen and Wen-Hung Chao, "A new audio watermarking based on modified discrete cosine transform of MPEG/Audio Layer III".
3. Wang H, Wang S. Cyber warfare: steganography vs. steganalysis.
4. Djebbar F, Ayad B, Abed-Meraim K, Hamam H. A view on latest audio steganography techniques, 2011.
5. Gadicha AB. Audio Wave Steganography. Int J Soft Comput Eng 2011;1(5).
   Padmashree G, Venugopala PS. Audio Steganography and Cryptography (IJEIT) October
6. 2012;2(4)
7. .A. Tahseen Suhail and H. Ghanim Ayoub Egyptian Informatics Journal xxx (xxxx) xxx
8. Singh, G., Tiwari, K. & Singh, S. (2014). Audio steganography us-ing RSA algorithm and genetic based substitution method to en-hance security. International Journal of Scientific and Engineering Research, 5(5), 703-707.
9. K.U. Singh, A Survey on Audio Steganography Approaches. International Journal of Computer Applications, Vol.95, No.14, 7-14, (2014).
10. T. Sandhya, . International Journal of Emerging Technology and Advanced Engineering, Vol.3, No.1, 63-72,(2014).
11. Bandyopadhyay, S. K. & Banik, B. G. (2012). , 1(1),