Malaya Journal of Matematik, Vol. S, No. 2, 4564-4568, 2020

https://doi.org/10.26637/MJM0S20/1177

New Innovative Secure Audio Stenography Using Frequency Hopped Spread Spectrum Techniques in Mobile Computing

M. Jeyalilly[1], S. Kannan[2], and A. Muthukumaravel[3]

Abstract

In this digital world, there is a tremendous amount of information sharing due to improved networking facilities. The data that we transmit also needs to be secured. The principle of "Steganography." is introduced by the need for secure touch. Steganography, the term itself means that knowledge is part of the database; it's the best strategy to conceal sensitive Awareness by the use of cover products. A text could be secret knowledge, an image or an audio file However; various steganographic techniques are available according to the classified information format. In this proposes an audio steganographic device approach since the information is in text format, the above offers A distinctive forum for in the audio file, hide the hidden knowledge. Several steganographic methods follow the LSB insertion technique in order to mask the hidden information. But there are many statistical techniques available for evaluating whether a stego object has been subjected to LSB embedding.

Stable audio stenography using Frequency Hopped Spread Spectrum techniques in mobile computing is used in this proposed process. A technique for communicating radio signs is this recurrence bouncing spread reach (FHSS) quickly changing the carrier frequency between several different frequencies which occupy a broad spectral band. A code that is transmitter and the receiver controls the changes. (FHSS) is used to avoid interference, to avoid eavesdropping and to allow multiple access (CDMA) communications for code-division. A frequency hopping method used in this technique, where users are made to switch the frequency of use, so called frequency hopping, from one to the other at a specified time interval. For example, sender 1 was assigned a frequency for a fixed period of time. Sender 1 now hops to the other frequency after a little bit, and sender 2 utilizes the first frequency previously used by sender one. This is called reuse of frequency. To give a reliable transmission, data frequencies are skipped from one to the other. The amount of time spent is known as Dwell Time in a frequency hop.

Keywords

Stenography, Frequency, Mobile Computing.

[1,2] *Department of Computer Science, Bharath Institute for Higher Education and Research, Selaiyur, Chennai-600073, Tamil Nadu, India.*

[3] *Dean, Faculty of Arts and Science, Bharath Institute for Higher Education and Research, Selaiyur, Chennai-600073, Tamil Nadu, India.*

Article History: Received **01** October **2020**; Accepted **10** December **2020**

Contents

1. Introduction

Major changes in the general society were triggered by the rapid improving The Internet and the new information movement. Adaptable and simple to-utilize innovation and diminishing advanced item costs (e.g. compact CD and mp3 players, DVD players, CD and DVD recorders, PCs, PDAs) have made it conceivable to fabricate, edit and distribute multimedia data for consumers from around the world. Broadband Internet connections allow individuals to transmit enormous interactive media documents and make precise advanced duplicates of them, with practically errorless information transmission.

It is distributed in an unsecured way to transmit confidential messages and data across the Internet, but everyone has something to keep hidden One of the most effective ways of protecting your privacy is the audio data hiding system. The most difficult tool to use when dealing with steganography is the conversion of coded messages into audio. This is because the human hear-capable system (HAS) has an especially remarkable arrived at that it can respond to them. The solitary (HAS) inadequacy is endeavouring to isolate disturbances (loud sounds overpower quiet sounds) and this is what ought to be used to encode secret messages in sound without being heard. While choosing an encoding strategy for sound, there are two standards to recall. They are computerized design for sound and mode for sound transmission. Typically, three fundamental advanced sound configurations are being used. They are Sample Quantization, Perceptual Sampling and Temporal Sampling Rate. In the 16-bit direct examining design utilized by mainstream sound arrangements including Sample Quantization (.WAV and .AIFF). The Temporary Sampling Rate utilizes selectable frequencies for sound testing (KHz). Perceptual Sampling and last sound organization. By translating just those pieces that are heard by audience, this configuration incredibly changes sound measurements, accordingly holding when choosing an encoding method for sound, there are two standards to recall. They are the high level course of action for sound and the vehicle for sound transmission. Customarily, three essential mechanized sound designs are being utilized. They are Sample Quantization, Temporal Sampling Rate and Perceptual Sampling. The 16-cycle direct inspecting design utilized by mainstream sound organizations including Sample Quantization (.WAV and .AIFF). The Temporary Sampling Rate utilizes selectable frequencies for the sound testing (KHz). Perceptual Sampling is the last sound arrangement. By deciphering just those pieces that are heard by the sound however changing the sign. ISO MPEG, the most common digital audio on the Internet today, uses this format (MP3). When encoding secret audio messages, the medium of transmission must also be considered. Many apps are Internet-based now a day and in some instances it is preferred that the contact be kept confidential. And, in other words,

steganography_medium = hidden_message + carrier + steganography_key

2. Histroy of steganography

Since the beginning, an assortment of strategies has been utilized to shroud data. As per the Greek history specialist Herodotus, a Greek named Histiaeus chose to convey a message to an inaccessible city through a human messenger. To pass these guidelines securely, Histiaeus shaved his courier's head, composed the message on his uncovered scalp and afterward trusted that the hair will develop back. This tedious correspondence technique, be that as it may, was compelling as the courier could go without raising any uncertainty through reviews. At the objective, the foreseen recipient shaved the top of the courier and read the letter. A later utilization of steganography was to help slaves escape preceding the common war. The Underground Railroad was one of the main departure courses utilized by slaves. To show data, quilts, hanging out to dry, were utilized unnoticeably. The stitches had extraordinary examples that offered subtleties to the captives to aid their getaway.

2.1 Classification of steganography:

Generally steganography is classified in following aspects A typical classification of [ASW 03] steganographic techniques is shown in Figure 1. Technical steganography utilizes scientific techniques. In certain non-obvious cases.A visual semagram uses guiltless looking or regular actual items to pass on a reason, for example, doodles or the area of stuff on a work area or site. A book semagram covers a message by modifying the presence of the transporter's content, for example, inconspicuous content. Changes in text dimension or shape, adding extra spaces, with letters or transcribed content being extraordinary.

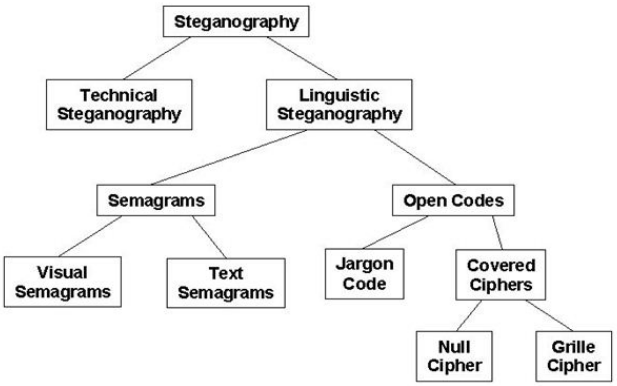

Figure 1. Classification of Techniques of Steganography

3. Digital audio

Numerous normal computerized steganography strategies utilize graphical pictures or sound documents as the transporter medium. Sound encoding includes transformation of a simple sign to a spot stream. Simple voice and music sound of various frequencies, communicated by sinus waves. The human ear can ostensibly hear frequencies in the scope of 20-20,000 cycles/second (Hertz or Hz). The sound is simple, which implies that it is a sign that is consistent. The transformation of the ceaseless sound wave to a bunch of tests that can be deciphered by a succession of zeros and ones includes carefully putting away the sound. Simple to-advanced change is cultivated by testing the simple sign (with a receiver or other sound finder) and changing those examples over to voltage levels. The volt, utilizing a plan called adjustment of heartbeat code, A coder-decoder or codec is known as the PC that plays out this transformation

As shown in Figure 2, the modulation of the pulse code gives only an estimation of the first simple sign. For instance,

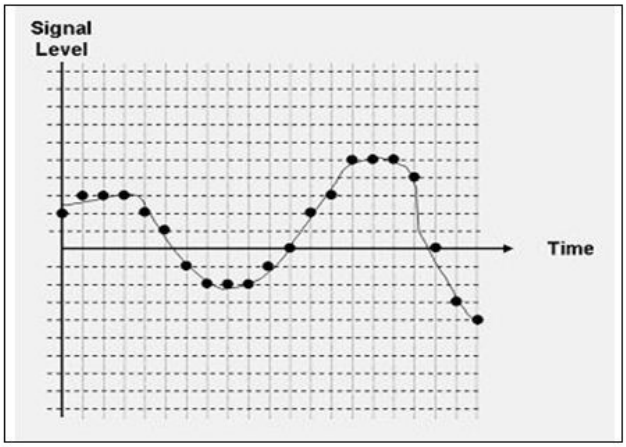

Figure 2. Modulation of simple pulse code

if the simple sound level was estimated at a degree of 4.86, the regulation of the beat code would be changed over to five. This is known as a quantization defect. Different sound executions indicate an alternate number of levels of heartbeat code regulation, so this 'bug' is practically imperceptible by the human ear. Each voice test is converted into an eight-bit esteem (0-255) by the phone organization, usually, 16-cycle esteems (0-65,535) [ASM 03] are utilized for music applications. Inspecting simple signs at a pace of double the most noteworthy recurrence segment of the sign is important with the goal that the first can be accurately duplicated from the examples alone. In the 0-4000 Hz recurrence range, the human voice is carried on the broadcast communications organization. Music sound frameworks accept the full reach and 44.1 kHz testing pace of the human ear.

The touch pace of uncompressed music can be handily assessed to be 1,411,200 pieces for each second, from the examining rate (44.1 kHz), beat code adjustment goal (16 pieces), and number of sound channels (two). This would imply that a one-minute sound document would devour 10.6 MB (1,411,200*60/8 = 10584000) (uncompressed). One evident arrangement is to decrease the quantity of channels to one or to diminish the testing rate to as low as 11 kHz in specific cases. For pressure, some codec's utilize restrictive plans. Both of these arrangements reduce the clearness of the tone.

WAV- Basic audio file format that is primarily used on Windows PCs. CD-quality sound files are widely used to store-uncompressed (PCM) sound records, which implies they can be huge in size, around 10 MB for each moment of sound. To decrease the file size, it's less than fine, documented It is possible to encode wave files with a variety of codec's.

MP3- The most common format for uploading and storing music is the layer-3 MPEG design. MP3 records are packed to the size of an identical PCM document of about one-tenth, thus retaining decent audio quality by removing parts of the audio file that are practically inaudible. For music collection, we suggest the MP3 format. For voice storage, didn't pleasant.

au – the standard sound record configuration used by sun, Unix and java. The sound in au records can be PCM or compacted with the ulaw, alaw or G729 codecs.

aiff -The standard sound record design utilized by Apple. It resembles a wav record for the Mac.

wma-The popular Window media Audio format owned by Microsoft. Designed with DRM (Digital Rights Management) abilities for copy protection.

ra- a Real Audio Format designed for streaming audio over the internet. The .ra format allows files to be stored in a self-contained fashion on a computer, with all of the audio data contained inside the file itself.

ram– a text file that contains a link to the internet address where the Real Audio file is stored. The .ram file contains no audio data itself. The above table clearly explain Sun, Unix and Java are clearly specified in the table above and use the same audio file format. The sound can be PCM or compacted with the codecs ulaw, alaw or G729 in au records. There are many sound highlights that can be modified in manners that are indistinguishable to human detects, and these unpretentious changes, for example, slight changes in stage point, voice rhythm, and recurrence, can ship covered data.

4. Audio steganography

A similar sound record design is utilized various languages. To essential models of sound steganography are transporter (sound record), message and secret word. A cover record that ensures the mystery information is regularly alluded to as a transporter. The message is the data the sender wishes to keep covered up. A message can be essential substance, picture, sound, or any record type. A mystery word is known as a stego-key, which infers that solitary the recipient who understands the relating unwinding key can get the message from a cover-report. The gathered information cover-archive is insinuated as the [JRA 11] stego-record.

The method of knowledge hiding consists of the two steps below.

1. Recognizable proof of a cover-repetitive record's parts. Excess pieces are those pieces that can be changed without bargaining the yield or losing the cover-uprightness. Records

2. To embed the secret information in the cover report, the outdated pieces in the cover record are replaced with bits of secret information.

5. Problem discussion

In this segment, some common audio techniques used to conceal confidential information are presented. Several of the software implementations of these techniques are available on the Web and are mentioned in the section relevant to them. Previous knowledge of signal processing methods and other areas of high-level mathematics is provided by many of the above approaches. One of the first problems when designing

Table 1. Some Common Digital Audio Formats

Types of audio	File formet-extention	Codec
AIFF (Mac)	aif, aiff	Pulse code modulation (or other)
AU (Sum/Next)	. au	μ-law (or other)
CD audio (CDDA)	n / a	Pulse code modulation
MP3	mp 3	MPEG Audio Layer III
Windows Media Audio	wma	Microsoft proprietary
Quick Time	.qt	Apple Computer proprietary
RealAudio	ra, ram	Real Networks proprietary
WAV	.wav	Pulse code modulation (or other)

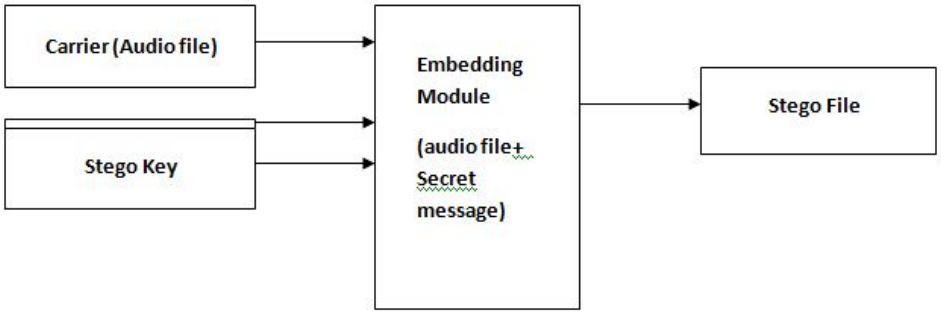

Figure 3. Steganographic Model for Audio

a data-hiding scheme for audio is the sound signal that will pass between encoding and decoding.

The carrier file is taken as a WAV audio file format in the suggested technique and the hidden message is a text format file. The carrier file is larger than the file-containing hidden letter. Here, the transmitter that is stored in a text file receives a key. In the first 2 bytes of the wav file, the header is put inside. The next two bytes are allocated to the secret key, except for the first 2 bytes, and the rest of the bytes of the file are all about the data. There will be no changes to be included in the header section. For embedding, the segment on Key and Data is used. Start from the 3rd data byte sample.

With regards to the point of recovering information on the collector side, the recuperation calculation should be followed: first, change the sound message into a parallel configuration that began from the source as a stego-object. Leave the initial 16 MSB bits with no adjustment in them. First, the beginning of the 32nd MSB bit is retrieved and the decryption process is performed with the transmitter's known key produced and the stego-file recovers the secret message.

6. Conclusion

Steganography is a fascinating and powerful technique used to hide documents history. Strategies can be utilized to uncover such shrewd procedures, yet information that there are even such techniques is the main move. There are also some good reasons for this form of data hiding to be used, including cryptography for items such as passwords, key processes or a more secure storage system. However, the innovation is anything but difficult to utilize and hard to identify. The more you think about its qualities and highlights, the more we'll be in the game ahead.

References

[1] S.S.Divya, M.Ram Mohan Reddy, Hiding Text In Audio Using Multiple LSB Steganography And Provide Security Using Cryptography, *IJSTR*, 1(6)(2012), 2277-8616.

[2] K. Sakthisudhan, P.Prabhu, P.Thangaraj, Secure Audio Steganography For Hiding Secret Information, *IJCA*, 2(3)(2012).

[3] Navnaths Narwade, Vikas Bhagasara, Mahesh Kanthali, Rushikeshpaiwar,Enhanced Data Hiding Model in Audio to Ensure Secrecy, *IJEIT*, 2(9)(2013).

[4] P. Jeyaram, H.R. Ranganatha, H.S.Anupama,Information Hiding Using Audio Steganography-A Survey, *IJMA*, 3(3)(2011).

[5] PoulamiDutta, Debanath Bhattacharyya, Tai-hoonKim, Data Hiding in Audio Signal: A Review, *IJDTA*, 2(2)(2009).

[6] K.P.Adhiya, Swati A.Patil,Hiding Text In Audio Using LSB Based Steganography, *IISTE*, 2(3)(2012).

[7] R. Sri Devi, Dr.A. Damodaram, Dr.SVL. Narasimham, Efficient Method Of Audio Steganography By Modified LSB Algorithm And Strong Encryption Key With Enchanced Security, *JATIT*, 2(7)(2009).

[8] Unal TATAR, Tolga MATARACIOGLU, *Analysis and Implementation of Distinct Steganographic Methods*, 2013.

[9] Bhagayashri. A.Patil, Vrishali A.Chakkarwar, Review Of An Improved Audio Steganographic techniques Over

LSB through Random Based Approach, *IOSR-JCE*, 9(2013), 30-34.

[10] Pratap Chandra Mandal, Modern Steganographic Technique: A Survey, *IJCSET*, 3(9)(2012).

⋆⋆⋆⋆⋆⋆⋆⋆⋆
ISSN(P):2319 – 3786
Malaya Journal of Matematik
ISSN(O):2321 – 5666
⋆⋆⋆⋆⋆⋆⋆⋆⋆