Analyzing the presence of a hidden message in an audio signal

Hanna Martyniuk[1,2,*,†] and Ihor Martyniuk[2,†]

[1] Mariupol State University, Preobrazhenska Str., 6, Kyiv, 03037, Ukraine
[2] State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Maksym Zalizniak Str., 3/6, Kyiv, 03142, Ukraine

Abstract

Today it is practically impossible to calculate the presence of a hidden message in an audio signal if it is not known by what steganographic method this message was hidden. During the analysis of audio signals, the authors hypothesized that the audio signal is a statistically homogeneous signal that has constant probabilistic characteristics. If the signal is heterogeneous, then it should be broken into some statistically homogeneous chunks, i.e., find the signal breakdown points and study the signal in the intervals of the breakdown point. In this paper, the method of finding the hidden message in audio signal is proposed by partitioning the signal into intervals with the help of breakdown points. Later, for each individual interval, statistical studies of the first two moments of the signal are performed and the presence or absence of hidden message is concluded.

Keywords

stegoanalysis methods, message hiding, steganography, breakpoints

1. Introduction

Due to Russia's full-scale invasion of Ukraine, martial law was introduced. At the same time, the Russian military is carrying out aggression against Ukraine not only on the 'physical' battlefield, but also in cyberspace. According to the State Service for Special Communications and Information Protection, the number of cyberattacks on state information systems and critical infrastructure has tripled. It should be noted that a large number of domestic and foreign scientists are working on the issue of protecting information and communication systems from outside interference. But at the same time, not many people think that attackers can covertly transmit the personal data of users through protected information and communication systems. For example, a text message may be embedded in a transmitted media file, which does not pose a threat to information from the cyber incident response side, but has great value to attackers, in particular hackers from the Russian Federation.

The issue of steganography and stegoanalysis in general is being studied by many scientists. However, the vast majority of works deal specifically with hiding information in an image. However, given the rapid development of information transmission through audio and video files, it is worth paying more attention to the methods of steganography and steganalysis of media files.

The vast majority of known studies are based on the improvement of already known methods of audio signal steganography [1–4], but they can still be divided into several types: using the least significant bits, phase modification, spectrum expansion, and echo coding. To find hidden information, steganalysis methods are used, as described in [5–7]. Thus, paper [5] presents a steganalysis method for audio signals in WAV and AU formats, but notes that they do not cope well

CH&CMiGIN'24: Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, January 24–27, 2024, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
ganna.martyniuk@gmail.com (H. Martyniuk); imartyniukiv@gmail.com (I. Martyniuk)
0000-0003-4234-025X (H. Martyniuk); 0009-0003-5565-0828 (I. Martyniuk)

with the task of detecting signals when using noise signals in audio files. Publications [6, 7] emphasizes that each specific method of information hiding has its own steganalysis method. In addition, it is important to understand that if the receiving party does not know which method was used to hide the information, it is almost impossible to detect the presence of a hidden message.

In view of the above, and given Russia's full-scale war against our country, the issue of creating modern methods of protecting the confidentiality and integrity of media data is more acute than ever, as there are no universal methods of protection that would take into account various factors, such as the quality and length of the communication channel, the level of access restriction, computing resources, etc.

2. Method for finding signal homogeneity intervals

As mentioned above, it is difficult to detect the fact that a message has been hidden in an audio file if the steganography algorithm used to do so is unknown. In this regard, the authors assumed that the audio signal can be investigated under conditions of uncertainty. As one of the hypotheses, the assumption was made that the audio signal can be considered as a signal with homogeneous statistical characteristics.

The hypothesis is as follows. All statistical processing of any sample (in this case audio signal) for the purpose of model building, parameter estimation, etc. is based on the assumption that the sample has not changed during data collection. Therefore, the preliminary stage of any statistical processing should be the stage of verification of such homogeneity. Thus, the question here is: is the sample presented statistically homogeneous in the sense of invariability of its probability characteristics? If the answer to this question is yes, then the usual statistical processing should be carried out, depending on the aims of the researcher. If the answer is no, then the task of detecting moments of change in probability characteristics and splitting the original sample into several statistically homogeneous pieces arises.

2.1. Breakdown points

The authors decided to consider the audio signal as a stationary signal. However, by treating stationary signals as time series and applying the stationarity test criteria to them, we can conclude that most of them are non-stationary. Consequently, in practice, various information signals from the physical point of view, as a rule, cannot be directly described by stationary models. Therefore, it is necessary to solve the problem of searching for such ways of information signals preprocessing that would allow to allocate intervals at which signals can be considered as conditionally stationary.

To analyse such signals, we propose to investigate the detection of instantaneous time moments of signal breakdown, provided that a non-stationary signal can be considered as piecewise stationary at different intervals of stationarity.

Under a breakdown is usually understood any changes in the system parameters, processes occurring instantly or very quickly compared to the characteristic period of measurements [8–18]. The problem of detecting breakdown moments arises in many tasks of control and diagnostics of technical systems. In this work it was decided to use algorithms of breakdown detection for audio signal estimation.

The following classification of breakdown types can be presented [9]:

1. ‘Random discharge’ - represents a single change in the mathematical expectation of some process.
2. ‘Mean bias’ - represents a change in the mathematical expectation of random variables on a certain time interval of a random process.
3. ‘Variance bias’ - represents a change in the variance on a particular time interval of a process.
4. Slow fluctuation - ‘trend’. Represents a change in the mathematical expectation at some time interval of a process according to a linear law over time.

5. Fast fluctuation - ‘oscillation’. Represents fluctuations of mathematical expectation at a certain time interval of the process according to a sinusoidal law.

According to the above classification of breakdown types, it can be concluded that such classification can be reduced to a simpler one:

- ‘mean bias’;
- ‘variance bias’;
- ‘trend’.

However, it should be noted that this classification applies more to random signals. Audio signals mostly lack a monotonic component, so the concept of ‘trend’ is generally not taken into account.

2.2. Algorithm for detecting instantaneous breakdowns

Based on the simplified classification of breakdown types, an algorithm for detecting instantaneous breakdowns of audio signals was developed, the structural and logic diagram of which is shown in Figure 1.

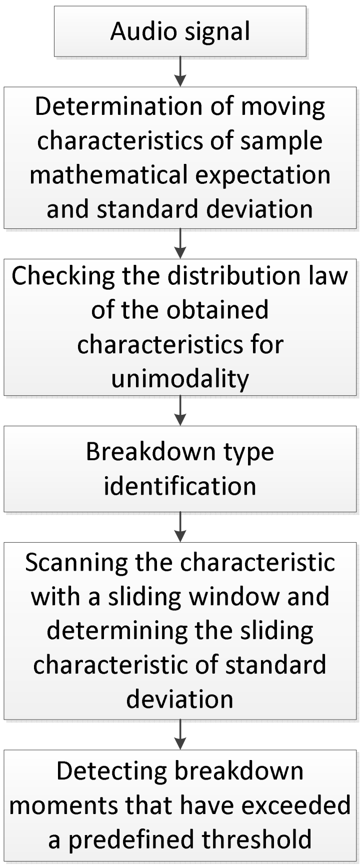

Figure 1: Structure-logic diagram of the method for detecting instantaneous breakdowns of audio time series.

1. Scan the time series of the audio signal $\hat{s}_r[j]$ with a sliding window of length W_{S1}=0.02J and determine the sliding characteristics of the sample mathematical expectation $\hat{M}[j]$ and standard deviation $\hat{\sigma}[j]$.

2. Check the nature of the distribution law of the obtained characteristics $\hat{M}[j]$ and $\hat{\sigma}[j]$. If there is a breakdown of the ‘variance bias’ or ‘mean bias’ type, the corresponding characteristics have

multimodal distribution laws (Figure 2 and Figure 3). In the study, the Hartigan criterion [10] was used to check for unimodality.

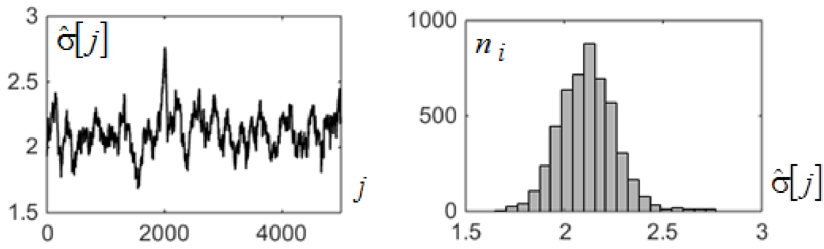

Figure 2: Plots of the moving characteristic of the sample standard deviation (a), and its frequency polygon (b) in the presence of a breakdown of the ‘mean bias’ type.

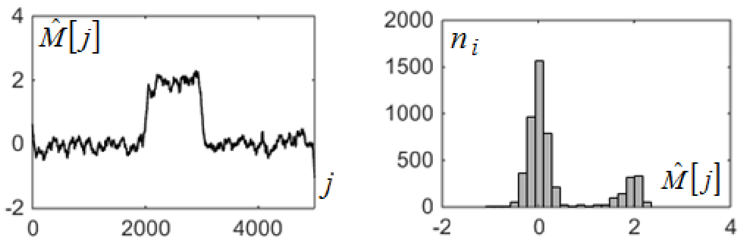

Figure 3: Plots of the moving characteristic of the sample mathematical expectation (a), and its frequency polygon (b) in the presence of a ‘mean bias’ type breakdown.

3. Once a breakdown has been detected and its type identified, a sliding analysis of the corresponding characteristic ($\hat{M}[j]$ or $\hat{\sigma}[j]$ according to Figures 2 and 3) is used to determine the breakdown moments.

To do this, scan the corresponding characteristic with a sliding window of length W_{S2}=0.05$\mathcal{J}$ and determine the sliding characteristic of the standard deviation $\hat{\sigma}_S[j]$. The sections of the characteristic $\hat{\sigma}_S[j]$, exceeding the limit value $L=\overline{\hat{\sigma}_S[j]}+1{,}1\sigma[\hat{\sigma}_S[j]]$ are considered to be those that indicate the beginning and end of breakdown (Figure 4).

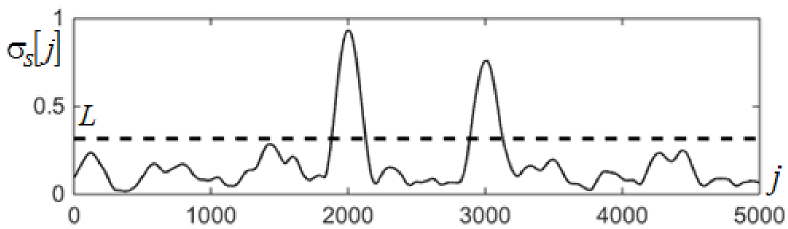

Figure 4: Illustration of a breakdown detection sign.

The paper then presents the application of this algorithm in practice.

2.3. Practical implementation of an algorithm for finding breakdowns for an audio signal

A song with a duration of 1 minute 50 seconds was taken as the investigated signal. Using DeepSound software, a 10,675-symbol text message was added to this song using some unknown steganography method.

During the experiment, the authors implemented the above algorithm for finding breakdown points for a time series of 500,000 samples in Matlab software. For this signal, the results shown in Table 1 were obtained.

Table 1
Audio Time Series Breakdown Points

Coordinates of breakdown points	Type of breakdown
240939	variance bias
476050	variance bias
482347	mean bias

The signal decomposition by breakdown intervals is shown in Figure 5.

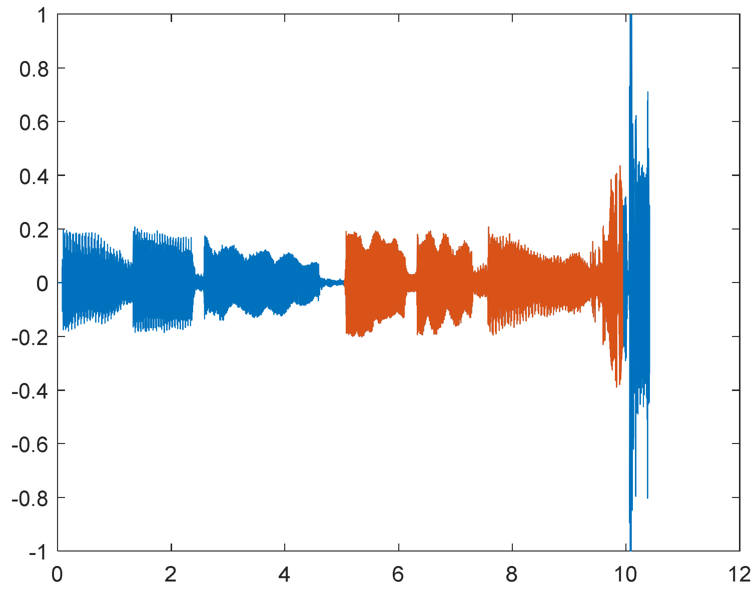

Figure 5: Illustration of breakdown point intervals.

As can be seen from Table 1 and Figure 5, the taken time series has 3 breakdown points, 2 of which show the presence of variance shift, and 1 point shows the presence of mean bias. After finding these intervals, we can evaluate the statistical characteristics of the time series at each interval separately and compare them with the characteristics of the reference signal.

3. Detection of information hiding in audio signal

To detect the fact of information hiding in the audio signal, we used the algorithm shown in Figure 6.

In the theory and practice of statistical estimation, the models, algorithms and software for calculating statistical estimates of characteristics of stationary processes have been most fully developed. The characteristics of stationary processes are: mathematical expectation, dispersion, correlation function, power spectral density and one-dimensional distribution function.

In this paper, the mean and standard deviation were chosen as statistical estimates. The results of the study of other characteristics will be presented in the following papers.

The resulting statistical characteristics of the mean and standard deviation are summarized in Table 2.

As can be seen from the data, the most different statistical characteristics are obtained in the second and third breakdown interval. Based on this, we can conclude that there is a hidden message in this signal.

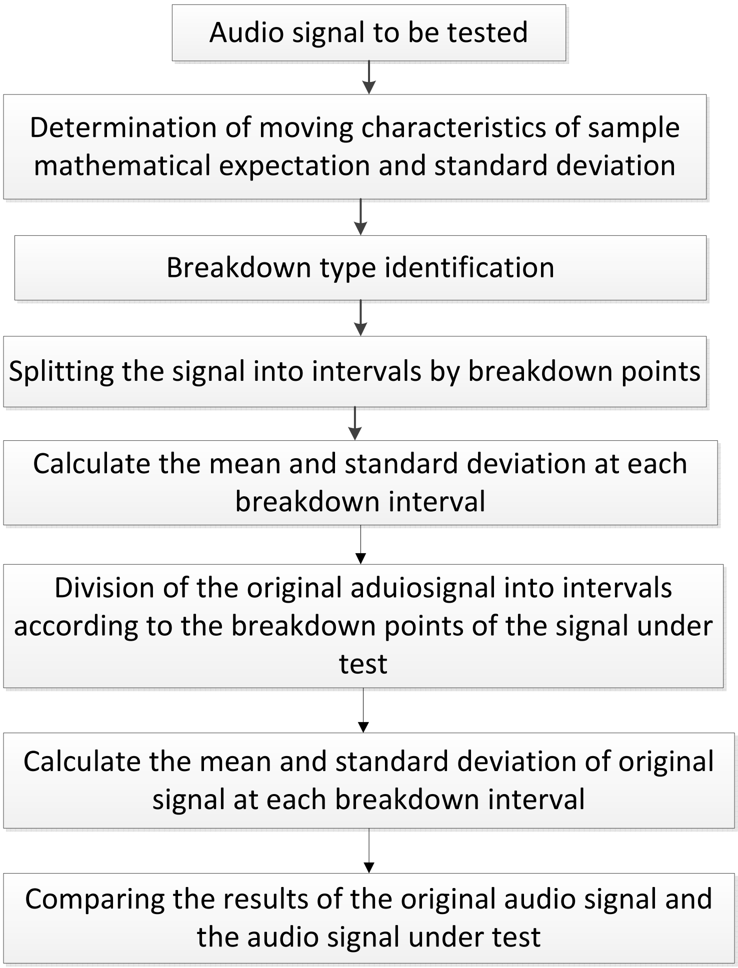

Figure 6: Algorithm for finding hidden information by statistical characteristics of the signal.

Table 2
Resulting Statistical Characteristics of the Source and Test Audio Signals

Coordinates of breakdown points	Mean of test signal	Mean of original signal	Standard deviation of test signal	Standard deviation of original signal
[0:240939]	-2.0458e-05	-1.7512e-05	0.0591	0.0591
[240940:476050]	-1.7131e-06	-9.1503e-06	0.0738	0.0725
[476051:482347]	-0.0039	0.0010	0.1565	0.1550

4. Conclusions

The paper proposes a new method for finding hidden containers in multimedia messages, which, unlike the known ones, will cope with the task of detecting noise audio signal by dividing the signal into intervals of homogeneity and conducting statistical evaluation of each interval separately. Homogeneity intervals are selected by the breakdown points of the signal.

The authors have developed algorithmic-software for detecting the fact of presence of a hidden message. Unlike the known methods of steganalysis, this algorithm will make it possible to detect a hidden container in media files regardless of what steganographic method it was embedded with.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] R. Din, M. Mahmuddin, A. J. Qasim, Review on steganography methods in multi-media domain, International Journal of Engineering & Technology 8 (1.7) (2019) 288–292.

[2] S. K. Moudgil, A. K. Goel, M. Sharma, Steganography on audio wave tenth layer by using signal to noise ratio test and spectrogram analyses, International Journal of Applied Engineering Research 13(4) (2018) 1931–1935.

[3] A. A. Alsabhany, F. Ridzuan, A. H. Azni, The adaptive multi-level phase coding method in audio steganography, IEEE Access 7 (2019) 129291–129306.

[4] A. Zharkikh, A. Gorbunov, Implementation of a software package for embedding and extracting hidden messages in audio files, Machine Learning and Data Analysis 2(4) (2016) 378–390.

[5] M. D. Hassan, M. A. M. Amin, S. Mahdi, Sound based steganalysis for waveform audio file format (wav) and audio file format (au), Journal of Electronic Systems 8(3) (2018) 103–111.

[6] J. Antony, C. C. Sobin, A. P. Sherly, Audio steganography in wavelet domain – a survey, International Journal of Computer Applications 52(13) (2020) 33–37.

[7] H. Ghasemzadeh, M. H. Kayvanrad, Comprehensive review of audio steganalysis methods, IET Signal Processing 3 (2018) 1–17.

[8] A. M. Yerina, V. B. Zahozhai,. D. L. Yerin, Methodology of Scientific Research, Centre for Educational Literature, Kyiv, 2004.

[9] H. Martyniuk, L. Scherbak. Noise Signals and Their Characteristics, LAP Lambert Academic Pub-lishing, Mauritius, 2018.

[10] J. A. Hartigan, P. M. Hartigan, The Dip test of unimodality, The Annals of Statistics 13(1) (1985) 70–84.

[11] Y. Averyanova, et al., UAS cyber security hazards analysis and approach to qualitative assessment, In: S. Shukla, A. Unal, J. Varghese Kureethara, D.K. Mishra, D.S. Han (Eds.), Data science and security, volume 290 of Lecture Notes in Networks and Systems, Springer, Singapore, 2021, pp. 258–265. doi: 10.1007/978-981-16-4486-3_28.

[12] H. V. Martyniuk, O. V. Dergunov, L. M. Scherbak, Method of identifying time series homogeneity intervals for estimating the characteristics of wind turbine noise signals, Modelling and Information Technologies: a collection of scientific papers 79 (2017) 101–106.

[13] H. V. Martyniuk, O. V. Dergunov, Method for detecting moments of breakdown of piecewise stationary time series, IT Systems, Mechanics and Control 16 (2017) 120–127.

[14] J. Korbicz, M. Kowal, Intelligent systems in technical and medical diagnostics, Springer Science + Business Media, New York, 2014.

[15] N. S. Kuzmenko, I. V. Ostroumov, K. Marais, An accuracy and availability estimation of aircraft positioning by navigational aids, in: Proceedings of 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC), IEEE, Kiev, Ukraine, 2018, pp. 36-40. doi: 10.1109/MSNMC.2018.8576276.

[16] I. Ostroumov, et al., A probability estimation of aircraft departures and arrivals delays, In: O. Gervasi, et al. (Eds.), Computational Science and Its Applications – ICCSA 2021. ICCSA 2021, volume 12950 of Lecture Notes in Computer Science, Springer, Cham, 2021, pp. 363–377. doi: 10.1007/978-3-030-86960-1_26.

[17] O. Sushchenko, et al., Airborne sensor for measuring components of terrestrial magnetic field, in: Proceedings of IEEE 41st International Conference on Electronics and Nanotechnology (ELNANO), IEEE, Kyiv, Ukraine, 2022, pp. 687–691. doi: 10.1109/ELNANO54667.2022.9926760.

[18] G. V. Martyniuk, L. M. Scherbak, M.E. Fryz, Information support of computer measuring experiments in evaluating of the noise processes characteristics, in: Proceedings of the seventh world congress “Aviation in the XXI-st Century”, NAU, Kyiv, Ukraine, 2016, pp. 1.6.10–1.6.14.