International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

REAL TIME IMPLEMENTATION OF SPEECH STEGANOGRAPHY FOR SECURITY APPLICATIONS

G. Swathi[1], Morla Siri Chandana[2], Kottam Hemanth[2], Goli Keerthana[2], Indur Srihari[2]
[1]Assistant Professor, [2]UG Scholar, [1,2]Department of Electronics and Communication
[1,2]Malla Reddy Engineering College and Management Sciences, Medchal, Telangana.

ABSTRACT
The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically in simple words "steganography means hiding one piece of data within another". Modern steganography uses the opportunity of hiding information into digital multimedia files and at the network packet level. Numerous conditions of workmanship algorithms proposed to build up an image Steganography, video Steganography et cetera. In any case, however those algorithms have been experiencing the substantial stockpiling region and even much complex to implant the information into the video. Here, we had implemented a speech Steganography using spread spectrum with FFT domain. It has performed good enough simulations with low bit error rate and excellent imperceptibility. The technique embeds the hidden information in the transformation domain of the Audio and uses simple arithmetic equations. Besides, the embedded confidential information can be extracted from stego-Audios without the assistance of original Audio data. The information to be embedded must first modulated using the pseudo-noise. This work discusses implementation of the method in audio data to hide text message.

Keywords: Speech steganography, security applications, spread spectrum.

1. INTRODUCTION

Steganography is the art or study of hiding information by inserting secret messages in other messages. Medium where information is inserted can be anything. This medium is called the cover object. Steganography that is applied to hide information on the cover of digital objects is called Digital Steganography. Cover objects that are used in digital steganography can vary, for example in the image archive. Steganography algorithms in the image archive have been widely developed. Meanwhile, steganography algorithms in audio archive are relatively few. This paper discusses the application of digital steganography on audio archives using the method of Direct sequence Spread Spectrum. The author also found relating book and paper that describe the theory about audio steganography using spread spectrum.

Steganography in the audio archive is not as easy as in the image archive. Unlike the archives of raw images, raw sound files are usually larger. In comparison, the raw image file type and resolution of 1280x800 24-bit color (standard resolution of desktop screen) has a size of about 3 MB of data. While the raw audio files with 44.1 kHz sampling frequency, 16-bit stereo channels with 4 minutes duration (the standard duration of song) has a size of about 40 MB of data. The difference is quite large, resulting in the implementation of steganography in audio data becomes more difficult. As an illustration, suppose we use the Discrete Fourier Transform to convert the data domain, then the audio archives clearly require substantial cost because the number of samples that must be transformed is much greater. Moreover, suppose we use the LSB method, the noise generated at the sound archive is greater. This is because

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

the range of the sound signal is lower than the pixel signal. Pixel is encoded by 24 bits, while sound signal is encoded by 15 bits (because there are positive and negative sound signal). In addition, the use of raw audio files (WAV) is less frequent than the raw image files (BMP), because the size in audio files is too large. Therefore, we need such a scheme that enables us to preserve the hidden messages, even if the audio files is compressed. In the next section, the author will explain some basic theories that need to be known in advance.

The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically in simple words "steganography means hiding one piece of data within another".

Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level.

Hiding information into a media requires following elements

- The cover media(C) that will hold the hidden data
- The secret message (M), may be plain text, cipher text or any type of data
- The stego function (Fe) and its inverse (Fe-1)
- An optional stego-key (K) or password may be used to hide and unhide the message.

The stego function operates over cover media and the message (to be hidden) along with a stego-key (optionally) to produce a stego media (S).The schematic of steganographic operation is shown below.

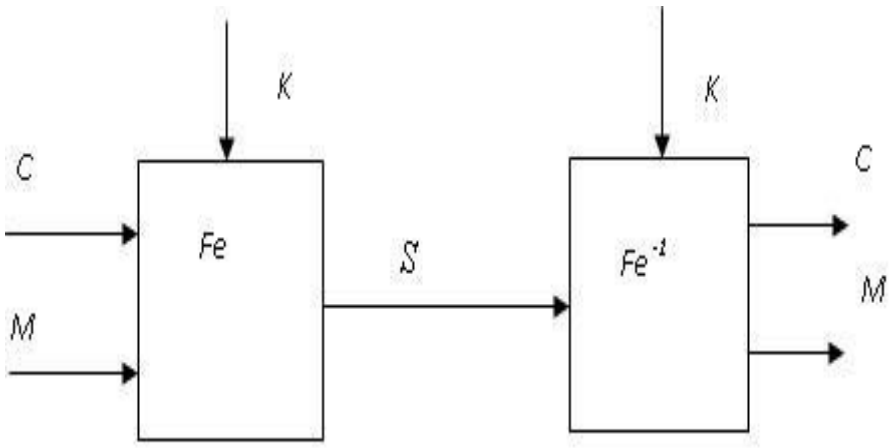


Fig. 1: The steganographic operation.

Steganography and Cryptography are great partners despite functional difference. It is common practice to use cryptography with steganography.

Fast Fourier Transform (FFT)

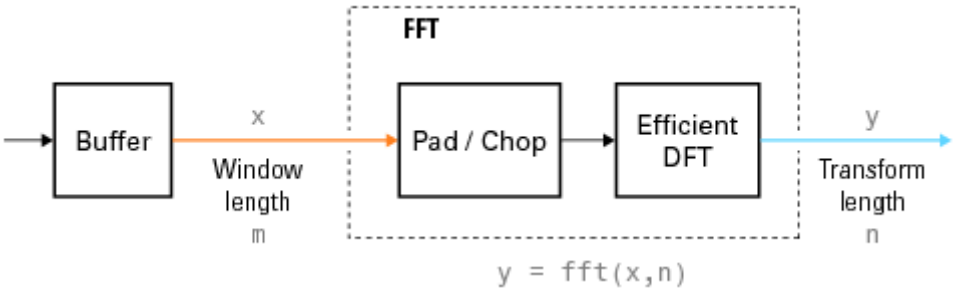
DFTs with a million points are common in many applications. Modern signal and image processing applications would be impossible without an efficient method for computing the DFT. Direct application of the definition of the DFT (see Discrete Fourier Transform (DFT)) to a data vector of length n requires n multiplications and n additions—a total of 2n2 floating-point operations. This does not include the generation of the powers of the complex nth root

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

of unity ω. To compute a million-point DFT, a computer capable of doing one multiplication and addition every microsecond requires a million seconds, or about 11.5 days.

Fast Fourier Transform (FFT) algorithms have computational complexity O(n log n) instead of O(n2). If n is a power of 2, a one-dimensional FFT of length n requires less than 3n log2 n floating-point operations (times a proportionality constant). For n = 220, that is a factor of almost 35,000 fasters than 2n2.

When using FFT algorithms, a distinction is made between the window length and the transform length. The window length is the length of the input data vector. It is determined by, for example, the size of an external buffer. The transform length is the length of the output, the computed DFT. An FFT algorithm pads or chops the input to achieve the desired transform length. The following figure illustrates the two lengths.



The execution time of an FFT algorithm depends on the transform length. It is fastest when the transform length is a power of two, and almost as fast when the transform length has only small prime factors. It is typically slower for transform lengths that are prime or have large prime factors. Time differences, however, are reduced to insignificance by modern FFT algorithms such as those used in MATLAB. Adjusting the transform length for efficiency is usually unnecessary in practice.

2. PROPOSED IMPLEMENTATION

Spread Spectrum Method

Spread spectrum is a technique of signal (electrical electromagnetic, or acoustic) generated in a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth. This technique is performed with a variety of reasons, including to secure communications network, strengthening the wave that is sent from interference or jamming and to avoid detection.

Spread spectrum was originally a technique used for radio communications for security reasons and to avoid jamming. Radio signals are sent intentionally deployed on a wider frequency range. The resulting radio signal is only visible as regular noise (static noise) and cannot be interpreted in the normal way. Spread spectrum has a very important characteristic that is its resistance from jamming and interference. If the signal is lost partially, the information conveyed can still be perceived. This property is suitable for steganography on audio file format which may experience compression, especially lossy compression like MP3. This spread spectrum steganography on audio data will be implemented with the following scheme:

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

1. Transform the audio cover object in time-domain into frequency-domain using Fast Fourier Transform (FFT)
2. Adding the information signal by using spread-spectrum to the cover object in frequency-domain
3. Transform back the audio cover object from frequency-domain into time-domain using inverse FFT

With this scheme, the audio cover objects are expected to be more resistant from the compression process, or manipulation, because the information is added to the frequency-domain.

The method has several types of spread spectrum, whereas this paper will discuss the direct sequence Spread Spectrum (DSSS). Direct sequence spread spectrum is a technique that uses Pseudo Noise Sequence (PN Sequence). The modulation technique is describing as follow:

1. Prepare the information signal to be spread
2. Prepare pseudo noise sequence that is used to modulate the information signal
3. Modulate the information signal with the PN sequence. However, the frequency of PN sequence must be greater (faster) than the frequency of information signal
4. Send or insert the resulting signal.
5. The recipient must have the same PN sequence to understand the message.
6. Modulate the resulting message with the same PN sequence
7. The result is the information signal.

Fast Fourier Transform

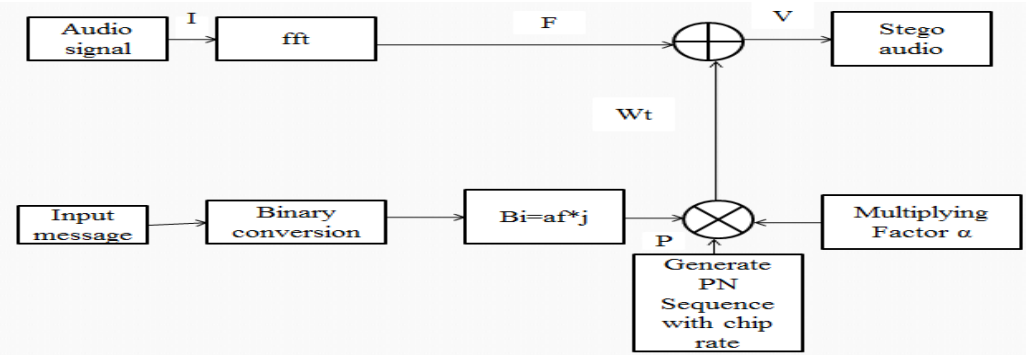


Fig. 2: FFT spread spectrum-based steganography.

Fast Fourier Transform (FFT) refers to a special class of algorithms used to compute DFT and inverse DFT efficiently. FFT algorithm is an important use for this DSSS implementation. If we calculate the DFT by brute-force, it requires a very large cost with complexity $O(n2)$ and is not practical for this use. Meanwhile, the FFT complexity is only$O(n\ logn)$.

FFT algorithm is very important to be implemented properly, because if the process of transformation takes a long time, the application of steganography in audio data using DSSS becomes impractical. The author tried several FFT and naïve DFT algorithms. Actually, the FFT libraries are widely available. One of the famous libraries was the Fastest Fourier Transform in the West (FFTW). However, we do not use FFTW with a number of reasons. FFTW can compute FFT very fast. It is possible because a certain FFTW planning features.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Before calculating the FFT, FFTW is estimating the algorithm that will be used. So if the same array is transformed again, the transformation process is faster, although the planning process takes longer time. However, because the audio data for steganography is very divers in length, of course, planning feature from FFTW is less suitable for application because it gives results that are not too much different from the ordinary FFT algorithm implementation.

PROPOSED METHOD

DWT:

The Stationary wavelet transform (SWT)[1] is a wavelet transform algorithm designed to overcome the lack of translation-invariance of the discrete wavelet transform (DWT). Translation-invariance is achieved by removing the down samplers and up samplers in the DWT and up sampling the filter coefficients by a factor of jth level of the algorithm.[2][3][4][5] The SWT is an inherently redundant scheme as the output of each level of SWT contains the same number of samples as the input – so for a decomposition of N levels there is a redundancy of N in the wavelet coefficients. This algorithm is more famously known as "algorithm à trous" in French (word trous means holes in English) which refers to inserting zeros in the filters. It was introduced by Holschneider et al.

The following block diagram depicts the digital implementation of SWT.

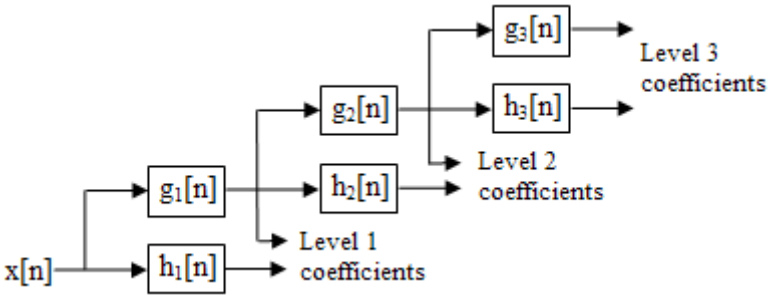


Fig. 3: A3 level SWT filter bank.

In the above diagram, filters in each level are up-sampled versions of the previous (see figure below).

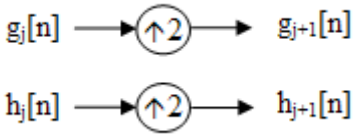


Fig. 4: SWT filters.

Conventionally, Fourier Transform (FT) is used as a signal analysis tool that converts the signal into constituent sinusoids of different frequencies. The major drawback with Fourier Transform is the loss of time information. Short Time Fourier Transform (STFT) is considered as a compromise between the time and frequency information. In STFT, a window is applied to the signal and then Fourier Transform is computed. The preciseness of STFT depends on window shape and size. Wavelet transform preserves both the time and frequency information by decomposing the signal in a hierarchy of increasing resolution. Wavelet transform of signal is represented as

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

$$W(a,b) = \int_{-\infty}^{\infty} x(t)\,\psi_{a,b}(t)\,dt,$$

where is the dilated and translated version of the mother wavelet and is calculated as

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t-a}{b}\right),$$

here a and b are real and positive number representing dilation and translation. Similarly, discrete wavelet transforms of signal $x[n]$ is represented as'

$$W(k,l) = \sum_{m=-\infty}^{\infty} x[m]\,\psi_{k,l}[m],$$

where $\psi k, l[m]$ is the dilated and translated version of the mother wavelet ψ and is calculated as

$$\psi_{k,l}[m] = 2^{-k/l}\psi\left[2^{-k}m - l\right].$$

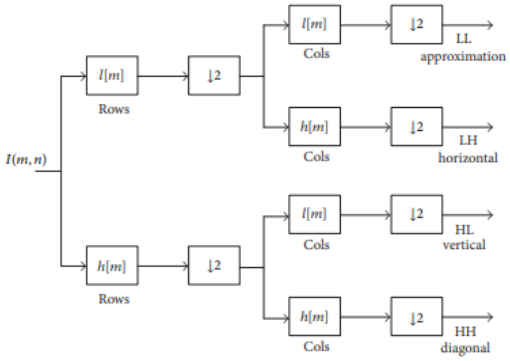


Fig. 5: Single level discrete wavelet transform decomposition of image into four sub bands.

Stationary wavelets transform (SWT) solves this problem of shift invariance. SWT differs from conventional DWT in terms of decimation and shift invariance, which makes it feasible for change detection, pattern recognition, and feature extraction. In conventional DWT, at each level of transform input signal is firstly convolved with low $l[m]$ and high $h[m]$ pass filter and then decimated by a factor of two to obtain wavelet transform coefficients. The resolution after DWT remains the same as the input signal. In SWT, the input signal is convolved with low $l[m]$ and high $h[m]$ pass filter in a similar manner as in DWT but no decimation is performed to obtain wavelet coefficients of different sub bands. As there is no decimation involved in SWT, therefore the number of coefficients is twice that of the samples in the input signal.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

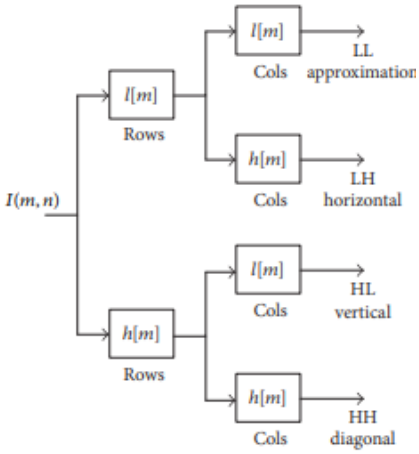


Fig. 6: Single level stationary wavelet transform decomposition of image into four sub bands.

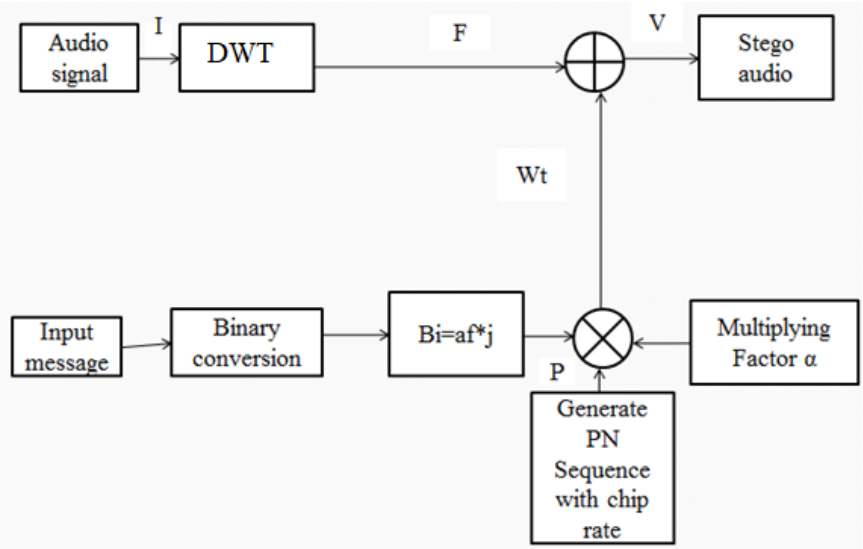


Fig. 7: DWT based speech steganography.

3. EXPERIMENT RESULTS

This section describes the experimental analysis of proposed speech steganography with comparison to the FFT-based approach. All the simulations have been done in MATLAB 2018a environment. We tested the proposed and existing methods for various speech samples of different kind of persons like male, female, child and old age with a chip rate $cr = 400$. First, it will ask the user to speak anything for a period of 5sec (this can be varied according to user interest).

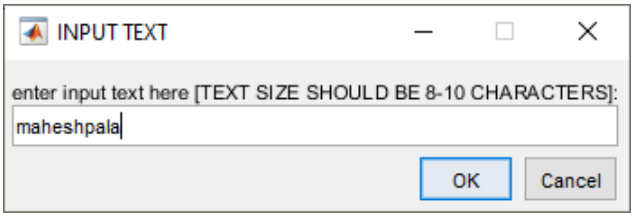


Fig. 8: Entering secret message to be embedded.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

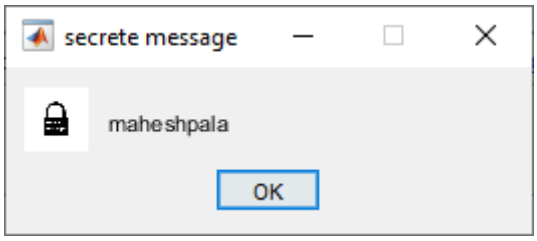


Fig. 9: Embedded message.

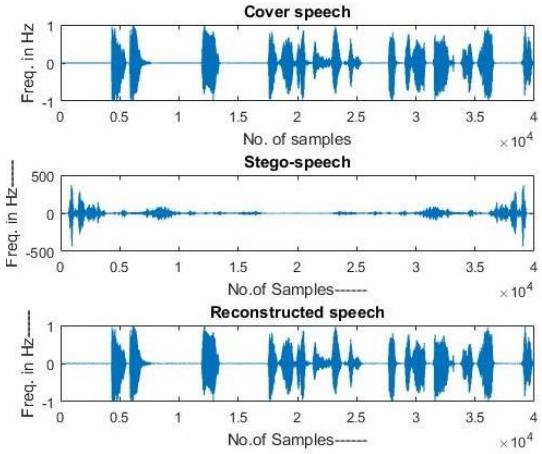


Fig. 10: Performance of FFT-based speech steganography.

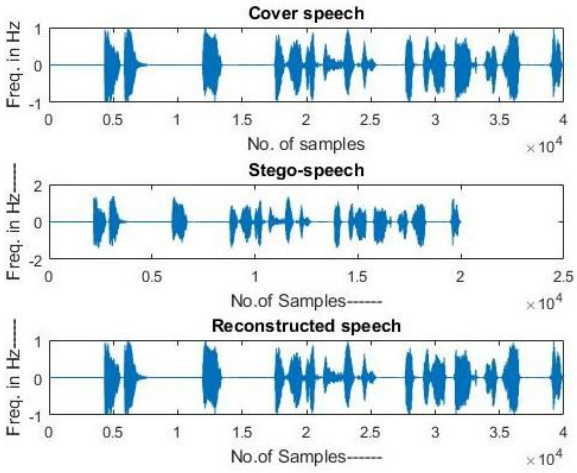


Fig. 11: Performance of proposed speech steganography.

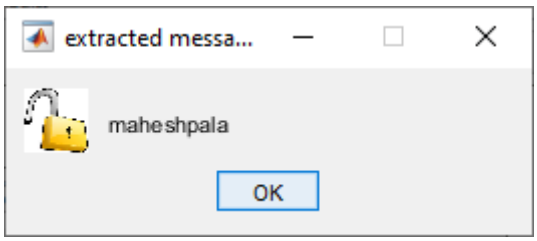


Fig. 12: Extracted message with proposed implementation.

This concludes that proposed speech steganography lessens the BER when there is a noisy attack. In addition, it produced accurate message at the receiver end without degrading the perceptual quality of secret message.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

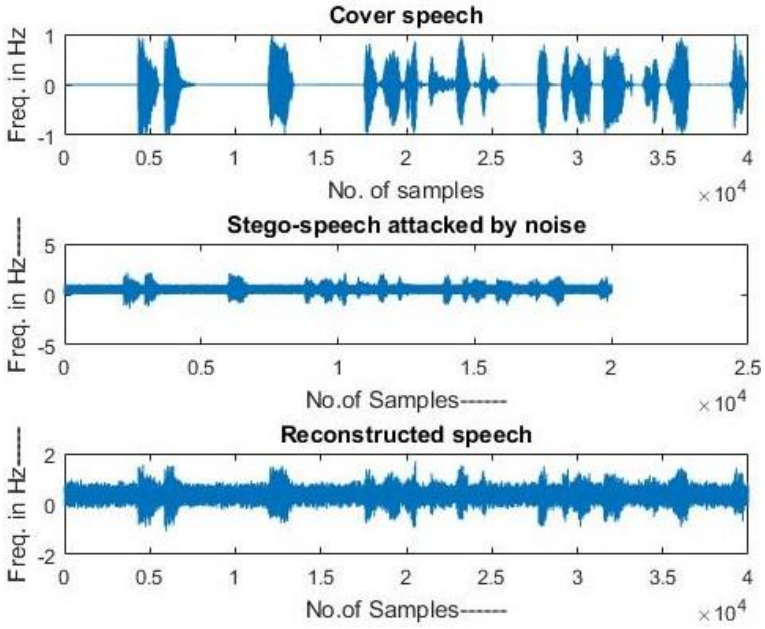
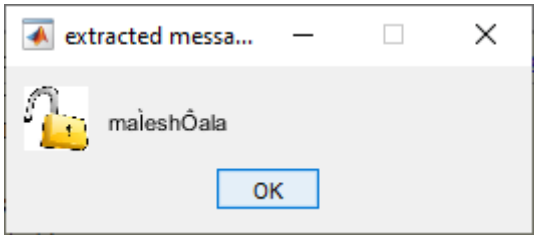


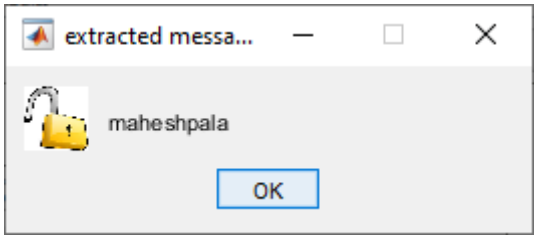
Fig. 13: Obtained results of proposed speech steganography with noise attack.

Table 1. Obtained BER values of existing and proposed speech steganography

Parameter	FFT-based speech steganography [11]	Proposed speech steganography
BER without noise	0.00145	0.0000001
BER with noisy attack	4.25	0.000452



(a)



(b)

Fig. 14: Extracted message from noisy stego-speech. (a) FFT-based speech steganography. (b) proposed speech steganography.

4. CONCLUSIONS

Based on the test results, we had concluded that the proposed speech steganography had shown the best results using FFT algorithm. This method proved that it is very robust against audio manipulation and very safe with the resulting noise is quite small. Also, it reduces

number of computations and does not use any complex equations. It is very simple and easy method to implement even in real time environment.

REFERENCES

[1] Shouyuan Yang, Zanjie Song and Jong Hyuk Park "High-capacity CDMA Watermarking Scheme based on orthogonal Pseudo random subspace projection". International Conference on Multimedia and Ubiquitous Engineering, June 2011

[2] Lionel Fillatre "Adaptive Steganalysis of Least Significant Bit Replacement in Grayscale Natural Images" IEEE Transactions on Signal Processing ,Vol. 60, No. 2, February 2012

[3] R.R.Ahirwal, Deep chandAhirwal and Jpgendarjain "A High Capacitive and Confidentiality based Image Steganography using Private Stego key" International coference on Information Science and applications, Feb 2010.

[4] Rikzy M. Naguraha "Implementation of Direct sequence Spread Spectrum on Audio Data" International Conference on Informatics Engineering, June 2011.

[5] Siwar Rekik, DrissGuerchi,Habib Hamam& Sid-Ahmed Selouani"Audio Steganography Coding Using the Discrete Wavelet Transforms".International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (1) : 2012

[6] Jie Chen, Jose Carlos, "A Spread Spectrum Representation Based FFT Domain Speech Steganography Method", IEEE Transaction on Audio, Speech and Language letters, Vol. 23, No. 1, 2015.