IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DATA HIDING IN AUDIO FILES

Mrs.S.Jasmin , Ms.B.Shiva Pushpa , M.P.Sakthivel

Instructor, Instructor, Student
DIPLOMA IN INFORMATION TECHNOLOGY
PSG POLYTECHNIC COLLEGE, COIMBATORE, INDIA

Abstract: Secure communication has become essential with the rapid growth of digital data transmission. Traditional methods such as Cryptography protect information by converting it into unreadable formats but may still reveal the presence of secret communication. Steganography provides an alternative approach by hiding the existence of the message itself. This paper presents a method for data hiding in audio files using audio steganography. In this method, an audio file is used as a carrier to embed a secret text message using the Low Bit Encoding technique. A key file is used to enhance security by utilizing ASCII values during the embedding process. The system includes two main modules: an embedding module for hiding the message and an extraction module for retrieving it. The proposed approach ensures secure data transmission while maintaining the quality of the original audio file.

1. INTRODUCTION

The project titled “Data Hiding in Audio Files” focuses on securing information using the technique of Steganography. The term steganography is derived from Greek words meaning “covered writing,” which refers to the practice of hiding information in such a way that its existence cannot be detected

Steganography is similar to covert communication techniques that provide an additional layer of security by concealing the presence of the message. Unlike encrypted messages that may raise suspicion, hidden messages remain unnoticed. In digital steganography, a host file known as a container or cover file is used to hide another message or data within it.

Traditionally, information security relied on techniques such as Cryptography, which use symmetric or asymmetric key systems to encrypt data. However, cryptography protects the content of the message but does not hide its existence. Steganography enhances security by embedding the secret information within digital media such as images, audio files, or software. This technique can also be used for digital watermarking, where hidden trademarks are embedded into media files.

In this work, a technique known as audio steganography is implemented to hide data within audio files. In this process, an audio file acts as a carrier file for embedding a secret text message. A key file containing characters is used for additional security, where the ASCII values of the characters are used during the encoding process. The message is embedded into the audio file using the Low Bit Encoding technique, and the hidden message can later be extracted using the corresponding extraction process.

2. REVIEW LITRATURE

2.1 EXISTING SYSTEM

Nowadays, several methods are used for communicating secret messages for defence purposes or in order to ensure the privacy of communication between two parties. So we go for hiding information in ways that prevent its detection. Some of the methods used for privacy communication are the use of invisible links covert channels are some of existing systems that are used to convey the messages

2.2 PROPOSED SYSTEM

The proposed system uses Audio file as a carrier medium which add another step in security. The objective of the newly proposed system is to create a system that makes it very difficult for an opponent to detect the existence of a secret message by encoding it in the carrier medium as a function of some secret key and that remains as the advantage of this system

3. SYSTEM DESIGN

Design is multi-step process that focuses on data structure software architecture, procedural details, (algorithms etc.) and interface between modules. The design process also translates the requirements into the presentation of software that can be accessed for quality before coding begins.

Computer software design changes continuously as new methods; better analysis and broader understanding evolved. Software Design is at relatively early stage in its revolution.

Therefore, Software Design methodology lacks the depth, flexibility and quantitative nature that are normally associated with more classical engineering disciplines. However techniques for software designs do exist, criteria for design qualities are available and design notation can be applied.

3.1 INPUT DESIGN

Input design is the process of converting a user-oriented description of the inputs to a computer based business system into a program-oriented specification.

The objectives in the input design:

- To produce a cost-effective method of input.
- To achieve a highest possible level of accuracy.
- To ensure that input is acceptable to and understood by the user staff.

AUDIO FILE FORMAT:

An audio format is a medium for storing sound and music. It is a container e.g. 44,100 times per second for CD audio or 48,000 or 96,000 times per second for DVD video) and store the value with a certain resolution (e.g. 16 bits per sample in CD audio). Therefore sample rate, resolution and number of channels are key parameters in audio file formats.

TYPES OF FORMATS:

There are three major groups of audio file formats:

1) Common formats, such as WAV, AIFF and AU.

2) Formats with lossless compression, such as FLAC, Monkey's Audio (filename extensionAPE), WavPack, Shorten, TTA, Apple Lossless,and lossless Windows Media Audio(WMA).

3) Formats with lossy compression, such as MP3, Vorbis, lossy Windows Media Audio (WMA) and AAC.

WAV is a flexible file format designed to store more or less any combination of sampling rates or bitrates. This makes it an adequate file format for storing and archiving an original recording.

WAV FORMAT:

WAV (or WAVE), short for Waveform audio format, is a Microsoft and IBM audio fileformat standard for storing audio on PCs. It is a variant of the RIFF bitstream format method for storing data in "chunks".

A WAVE file is often just a RIFF file with a single "WAVE" chunk which consists of two sub-chunks a "fmt" chunk specifying the data format and a "data" chunk containing the actual sample data.

3.2 OUTPUT DESIGN:

Output design generally refers to the results and information that are generated by the system for many end-users; output is the main reason for developing the system and the basis on which they evaluate the usefulness of the application.

In the project, if the employee has to communicate with other employees they can communicate through send and receive message.

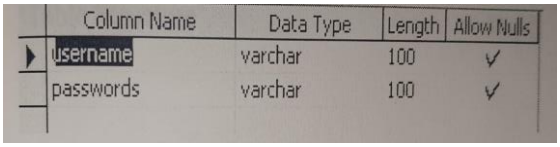
INTERFACE DESIGN

The ODBC (Open Database Connectivity) interface is a pure .NET to execute SQL statement. The ODBC provides a set classes and interfaces that can be used by developers to write database applications. Basic ODBC interactions in its simplest form, can be broken down
into four steps:

1. Open a connection to the database.
2. Execute a SQL statement
3. Process the result
4. Close the connection to the database

TABLE AND DATABASE DESIGN:

ADMIN LOGIN TABLE



Column Name	Data Type	Length	Allow Nulls
username	varchar	100	✓
passwords	varchar	100	✓

Normalization:

Normalization is the process of strutting relational database schema such that most ambiguity is removed. The stage of normalization are referred to as forms and progress from the least restrictive(first normal form)through the most restrictive(Fifth normal form), generally, most database designers do not attempt to implement anything higher then normal form of Boyce code Normal Form.

1 FIRST NORMAL FORM:

A relation is said to be in First normal form (INF) if and each attributed of the relation is atomic. More simply, to be INF, each column must contain only a single value and each now contain in the same column.

2 SECOND NORMAL FORM:

In the Second normal Form, a relation must first fulfill the requirement to be in first Normal Form. Additional, each donkey attribute in the relation must be functionality dependent upon
the primary key.

3 THIRD NORMAL FORM:

A table is said to be in third normal form and every non key attribute is functionality dependent only on the primary key. This normalization process is applied to this system and the normalized tables are given in the above section.

3.3 DATABASE DESIGN :

The database design is a must for any application developed especially more for the data store projects. Since the chatting method involves storing the message in the table and produced to the sender and receiver, proper handling of the table is a must.

In the project, login table is designed to be unique in accepting the username and the length of the username and password should be greater than zero

The complete listing of the tables and their fields are provided in the annexure under the title 'Table Structure'.

4.SYSTEM TESTING

System testing is the stage of implementation that is aimed at ensuring that the system works accurately and efficiently before live operation commences. Testing is vital to the success of the system. System testing makes logical assumption that if all the parts of the system are correct, then the goal will be successfully achieved. A series of testing are done for the proposed system before the system is ready for the user acceptance testing.

The following are the types of Testing:

- Unit Testing
- Integration Testing
- Validation Testing

4.1 UNIT TESTING:

The procedure level testing is made first. By giving improper inputs, the errors occurred are noted and eliminated. Then the web form level testing is made. For example storage of data to the table in the correct manner.

In the company as well as seeker registration form, the zero length username and password are given and checked. Also the duplicate username is given and checked. In the job and question entry, the button will send data to the server only if the client side validations are made.

The dates are entered in wrong manner and checked. Wrong email-id and web site URL (Universal Resource Locator) is given and checked.

4.2 INTEGRATION TESTING:

Testing is done for each module. After testing all the modules, the modules are integrated and testing of the final system is done with the test data, specially designed to show that the system will operate successfully in all its aspects conditions. Thus the system testing is a confirmation that all is correct and an opportunity to show the user that the system works.

4.3 VALIDATION TESTING:

The final step involves Validation testing, which determines whether the software function as the user expected. The end-user rather than the system developer conduct this test most software developers as a process called "Alpha and Beta Testing" to uncover that only the end user seems able to find.

The compilation of the entire project is based on the full satisfaction of the end users. In the project, validation testing is made in various forms. In question entry form, the correct answer only will be accepted in the answer box. The answers other than the four given choices will not be accepted.

MAINTENANCE:

The objectives of this maintenance work are to make sure that the system gets into work all time without any bug. Provision must be for environmental changes which may affect the computer or software system. This is called the maintenance of the system. Nowadays there is the rapid change in the software world. Due to this rapid change, the system should be capable of adapting these changes. In our project the process can be added without affecting other parts of the system.

Maintenance plays a vital role. The system liable to accept any modification after its implementation. This system has been designed to favour all new changes. Doing this will not affect the system's performance or its accuracy.

5.0 CONCLUSION

Steganography transmits secrets through apparently innocuous covers in an effort to conceal the existence of a secret. Audio file Steganography and its derivatives are growing in use and application. In areas where cryptography and strong encryption are being outlawed, citizens are looking at Steganography to circumvent such policies and pass messages covertly.

Although the algorithm presented is a simple one and not without its drawbacks, it represents a significant improvement over simplistic steganographic algorithms that do not use keys. By using this algorithm, two parties can communicate with a fairly high level of confidence about the communication not being detected.

In designing the “Steganography”, utmost care was taken to meet user requirements as much as possible. The analysis and design phase was reviewed. Care was taken strictly to follow the software engineering concepts and principles so as to maintain good quality in the developed system as per the user requirements.

6.0 FUTURE PLANS

Every application has its own merits and demerits. The project has covered almost all the requirements. Further requirements and improvements can easily be done since the coding is mainly structured or modular in nature. Changing the existing modules or adding new modules can append improvements. Further enhancements can be made to the application, so that the web site functions very attractive and useful manner than the present one.

REFERENCES

1. F. Djebbar, B. Ayad, K. Abed-Meraim, and H. Hamam, "Comparative study of digital audio steganography techniques," *EURASIP Journal on Audio, Speech, and Music Processing*, vol. 2012, no. 25, pp. 1–16, 2012.

2. A. Al-Sanjary, A. Ahmed, and R. Al-Sanjary, "Hiding data in audio files: A smoothing-based approach to improve the quality of the stego audio," *Heliyon*, vol. 6, no. 3, 2020.

3. F. S. Mohamad, N. S. M. Yasin, and M. Iqtait, "Information hiding based on audio steganography using least significant bit," *International Journal of Engineering and Technology*, vol. 7, no. 4, pp. 334–336, 2018.

4. R. H. Ali, "Steganography in audio using wavelet and DES," *Baghdad Science Journal*, vol. 12, no. 2, pp. 431–436, 2015.

5. K. Singh and P. Jain, "Hiding secured text data in audio signals using 3-LSB technique," *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 6, no. 1, pp. 229–233, 2020.

6. N. Cvejic and T. Seppänen, "Increasing robustness of LSB audio steganography using a novel embedding method," in *Proceedings of the IEEE International Conference on Information Technology: Coding and Computing*, 2004, pp. 533–537.

7. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol. 35, no. 3–4, pp. 313–336, 1996.

8. N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *IEEE Security & Privacy*, vol. 1, no. 3, pp. 32–44, 2003.