Journal of Computer Engineering and Information Technology

Opinion Article A SCITECHNOL JOURNAL

Review of an Improved Stenographic Technique through Random Based Approach

Mokhtar Hasan*

Department of Computer Engineering, University of Rome, Aldo Moro, Roma, Italy

***Corresponding author:** Mokhtar Hasan, Department of Computer Engineering University of Rome, Aldo Moro, Roma, Italy. E-mail: hsaniktar@gmail.com

Received date: 06 June, 2022, Manuscript No. JCEIT-22-61675;

Editor assigned date: 08 June, 2022, PreQC No. JCEIT-22-61675(PQ);

Reviewed date: 15 June, 2022, QC No JCEIT-22-61675;

Revised date: 13 July, 2022, Manuscript No. JCEIT-22-61675(R);

Published date: 29 July, 2022, DOI:10.4172/jceit.1000240.

Description

The huge amount information exchange takes place due to enhanced facilities of networking. Therefore it is necessary to secure the information which we transmit. The need for secured communication introduces the concept of "Steganography". Steganography, the word itself indicates that information within information; it is the best technique to hide the secret information by using cover objects. Secret information may be a text, image or an audio file. But as per secret information format there are different steganography techniques are available. This paper proposes a method of audio steganography system that provides a unique platform to hide the secret information in audio file though the information is in text, image or in an audio format. So there is no need to go for different techniques of steganography as per information format. Many steganography methods follow the LSB insertion technique to hide the secret information. But there are many statistical techniques available to determine if a stego object has been subjected to LSB Embedding. The proposed system hides secret information in audio file through random based approach and provides security by using PKE algorithm. This paper focuses on combining the strengths of cryptography and steganography for secured communication. Audio Steganography, PKE algorithm, Random based approach. Due to digitization, information and other works become easily available in digital form. So it is possible that when information exchange takes place during communication, an intruder may interpret with secret message to make copy of our secret information or to destroy our information. The first possibility may result in to large-scale unauthorized copying which might undermine the music, film, book, and software publishing industries. And the second possibility may result to destroy of information which again results in to miscommunication. These two problems had given an importance to Information Security.

Stego Audio Signal

Steganography plays a very important role in information security as various methods to hide the information in cover object are available. Steganography means "concealed writing" which is originated from Greek words "stegano" means covered and "graphie" means writing. Information security using steganography is the way of writing hidden messages in such a way that other than sender and intended recipient, nobody knows the existence of the message in cover object. Here the secret message and cover object may be in any format like text or image or audio file. For each format of information, steganography provides different way to hide the secret message. Only the drawback is that as per information format, steganography method is selected. Why to go for method selection? This paper overcomes the problem of steganography method selection. The proposed system of audio steganography combines the features of both cryptography and steganography. It allows the user to select any format of information among text, image and audio which is to be transmitted. Cryptography is used to encrypt the secret message. For encrypting secret message PKE (Public Key Encryption) algorithm is used. This encrypted message is then hidden in cover object in an audio file. Finally this stego audio file is transmitted to intended recipient to avoid the possible vulnerable attacks of intruder. In digital audio steganography system, secret message is embedded in audio file. The binary sequence of an audio file (cover object) is slightly changed by adding secret message in it. The audio file formats used by currently existing audio steganography software are WAV, AU, and even MP3 sound files. Audio steganography is a way of embedding information inside an audio signal. As data is embedded in the signal, the signal is get modified. This modification should not be made identified to the human ear. Embedding secret messages in audio file is more difficult than embedding messages in digital image. In order to hide secret messages, various methods for embedding information in digital audio have been introduced. These methods range from simple algorithms which insert information in the form of noise in audio.

Signal to more powerful methods that uses signal processing techniques to hide information. Maximum steganography method uses Least Significant Bit (LSB) insertion method to hide the secret message in cover object. But there are various techniques available to detect secret message which is present at LSB position. Therefore in proposed system, the secret message is hidden in cover object through random based approach. Parity coding technique operates on a group of samples instead of individual samples. Here individual samples are grouped and parity of each group is calculated. For inserting message bit one by one, check the parity bit of a group of samples. If the parity bit and message bit matches do nothing. Otherwise change the LSB's of any one of the individual samples in that group to make the parity bit equal to the message bit. In echo hiding method data is embedded in the echo part of the host audio signal. The echo is a resonance added to the host signal and hence the problem with the additive noise is avoided here. While using echo hiding three parameters are to be considered, they are initial amplitude, offset (delay), and decay rate, so that echo is not audible. The main disadvantage of this method is lenient detection and low detection ratio. Due to its low embedding rate and low security no researches are going on echo hiding technique. Frequency domain techniques and wavelet domain technique comes under transform domain. The main techniques under frequency domain are tone insertion, phase coding and spread spectrum technique.

Spread Spectrum Technique

Frequency masking property is exploited in tone insertion method. A weak pure tone is masked in the presence of a stronger tone. This property of inaudibility is used in different ways to embed information. Phase coding method is based on the fact that the phase components are not audible to human as noise components. This method embeds the secret message bits as phase shift in the phase

spectrum of the original audio signal. The method tolerates better signal distortion, better robustness but it does not survive low pass filtering. Here the secret message is inserted only at the phase vector of the first signal segment. This technique takes the advantage of masking property of HAS. A masking threshold is calculated using a psycho acoustic model. The spread signal now lies below the masking threshold. Apart from phase shifting, here the secret message is distributed along with the host signal. Here the final signal occupies a bandwidth which is more than what is actually required for transmission. Wavelet domain is suitable for frequency analysis because of its multi-resolution properties that provides access to both most significant parts and details of spectrum. Wavelet domain techniques works with wavelet coefficients. Upon applying the inverse transform, the stegano signal can be reconstructed.

Now days, multiple techniques of steganography are present but are in scattered format. For example text to audio steganography, image to audio steganography, audio to audio steganography. The proposed system combines the above specified techniques of steganography in to one system along with each methods good quality features. Maximum audio steganography algorithms basically work with LSB insertion method. To overcome the drawbacks of existing system, an efficient encryption algorithm should be used. So the proposed system uses public key encryption algorithm through random based approach. It also provides a good platform of to perform all steganography techniques under one system. This system consists of text to audio, image to audio as well as audio to audio steganography. Input given to the system is secret message which is either a text file or image file or an audio file. After this a cover object audio file is selected to perform encryption as well as to hide the encrypted data. Secret message file is converted to binary file format. Among this binary format, a salt of 1024 byte is selected for encryption. Simultaneously a salt is also taken from audio file, where salt is nothing but a small part of file which is to be read. Audio file salt selection is based upon random based approach means random salt from cover audio file is selected.