International Journal on Applications in Engineering and Technology
Volume 8 : Issue 2 : May 2022, pp 145 –148 www.aetsjournal.com ISSN (Online) : 2455 - 0523

DISCRETE WAVELET TRANSFORM AUDIO STEGANOGRAPHY

NIKESH B[1], RAMESH KUMAR A[2], SANTHOSH S[3] , SARANYA R[4]

[1,2,3] *Undergraduate student, Department of Computer Science and Engineering,*

Paavai College of Engineering

[4] *Assistant Professor, Department of Computer Science and Engineering,*

Paavai College of Engineering

Abstract: - Steganography was the practise of concealing information or a hidden message behind a cover item, such as a picture, audio, or video. Only authorised recipients can see the message delivered from the source end as a result of this. Steganography is the art of concealing information behind a cover object. This has a wide range of applications in disciplines such as multimedia, military, navy, and civil engineering, among others. In practise, most steganography methods were also used to encrypt photos and movies. Speech steganography has a small number of research papers published because it is more difficult to construct than image or video steganographic systems.

***Key Words*:** Audio steganography, adaptive steganography, information concealment, least significant bit (LSB)

I. INTRODUCTION

Steganography is a form of encrypted communication that allows for private and secure communication. It has a wide range of applications, including audio-video synchronisation, copyright control, television transmission, military use, and digital watermarking. Broadband internet connections allow for practically error-free data transmission, allowing individuals to distribute big multimedia files and duplicate them. Sensitive messages and files are sent over the internet in an unsecured format, but everyone has something to keep hidden. The goal of steganography is to hide hidden data inside the cover medium while maintaining the cover medium's overall quality.

1.1 OBJECTIVE

The widespread usage of the Internet among the general public, as well as the abundance of public and private digital data, has prompted industry experts and researchers to devote special attention to data security. Cryptography, watermarking, and steganography are the three main approaches now in use. The substance of a message is garbled for unauthorised users using cryptography techniques. Watermarking is the process of concealing data in order to convey information about the cover media, such as ownership and copyright. Despite the fact that cryptography and watermarking techniques are important for data security, much current research has been focused on finding better or complementary new techniques. The contrasts and parallels between steganography, watermarking, and cryptography are depicted

1.2 PROJECT DESCRIPTION

Accqisition of the audio file steganography is the skill of concealing classified information in a cover material without drawing notice to itself. Modern steganography techniques take advantage of the properties of digital media by using them as carriers (covers) for hidden data. Text, speech/audio, image, and video are all examples of cover types. As a result, the sender embeds secret data in a digital cover file using a key to create a stego-file, making it impossible for an observer to detect the concealed message. The sender's input can be gathered in this module. Audio files or speech data can be used as input. It is saved as a WAV file. It can be uploaded in a variety of sizes and formats.

SECRET DATA

Secret information and secret data can be selected in this module. The sender can choose which information should be kept private. Secret data can be in the form of a message, a file, or text.secret data cannot be able to read by other users because it may contains user id and password , sender only can able to create recievers user id and password in which the reciever used to login and view the hidden messages which the user send

DATA EMBEDDING

The suggested real-time implementation of speech steganography, in which the speech or speech is used as a cover object, is described in this module. The majority of the time, speech signals will be in.MP3 format. Because spread spectrum technology is used for steganography, these MP3 speech signals have information in byte sequences that are afterwards converted to bit sequences and then represented in

the range of -1 to 1. This module allows you to split an audio file using the DWT algorithm. Low frequency values are chosen using the DWT algorithm. Message

DATA EXTRACTION

The user can get a stegno file in this module. Data can be extracted using discrete wavelet transform and stegno key. At the receiver's end, the cover file and data are extracted. Data extraction can be done by the receiver. The data can be received in a variety of formats by the receiver. The shares are then combined to create a single shared data set. From a stego video, extract speech frames. Compress with a 1-level 2-D DWT compression. To extract the text data, use the LSB technique on each pixel of the video frame. This will return the original text and speech files.

II. ANALYSIS OF THE SYSTEM

2.1 EXISTING SYSTEM

A large number of alternative chaos-based image and video encryption methods have been proposed and published in recent years. While every algorithm is subjected to a more or less rigorous experimental security study before being released, many of these schemes are broken in subsequent publications. We show in this paper that two of the most common reasons for choosing chaos-based image encryption over traditional strong cryptography, namely computational effort and security benefits, are highly dubious. Several statistical techniques routinely employed to analyse the security of chaos-based encryption schemes are shown to be insufficient for security analysis. We achieve this by building apparently insecure encryption schemes and demonstrating that they perform well and/or pass numerous of these tests in an experimental setting

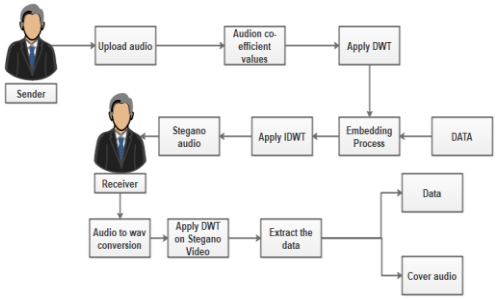
.

2.2 SYSTEM PROPOSED

Steganography is a form of clandestine communication in which a secret message is stored in a covered medium. Steganography is a technique for hiding the existence of a secret message contained in the cover medium. Speech steganography's goal is to hide as much information as possible while minimising the impact on the quality of the cover speech and complicating steganalysis (the process of the opponent finding the secret message). Unlike wideband speech, which can withstand more spectral alterations due to its broader bandwidth, hiding in narrowband speech is a specific task that must be completed with care. The suggested DWT-based real-time speech steganography for military applications is explained in this section.sample paragraph

III SYSTEM DIAGRAM

Architecture of the system is the suggested method for providing steganography to audio files is described in this architecture diagram. The sender can submit an audio file and use the DWT algorithm to extract the features and encrypt the audio. Extract the audio and data as quickly as possible on the receiver side.



SYSTEM ARCHITECTURE

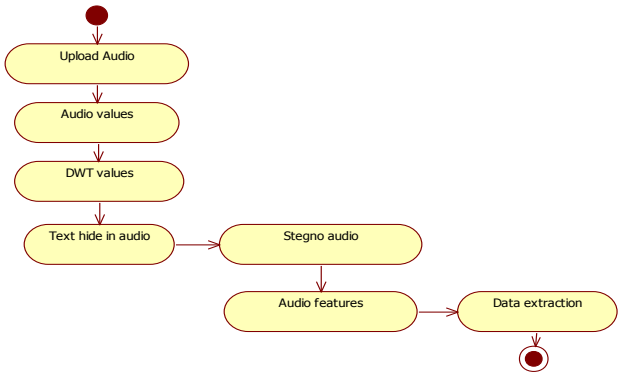
A two-dimensional diagram depicts how data in a system is processed and transferred. The graphical representation identifies each data source and how it interacts with other data sources in order to arrive at a common outcome. Individuals attempting to create a data flow diagram must first identify external inputs and outputs, then determine how the inputs and outputs relate to one another, and then explain how these connections relate and what they result in using graphics. This diagram aids business development and design teams in visualising data processing and identifying or improving certain aspects.

3.1 DATA FLOW DIAGRAM

A two-dimensional diagram depicts how data in a system is processed and transferred. The graphical representation identifies each data source and how it interacts with other data sources in order to arrive at a common outcome. Individuals attempting to create a data flow diagram must first identify external sources and outputs, then decide how the inputs and outputs relate to one another, and then explain how these connections interact and what they result in using images. This graphic aids business development and design teams in visualising data processing and identifying or improving parti cular components.

3.2 ACTIVITY DIAGRAM

Another significant diagram in UML for describing dynamic characteristics of the system is the activity diagram. An activity diagram is essentially a flow chart that depicts the flow of information from one action to the next. The action can be described as a system operation. As a result, the control flow is transferred from one operation to the next. This flow can be sequential, branching, or running at the same time. Using numerous parts such as fork, join, and others, activity diagrams deal with all types of flow control. Activity diagrams provide the same basic goals as the other four diagrams. It depicts the system's dynamic behaviour



IV SYSTEM TESTING

4.1 UNIT TESTING

Collection of tests done by a single programmer prior to the unit's integration into a larger system is referred to as unit testing. The module interface is checked to ensure that data enters and exits the programme unit correctly. The local data structure is inspected to guarantee that data saved temporarily retains its integrity throughout the execution of an algorithm. Boundary conditions are checked to ensure that the module works correctly at the limits or restrictions set by the user. Each of the control structure's independent pathways is examined. All error-handling paths have been put through their paces.

4.2 BLOCK BOX TESTING

Black-box testing is a type of software testing that looks at an application's functioning without seeing inside its internal structures or workings. This test approach can be used at all levels of software testing, including unit, integration, system, and acceptance. Specification-based testing is another name for it.

V CONCLUSION

Speech is naturally considered an ideal carrier by the steganographic research community because to its increasing popularity and widespread effect in mobile communications, and certain relevant steganographic techniques have been successfully created. Speech-based steganography, on the other hand, is a two-edged sword. Illegal application of this approach would aid cybercrime and so constitute a significant threat to information security. As a result, its countermeasure, speech steganalysis, has become a substantial subject worth investigating. Although some useful steganalysis studies for speech have been carried out, all current methods assume that the embedding rate of the steganographic samples to be analysed is precisely known, which is impractical.

.

REFERE NCES

[1]. M. Indra Sena Reddy and Dr. A.P. Siva Kumar, "Secure Data Transmission Using Wavelet-Based Steganography and Cryptography Using the AES Algorithm," International Conference on Computational Modeling and Security, Procedia Computer Science, Vol. 85, 2016, pp. 62–69.

[2]. Marwa M. Emam, Abdelmgeid A. Aly, and Fatma A. Omara, "An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection," International Journal of Advanced Computer Science and Applications, Vol. 7, Issue 3, 2016, pp. 361–366.

[3]. "A Hybrid Approach for Video Steganography Using Edge Detection and Identical Match Techniques," International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016, pp. 896 - 900. Ramandeep Kaur, Pooja, Varsha, "A Hybrid Approach for Video Steganography Using Edge Detection and Identical Match Techniques," International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016,

[4]. Yingnan Zhang, Minqing Zhang, Xiaoyuan Yang, Duntao Guo, and Longfei Liu, "Novel Video Steganography Algorithm Based on Secret Sharing and Error-Correcting Code for H.264/AVC," TSINGHUA SCIENCE AND TECHNOLOGY, Vol: 22, Issue: 2, 2017, pp: 198 - 209; TSINGHUA SCIENCE AND

[5]. Ramadhan J. Mstafa, Khaled M. Elleithy, and Eman Abdelfattah, "A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC," IEEE Access, Volume 5, 2017, pp. 5354–5365.

[6]. Mazhar Tayel, Ahmed Gamal, and Hamed Shawky, "A Proposed Implementation Method of an Audio Steganography Technique," ICACT, pp. 180-184, 2016.

[7]. "A Novel Video Steganography Algorithm in the DCT Domain Based on Hamming and BCH Codes," IEEE 37th Sarnoff Symposium, pp. 208 - 213. Ramadhan J. Mstafa and Khaled M. Elleithy, "A Novel Video Steganography Algorithm in the DCT Domain Based on Hamming and BCH Codes," IEEE 37th Sarnoff Symposium, pp. 208 - 213.

[8]. S. Krishnan and M. S. Abdullah, "Enhanced Security Audio Steganography by Using Higher Least Significant Bit," Journal of Advanced Research in Computing and Applications, Vol. 2, No. 1, 2016, pp. 39-54.

[9]. Ratul Chowdhury, Debnath Bhattacharyya, Samir Kumar Bandyopadhyay, and Tai-hoon Kim, "A View on LSB Based Audio Steganography," International Journal of Security and Its Applications, Vol. 10, No. 2, 2016, pp. 51-62.

[10]. Prabira Kumar Sethy, Kamal Pradhan, and Santi Kumari Behera, "A Security Enhanced Approach for Video Steganography Using K-Means Clustering and Direct Mapping," ICACDOT, 2016, 618-622.

ISSN (Online) : 2455 - 0523

BIOGRAPHIES

NIKESH B is an undergraduate student department of computer science and engineering in paavai college of engineering .

RAMESH KUMAR A is an undergraduate student department of computer science and engineering in paavai college of engineering .

SANTHOSH S is an undergraduate student department of computer science and engineering in paavai college of engineering .

SARANYA R is an Assistant professor department of computer science and engineering in paavai college of engineering .