Algorithm of information stability in hydroacoustic control channel for aquaculture

Igor Kartsan[1,2*], and Nikolai Tuzov[1]

[1]Sevastopol State University, 33 Universitetskaya str., Sevastopol, 299053, Russia
[2]Marine Hydrophysical Institute, Russian Academy of Sciences, 2, Kapitanskaya str., Sevastopol, 299011, Russia

Abstract. Increasing attention is being paid to the mechanisms of data transfer between ocean research devices and data collection and analysis centers for the subsequent study and theorization of ocean evolution. All transmitted data are vulnerable to interception by unauthorized parties, so one of the main challenges is to protect the transmitted information. The proposed algorithm is based on steganographic method and solves the authentication problem by embedding additional data into the original signal in such a way that it is not empirically detectable. Among the first and best-known methods for hidden data embedding is a technique based on spread spectrum technology and its various adaptations, which incorporate additional parameters into the mathematical equation to improve the efficiency of the method. However, when auxiliary information is encoded into the original audio signal, these parameters affect both the covertness and robustness of the embedded data, potentially compromising the integrity of the steganographic system. Consequently, the development of steganographic techniques is aimed at simultaneously improving stealth and robustness.

1 Introduction

The widespread adoption and improvement of digital systems and data processing technologies has led to increased bandwidth, greater integration into service delivery, and new methods of manipulating, transmitting, and archiving information. Consequently, the number and complexity of new cybersecurity risks has increased, raising the importance of data validation [1]. One approach to simultaneously ensure data secrecy, availability, and integrity is to use cryptographic and steganographic security techniques. However, cryptographic methods may not always be practical for ordinary users due to their complex implementation, while steganographic methods are devoid of this drawback [2-4].

In the modern digital age, steganography serves various purposes, one of its most common applications is the protection of intellectual property by embedding additional data known as a watermark.

Digital steganographic methods of information hiding and steganography as a discipline evolved from another data protection technology called "cryptography" [5-8].

* Corresponding author: kartsan2003@mail.ru

Functionally, steganographic techniques aim to hide the very existence of data transmission by "camouflaging" it. An ideal steganographic technique conceals essential information while ensuring that the altered object remains visually or aurally indistinguishable from its original form.

Digital steganography as a scientific direction has emerged recently, and, accordingly, in Russia there is no legal framework regulating and unambiguously defining its principles, classification of methods, purposes of use and terminology. This absence leads to the fact that the same terms are interpreted differently in different sources.

The term "steganography" refers to a method of transmitting (or storing) information in which the fact of transmission (or storage) remains confidential. In this context, covert (steganographic) information transfer includes methods of embedding additional data into redundant data structures presented in a digital format and used as a container.

2 Coding algorithm

Parameters used in a mathematical scheme to determine the most stable pseudorandom signal when transmitted over communication channels:

- Decreasing the sampling rate of the digital signal containing the watermark to 8 kHz and then increasing it to 16 kHz.
- Changing the quantization level of the digital signal containing the watermark to 8 bits per sample and then increasing it to 16 bits per sample.
- Applying a low-pass filter with a threshold of 4 kHz.
- Application of a low-pass filter with a threshold of 8 kHz.
- Adjusting the value of the digital watermarked voice signal to 85% of the original value.
- Adding zero mean white Gaussian noise to the digital watermarked voice signal with a signal-to-noise ratio (SNR) of 30 dB.
- Adding zero mean white Gaussian noise to the digital voice signal containing the watermark, with a signal-to-noise ratio (SNR) of 20 dB.
- Temporal offset of the digital voice signal containing the watermark by one unit in the negative direction.
- Temporal offset of the digital voice signal containing the watermark by three units in the negative direction.

The process of encoding additional data (message) can be divided into two phases. The initial phase (pre-coding) includes conversion of the alphabet of the transmitted message, pre-modulation of the generated pseudo-random signal and creation of a basis that determines the number of segments in which the information will be encoded.

First level:

- Partitioning the sound signal $\vec{x} = [x_1, x_2, .., x_N]$, into segments of length $\vec{c} = 1024$, where *N* is the number of segments.
- Normalization by amplitude [-1;1] of the noise-like signal:

$$\vec{m}_n = \frac{max(\vec{u}) + min\,(\vec{u})}{2} \quad (1)$$

where $max(.)$ is the maximum value of the amplitude $\vec{u}$; $min(.)$ is the minimum value of the amplitude u.

- Alphabetization of the transmitted message $\vec{M} = \{m_1, m_2, .., m_l, .., m_L, \}$, where *L* is the number of elements) to the form $e \in \{-1; 1\}$, where e is a bit of information.
- Calculation of the energy of the noise-like signal E_u;

$$E_u = \sum_{i=0}^{c} {u_i}^2 \quad (2)$$

where c is the segment length; u_i is the element of the noise-like signal.

- Normalization of the noise-like signal energy u_n:

$$\vec{u}_n = \frac{\vec{u}}{\sqrt{E_u}} \quad (3)$$

- Calculation of the filtration coefficient α:

$$\vec{\alpha} = \langle \vec{c} \cdot \vec{u}_n \rangle \quad (4)$$

- Formation of digital watermark w_n:

$$\vec{w}_n = e \cdot |\vec{\alpha}| \cdot \vec{u}_n \quad (5)$$

The second level filters and embeds a digital watermark in each segment of length $\vec{c} = 1024$ audio signals $\vec{x} = [x_1, x_2, .., x_N]$, where N is the number of segments:

$$\vec{y} = \vec{c} - \vec{\alpha} \cdot \vec{u}_n + \vec{w}_n \quad (6)$$

Figure 1 shows the algorithm using an optimized spectrum broadening model based on a series of mathematical transformations of the noise-like signal.

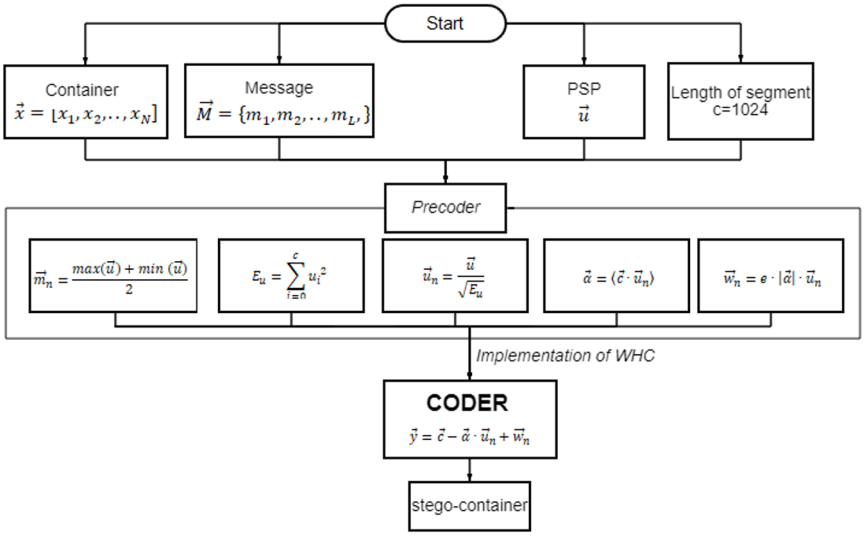

Fig. 1. Coding algorithm.

3 Algorithm for extracting information signals

Schematically, the information (message) extraction algorithm has the form shown in Figure 2. The extraction of bit e_n information occurs according to the formula:

$$e_n = sign(\langle \vec{y}, \vec{u}_n \rangle) \quad (7)$$

where e_n is the reconstructed element of the digital watermark, taking the values $e_n \in \{-1; 1\}$; $sign()$ is the sign detection function; $\langle .,. \rangle$ is the scalar product of the vectors, taking the form:

$$\langle \vec{y}, \vec{u}_n \rangle = \sum_{i=1}^{I} y_i \cdot \vec{u}_{ni} \quad (8)$$

where y_i is the element of the received stegacontainer $\vec{y}$; $\vec{u}_{ni}$ is the element of the received normalized noise $\vec{u}_n$.

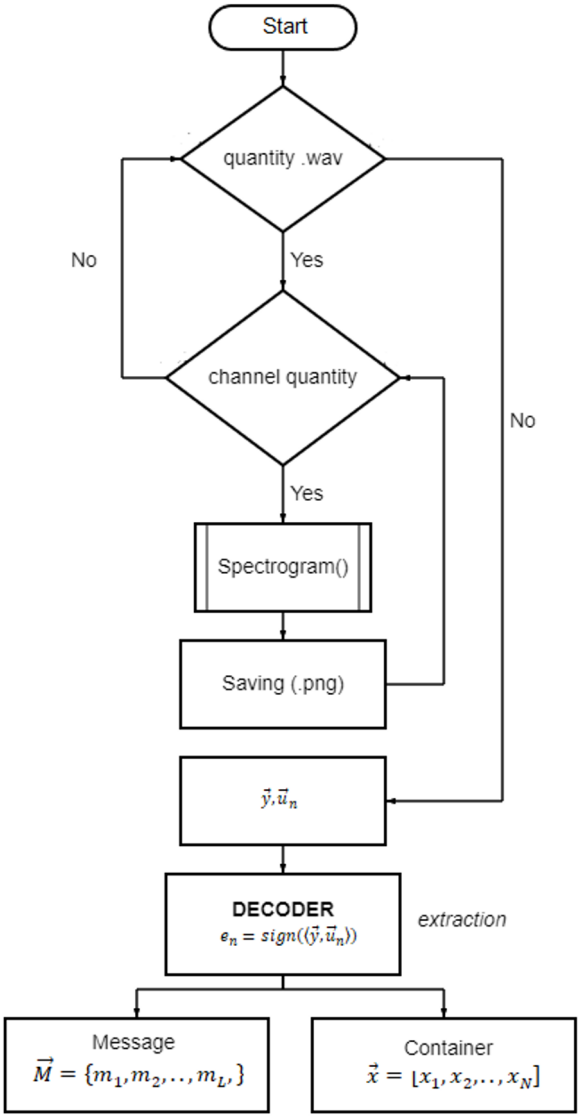

Fig. 2. Algorithm of information transformations occurring in the decoder.

It is also worth noting that at the very beginning of the algorithm the spectrogram is saved for further analysis, including evaluation of transcribing ability and database compilation. After recording a sound fragment, the first thing is its verification, during which the absence of interference, loud noises or artifacts is checked. After obtaining correct sound fragments, it is possible to move to the second part of the evaluation model, in which the direct analysis of opportunities based on the results obtained, as well as the signal-to-noise ratio takes place. The main blocks of the second part of the model are interference, noise and Levenshtein

estimation blocks. The interference block involves selecting the type of interference to be used and at what signal-to-noise ratio. The noise block includes a hydroacoustic model, based on which the original audio recording is noisy in a previously selected way.

This model takes into account the ability to learn and memorize the records it has previously learned. In case the record used was previously learned and the system recognized it from the first time using the maximum noise factor, this record is not taken into account in plotting, excluded and not used in further studies.

4 Conclusion

Thus, the proposed algorithm with spectrum expansion using a specific parameterization of the selected noise for further experiments to evaluate its performance. One of the challenges associated with digital steganography is the diversity of tasks and requirements depending on the application domain. This diversity leads to a multitude of methods solving the same problem, making it difficult to isolate a single application area. By analyzing the current use and ultimate goals of steganographic algorithms, we can divide their applications into the following areas:

- Copy protection.
- Hiding part of the document.
- Authentication.
- Covert communication.

Beyond these areas, steganographic techniques can be applied to a new field, potentially helping to address new, unprecedented challenges associated with the evolving capabilities and widespread adoption of artificial intelligence.

5 Acknowledgements

The study was funded by the Russian Science Foundation grant No. 24-21-20070, https://rscf.ru/en/project/24-21-20070/

References

1. V.S. Averyanov, I.N. Kartsan, Information Protection. Inside, **1(109)**, 18-23 (2023)
2. A.D. Ivannikov, V.P. Kulagin, A.N. Tikhonov, V.Y. Tsvetkov, Information technologies, **8**, 1-32 (2004)
3. S.A. Nuriev, I.N. Kartsan, Information protection. Inside, **5(113)**, 5-9 (2023)
4. S.A. Nuriev, I.N. Kartsan, Modern innovations, systems and technologies, **3(4)**, 349-362 (2023) DOI: 10.47813/2782-2818-2023-3-4-0349-0362
5. M.I. Ozhiganova, E.S. Kurtametov, NBI Technology, **2(14)**, 16-20 (2020)
6. M.I. Ozhiganova, A.O. Kalita, E.N. Tishchenko, NBI Technologies, **4(13)**, 12-21 (2019)
7. I.N. Kartsan, A.O. Zhukov, Information and Telecommunication Technologies, **52**, 19-26 (2021)
8. M.V. Karaseva, I.N. Kartsan, P.V. Zelenkov, Bulletin of Siberian State Aerospace University named after academician M.F. Reshetnev, **3(16),** 69-70 (2007)