sensors

MDPI

Article

Direct Spread Spectrum Technology for Data Hiding in Audio †

Alexandr Kuznetsov [1,2], Alexander Onikiychuk [1], Olga Peshkova [1], Tomasz Gancarczyk [3], Kornel Warwas [3] and Ruslana Ziubina [3,*]

[1] Department of Information Systems and Technologies Security, V.N. Karazin Kharkiv National University, Svobody Sq. 4, 61022 Kharkiv, Ukraine; kuznetsov@karazin.ua (A.K.); onik@karazin.ua (A.O.); o.g.peshkova@karazin.ua (O.P.)

[2] JSC "Institute of Information Technologies", Bakulin St. 12, 61022 Kharkiv, Ukraine

[3] Department of Computer Science and Automatics, University of Bielsko-Biala, Willowa St. 2, 43309 Bielsko-Biala, Poland; tgan@ath.bielsko.pl (T.G.); kwarwas@ath.bielsko.pl (K.W.)

* Correspondence: rziubina@ath.bielsko.pl

† This paper is an extension version of the conference paper: Kuznetsov, A.; Smirnov, O.; Zhora, V.; Onikiychuk, A.; Pieshkova, O. Hiding Messages in Audio Files Using Direct Spread Spectrum. In Proceedings of the 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Krakow, Poland, 22–25 September 2021.

Abstract: Direct spread spectrum technology is traditionally used in radio communication systems with multiple access, for example, in CDMA standards, in global satellite navigation systems, in Wi-Fi network wireless protocols, etc. It ensures high security and reliability of information transfer. In addition, spread spectrum technology provides the transmitted signals with a noise-like appearance, thus hiding the semantic content of the messages. We researched this technology for other implementations. The purpose of our study was to investigate new technologies for hiding data in multimedia files. In particular, we investigated the direct spread spectrum in the context of the development of methods for hiding data in audio containers. We considered various spreading sequences (chip codes) and also explored their use for hiding information in audio files. We conducted experimental studies and estimated the bit error rate (BER) in the recovered data. The article also evaluates the distortion of an audio container by the peak signal-to-noise ratio (PSNR). The results of our research enable us to find out which method of forming chip codes gives a lower BER with equal PSNR. We provide recommendations on the formation of spreading sequences to reliably and safely hide informational messages in audio files.

Keywords: spread spectrum technology; data hiding; steganography; chip codes; audio

check for updates

Citation: Kuznetsov, A.; Onikiychuk, A.; Peshkova, O.; Gancarczyk, T.; Warwas, K.; Ziubina, R. Direct Spread Spectrum Technology for Data Hiding in Audio. *Sensors* **2022**, *22*, 3115. https://doi.org/10.3390/s22093115

Academic Editor: Evangelos Kranakis

Received: 14 March 2022
Accepted: 15 April 2022
Published: 19 April 2022

1. Introduction

Various techniques are used to conceal information [1–3]. The most common of them are cryptography techniques [4–6]. In this case, meaningful messages are converted into meaningless, noise-like forms, i.e., this becomes useless data for an unauthorized user (who does not know the secret cryptographic key). Thus, cryptography hides the semantic content of the transmitted data, whereas the very existence of messages is not hidden [3,7].

Another approach is to use steganographic techniques [3,8]. In this case, informational messages are hidden inside other data (also called containers, covers, carriers, etc.). Carriers can be presented, for example, in the form of various multimedia files (images, video, audio, texts, etc.) [9]. A range of applications exist with multimedia data, so the transfer of video or audio files on the internet does not cause any suspicion. At the same time, only the one who has the secret steganographic key knows that an informational message is hidden in these covers. It is similar to a suitcase with a double bottom; the second bottom is reliably disguised, and it is difficult to detect a hidden message without a secret key. Thus, steganography hides the fact that messages exist [2,8].

The present paper discusses steganographic information hiding techniques in which audio files act as multimedia containers. Hiding data in audio has great prospects. Firstly, such data are significantly popular on the internet. For example, we can use audio messages in messengers and social networks as covers. At the same time, the amount of hidden data can be quite large. In addition, there is a problem with copyright protection of audio content on the internet. Hiding digital watermarks (with a copyright label) in audio containers can be an effective solution. Thus, hiding data in audio is really very relevant and may have a commercial implementation.

In our experiments, we used the simplest audio signals recorded in the digital WAV format [10,11]. However, all our results and suggestions can be interpreted for a more general case with other audio container formats.

In order to conceal information, this work employs a special technology traditionally used in radio communication systems [12–15]. This is a direct spreading of the spectrum [16], which implements wideband modulation with pseudo-random sequences (chip codes) [17]. The correlation properties of chip codes guarantee the absence of mutual interference in the communication channel [18]. As a result, the radio communication system acquires numerous useful properties: noise immunity, high bandwidth and subscriber capacity, absence of mutual interference, environmental friendliness of communication, and many others [19].

Direct spread spectrum technology is implemented in many industry standards and applications, for example:

- Code division multiple access communication systems (IS-95, CDMA2000, WCDMA, DS-CDMA, TD-CDMA, TD-SCDMA, etc.);
- Global satellite navigation systems (American GPS, European Galileo, and Russian GLONASS);
- Family of wireless network protocols Wi-Fi (family of standards IEEE 802.11), and much more.

Direct spread spectrum technology can also be used in steganography [20–22]. In particular, in one of the first works [21] in this area, it was proposed to interpret the carrier as noise in the communication channel. In this case, the task of hiding information in multimedia files is equivalent to transmitting useful signals over communication channels with natural additive noise.

Currently, a large number of studies on steganography and the direct spreading of the spectrum have already been conducted. Various researchers studied this issue in relation to various computer applications. It turns out that the main characteristics of reliability and safety depend on the properties of the spreading sequences. In particular, in [23,24], we investigated various ways of generating chip codes in relation to cover images. In this paper, we continue these studies in relation to another type of multimedia data—audio carriers.

We studied the basic characteristics of an audio stegosystem for various spreading sequences. In our experiments, we estimate the bit error rate (BER) of hidden information data. This is the most important indicator of the quality of recovered messages. In addition, we evaluated the distortions of the audio container, which characterize the quality of multimedia data after hiding information messages in them. Therefore, we used the mean squared error (MSE) and the peak signal-to-noise ratio (PSNR). In this article, we demonstrated that the variety of ways of generating chip codes have different results for BER, MSE, and PSNR. It becomes an area for possible optimization, as the choice of the method of forming the spreading sequences is very important for various computer applications. Thus, the main goal of our work is to find the best chip codes that would minimize the BER for comparable PSNR.

2. Related Works

Hiding data in audio was investigated in many related papers, e.g., in papers [25–29], the simplest LSB techniques were studied, which, nevertheless, have some advantages. By encoding the LSB of the container, you can hide a very large amount of data. However, LSB techniques are also easily detected, and this is their main drawback. Various authors tried to improve LSB. In [26], the authors used augmentation operations to increase resistance to attacks. In [25], the LSB method was applied to the coefficients of the discrete wavelet transform. In [27], an LSB was proposed with an adaptive number of hiding bits for each audio sample (depending on the size of the hidden data, the size of the covering carrier, and the signal-to-noise ratio). In [28], binary data values were hidden in different places to increase security. In [29], the LSB technique was supplemented with data encryption. There are many other works in this area; however, each improvement of the LSB method leads, as a rule, to a decrease in the volume of hidden data [30,31].

Other approaches to hiding data in audio use various techniques: in [32], Cochlear Delay Characteristics were used to hide data; in [33], authors investigated bit reduction techniques; in [34–36], echo signals were used; in [37–39], data were hidden in the phases of audio signals. All these techniques have their advantages and disadvantages [31]. In particular, the amount of hidden data is significantly less than in LSB methods. However, the security of the hidden data is higher.

One of the prospective methods is steganography with direct spectrum expansion. These techniques combine high throughput and data security.

The first works [20,21,40] were devoted to the substantiation of the general concepts and structure of the steganosystem using a direct spread spectrum. Images were used to hide the messages. Already in those articles, the authors noted several conflicting requirements [41]. In particular, increasing the size of messages leads to increasing the corruption of containers; small BER values can be achieved only with a large "energy" of the embedded message, which significantly distorts the container. In order to eliminate some of these contradictions, the authors suggested using special filtering and correcting codes [41]. These and other ideas were developed in subsequent works. For example, in [42], correction codes were investigated; in [43,44], a discrete cosine transform (DCT) was implemented together with the direct spreading of the spectrum, etc. Papers [45,46] are devoted to the study of chaos. In works [47,48], hiding information in video data was studied, and in [42,49], audio signals were used for hiding information. Indeed, hiding messages in audio signals is a promising direction [50]; these methods can be used, for example, to protect the property rights of digital audio signals [51].

Note that in these numerous works, the properties of spreading sequences (chip codes) were almost not explored. The exceptions are our two recent works [23,24], in which we analyzed various methods of forming spreading sequences, as well as their influence on the characteristics of Spread Spectrum Image Steganography.

In this work, we continued our research and expanded their field to audio files. First, we looked at different ways to form spreading sequences and explored BER, MSE, and PSNR. Then, we explored possible compromises, such as how to minimize carrier distortion with low bit error rates. It turned out that the Walsh–Hadamard expansion sequences were best suited for this, and our experiments clearly demonstrated this.

3. Materials and Methods

Direct spread spectrum technology is a wideband modulation in which the original bit sequence is converted into a pseudo-random spreading sequence [18]. As a result, we obtained the transmission of a significantly larger number of extended (direct) sequence bits in the same time interval. Consequently, the frequency range for transmitting signals increases in proportion to the length of the spreading sequence [19].

3.1. Direct Spread Spectrum Technology in Telecommunications

The fundamental Shannon–Hartley theorem sets a constraint on the channel capacity, i.e., to the upper limit of the maximum amount of information that can be transmitted in a communication system with a given frequency band and power of additive white Gaussian noise [52]:

$$C = \Delta \mathrm{F} \log_2 \left(1 + \frac{P_S}{P_N} \right), \tag{1}$$

where:

- C—channel throughput, bit/s;
- ΔF—frequency band, Hz;
- P_S—desired signal power;
- P_N—additive white Gaussian noise power;
- $\frac{P_S}{P_N}$—signal power to noise ratio (SNR).

From Equation (1), we see that at low SNRs, the throughput can be increased only by expanding the frequency band, and direct spread spectrum technology is well suited for this. Indeed, using very long spreading sequences, even at a very low SNR value, high-speed information transmission can be realized. This circumstance can also be used, e.g., to build environmentally friendliness of communication systems, i.e., when $P_S \approx P_N$. Then, using spreading sequences with a bit length 10^8 or more, it is possible to realize information transfer at rates of tens and hundreds of Mb/s.

Let us explain the technology of spreading the spectrum with a direct sequence in the following simple way.

Consider a set $s = (s_1, s_2, \ldots, s_k)$ of pseudo-random bit sequences (vectors):

$$\begin{gathered} s_1 = (s_{1,0}, s_{1,1}, \ldots, s_{1,n-1}), \\ s_2 = (s_{2,0}, s_{2,1}, \ldots, s_{2,n-1}), \\ \ldots, \\ s_k = (s_{k,0}, s_{k,1}, \ldots, s_{k,n-1}), \end{gathered}$$

represented, for example, in polar form, i.e.,

$$\forall i, j : s_{i,j} = \begin{cases} 1, \\ -1. \end{cases}$$

Vectors are designed to spread the spectrum of the original message, so they are called chip codes or chipping codes. Each value $s_{i,j}$ is called a chip or sequence element.

The vectors $s_1, s_2, \ldots, s_k \in s$ are formed so that their cross-correlation is negligible, i.e.,

$$\forall i \neq j : \rho(s_i, s_j) = \sum_{v=0}^{n-1} s_{i,v} s_{j,v} \approx 0 \tag{2}$$

For example, if the vectors $s_1, s_2, \ldots, s_k$ are taken equal to the rows (or columns) of the Hadamard matrix, we obtain orthogonal chip codes, i.e.,

$$\forall i \neq j : \rho(s_i, s_j) = 0$$

There are other ways to generate chip codes, for example, when the elements $s_{i,j}$ take a random value over an interval $[-1, 1]$. However, condition (2) for the generation of spreading sequences is decisive.

Suppose the message is made up of k bits, i.e., $m_1, m_2, \ldots, m_k$, e.g., let us write the information bits $m_i, i = 1, 2, \ldots, k$ also in polar form, i.e.,

$$\forall i : m_i = \begin{cases} 1, \\ -1. \end{cases}$$

Modulation of the information bits $m_i, i = 1, 2, \ldots, k$ can be achieved in different ways, e.g., with polar notation according to the expression:

$$\forall i : M_i = m_i s_i = (m_i s_{i,0}, m_i s_{i,1}, \ldots, m_i s_{i,n-1}) \tag{3}$$

In this way, instead of one binary element, m_i a vector (sequence) M_i of binary elements n, is transmitted.

Let us assume that the durations of an element m_i and its extended chip version M_i are the same. Suppose, for example, that they are equal to T seconds. Then the duration of one chip $s_{i,j}$ will be n times less: $T_{chip} = \frac{T}{n}$. Therefore, the chips are transmitted at a frequency

$$F_{chip} = \frac{1}{T_{chip}} = \frac{n}{T} \text{ Hertz.}$$

This frequency is n times greater than the frequency of information bits $F = \frac{1}{T}$. Thus, we obtained the spread of the frequency of the original message by n times.

The multiplying of the signal duration by its frequency is called the base B. If $B > 1$, then the signals are called complex.

For our case, we have

$$B = T_{chip}F_{chip} = n > 1$$

and direct spreading signals are complex signals.

Several information bits can be simultaneously transmitted to the communication channel, i.e., the receiver obtains an additive mixture:

$$Mix = N + \sum_{j=1}^{k} M_j \tag{4}$$

where the symbol N denotes the sequence of random elements caused by noise (for example, additive white Gaussian noise).

The receiver has synchronized copies of the chip codes $s_1, s_2, \ldots, s_k \in s$. In order to restore the information bits, it is necessary to calculate the correlation between the received signal and the corresponding chip codes. For example, to restore the value m_i in (3), the receiver computes $\rho(s_i, Mix)$. Equation (2) is linear, i.e., write down

$$\rho(s_i, Mix) = \rho(s_i, N) + \rho(s_i, \sum_{j=1}^{k} M_j) \tag{5}$$

For random noise, N, we have:

$$\rho(s_i, N) \approx 0 \tag{6}$$

Moreover, $\forall i \neq j : \rho(s_i, s_j) \approx 0$; therefore,

$$\rho(s_i, Mix) \approx \sum_j \rho(s_i, m_j s_j) \approx \rho(s_i, m_i s_i) \tag{7}$$

In this way, we can write the information bit recovery rule

$$m_i = \rho(s_i, Mix) = \begin{cases} -1, & \rho(s_i, Mix) < 0; \\ +1, & \rho(s_i, Mix) > 0. \end{cases} \tag{8}$$

Note that in the above reasoning, individual bits $m_i, i = 1, 2, \ldots, k$ may belong to different senders. In this case, code division multiple access is implemented [18].

Let us note the following advantages of using direct spread spectrum technology:

- Resistance to unintended or intended jamming;
- Sharing a single channel among multiple users;
- Reduced signal/background-noise level hampers interception;
- Determination of relative timing between transmitter and receiver and much more.

We are considering the use of this technology in steganography, i.e., to hide informational messages in multimedia files.

3.2. Direct Spread Spectrum in Steganography

Direct spread spectrum technology has long been used in steganography.

In the first works [20,21,40], a general scheme of a steganosystem with the direct spreading of the spectrum was proposed. The authors used cover images, but all their reasoning can be extended to other multimedia data.

The general idea of such a stegosystem is as follows (Figure 1).

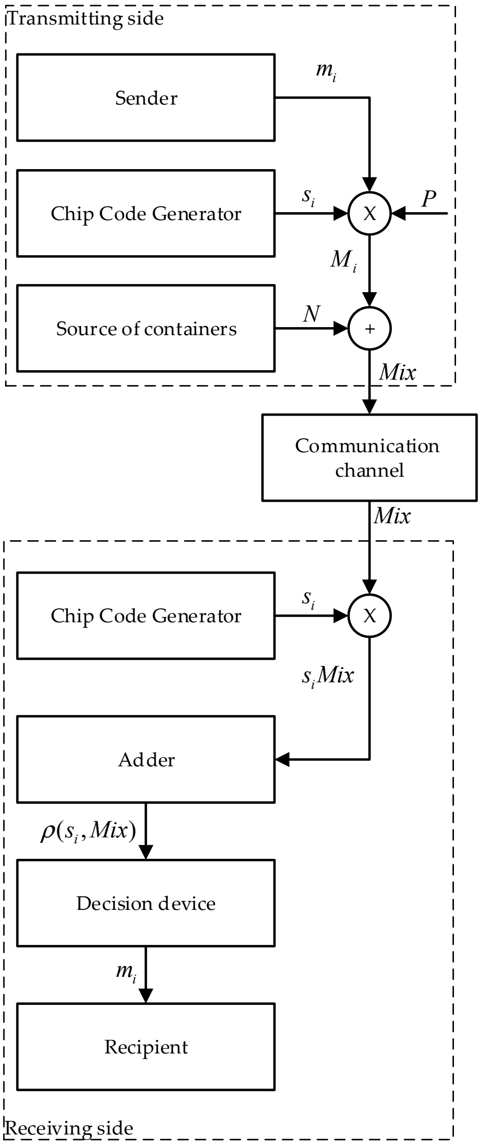

Figure 1. Block diagram of concealment and recovery.

In order to hide the data, the following steps are performed:

Step 1 The information message is presented in polar form m_i;
Step 2 m_i multiplied bit by bit by the spreading sequence as in (3);
Step 3 Multimedia data (images, audio, video, etc.) are interpreted as noise in the communication channel. Using our notation, this is N in (4).
Step 4 Further, these data are hidden in the cover data according to rule (4). However, we currently denote:

1. N—multimedia data (container, cover), inside which the message is hidden;
2. Mix—modified multimedia data (filled container) after hiding messages in them.

In order to restore the data, the following steps are performed:

Step 1 Correlation is calculated.

- The product is calculated $s_i Mix$;
- The sum is calculated $\rho(s_i, Mix) = \sum_{v=0}^{n-1} s_{i,v} Mix_v$;

Step 2 If Equations (6) and (7) are true, then the value of the recovered bit is calculated by the Equation (8).

Step 3 The recovered message is presented in a custom view.

It should be noted that even in the first works, the authors encountered significant difficulties. For example, in [53] was shown that the error rate in the extracted messages is very high (see, for example, Table 2 on page 12 of [53]). BER can be reduced in different ways, for example, by using filtering, correction codes, etc. The simplest is to increase the power of chip codes. For this, Equation (4) can be rewritten as

$$Mix = N + P\sum_{j=1}^{k} M_j = N + \sum_{j=1}^{k} m_j(Ps_j) \tag{9}$$

where the value P specifies the power amplification factor of the chip codes $s_j = (s_{j,0}, s_{j,1}, \ldots, s_{j,n-1})$.

By increasing the power, P, it is actually possible to achieve a decrease in BER. However, this inevitably leads to distortion of the container N. For example, for $k = 10$ and $P = 10$, each value of the cover file N may be skewed by $\pm kP = 100$. This may present a real problem because BER is still high. For example, in [53], it is shown that even with $P = 100$ an error rate is more than 10% (see Table 2 from [53]).

We carried out detailed studies of this problem in [23,24]. In particular, we repeated the experiments with images from [21,40,53,54]. We studied the effect of different ways of forming spreading sequences on the BER value. The general conclusions about the high BER were confirmed, and the explanation for this phenomenon is, in our opinion, the following. The first term in (4) presents a certain implementation of random additive white noise N. This is indeed the case for spread spectrum communications systems. Those assumption (6) is fulfilled, which gives an almost error-free recovery of the message according to rule (8). However, in the stagnosystem, in (4), multimedia data are meant. This is usually highly redundant, highly correlated data. This is not a random realization of Gaussian noise, and assumption (6) is often not met. Obviously, this leads to errors in the recovered bits according to rule (8). In works [55,56], an effective way to combat this phenomenon was proposed. We proposed to form chip sequences in a special, adaptive way. Indeed, if we take into account the statistical properties of multimedia data (in [55,56], we used cover images), then it is possible to form chip codes $s_1, s_2, \ldots, s_k$, in such a way that condition (6) is guaranteed to be satisfied. In this case, it is possible to ensure an almost error-free extraction of information messages according to rule (8).

In this article, we continued our experiments. We used audio covers and experimented with different ways to generate chip codes. We showed that the variety of ways of generating spreading sequences produces different BER values. This is an area for possible optimization of the stegosystem, and we showed which chip codes are really best used to hide information messages in audio containers.

3.3. Initial Data for Hiding Messages

We used various audio carriers and various families of chip codes as the initial data for our experiments. We were guided by the works [21,40] and our papers [23,24] when choosing the initial data and research methodology.

An audio signal recorded in the digital WAV format [10,11] was used as an audio container. In our experiments, we used an audio file with a student anthem (Gaudeamus Igitur) downloaded from an internet resource [57] and converted to WAV format.

WAV audio is most commonly encoded using linear pulse code modulation (LPCM). Such a cover file contains uncompressed audio signal data; its main characteristics are:

- the number of channels (streams) of audio data $N_{channel}$. We used stereo signals, i.e.,$N_{channel} = 2$;
- sampling frequency f_d. Our audio signals from $f_d = 22050$;
- the number of bits allocated to encode each discrete sample of the audio signal. We used covers from $B = 8$ bit.

As input information messages, we used plain text files (steganography textbooks), processed and presented in binary polar form.

In order to hide information, various spreading sequences were used, studied by many authors, for example, in [21,40] and also in our previous works [23,24]. Let us consider these chip codes in more detail.

3.4. Used Chip Codes

In this article, various methods for generating chip codes were considered, and their influence on the characteristics of a steganosystem was studied. Specifically, we explored five different ways to generate spreading sequences.

1. Spread sequences from [21,40]

In the basic works [21,40] on Spread Spectrum Steganography, a nonlinear rule for the formation of chip codes $s = (s_1, s_2, \dots, s_k)$ was used. In particular, each chip $s_{i,j}$ was formed as a realization of a random variable distributed according to the standard normal law.

For this, the rule was proposed:

$$s_{i,j} = \begin{cases} \Phi^{-1}(u_{i,j}),\ m_i = -1; \\ \Phi^{-1}(u\prime_{i,j}),\ m_i = 1, \end{cases} \tag{10}$$

where

$$u\prime_{i,j} = \begin{cases} u_{i,j} + 0.5,\ u_i < 0.5; \\ u_{i,j} - 0.5,\ u_i \geq 0.5, \end{cases}$$

- $u_{i,j}$—implementation of a random variable uniformly distributed over the interval $[0,1]$;
- Φ^{-1}—inverse cumulative distribution function for a standard Gaussian random variable.

In our experiments, we used chip codes of length $n = 1024$ generated according to rule (10).

Spreading sequences with a Gaussian chip distribution (10) were also studied by us earlier in relation to cover images in [23,24]. We are expanding our research to the case of audio containers now.

2. Chip codes from random numbers uniformly distributed over the interval $[-1, 1]$

We also implemented the formation of spreading sequences of length $n = 1024$ from random numbers uniformly distributed over the interval $[-1, 1]$. Each chip $s_{i,j}$ is formed randomly with equal probability and independently of other values.

3. Chip codes from normally distributed random numbers

This method of forming spreading sequences of length $n = 1024$ consists in generating normally distributed random numbers. In fact, the second and third methods are very similar. Each chip $s_{i,j}$ is randomly formed. The second method uses a uniform distribution on the interval $[-1, 1]$, and the third one uses a standard normal distribution. The third method is also similar to the first, but the rule for generating chip codes is somewhat different.

4. Binary chip codes generated by a pseudo-random bit generator

The simplest, in our opinion, is the formation of individual chips using a pseudo-random bit generator. We converted the generated bits to polar form and formed spreading sequences of length $n = 1024$.

5. Walsh–Hadamard spreading sequences

These are discrete sequences of length $n = 2^w$, $w = 1, 2, \ldots$, which can be formed as rows (or columns) of the Hadamard matrix H_n of order $n = 2^w$:

$$H_{2^w} = \begin{bmatrix} H_{2^{w-1}} & H_{2^{w-1}} \\ H_{2^{w-1}} & -H_{2^{w-1}} \end{bmatrix},\ H_1 = [1]. \tag{11}$$

For example, for $n = 4$, we have four chip codes:

$$\begin{aligned} s_1 &= (1,1,1,1), \\ s_2 &= (1,-1,1,-1), \\ s_3 &= (1,1,-1,-1), \\ s_4 &= (1,-1,-1,1). \end{aligned}$$

In our experiments, we used spreading sequences with a length of $n = 2^{10} = 1024$. Therefore, we recursively generated H_{1024} according to rule (11) and formed $s = (s_1, s_2, \ldots, s_{k=1024})$ as a set of strings H_{1024}.

The Walsh–Hadamard sequences form an orthogonal system, i.e.,

$$\forall i \neq j : \rho(s_i, s_j) = 0$$

which is in good agreement with (2).

Nevertheless, the main disadvantage of such chip codes should be pointed out. The number of different orthogonal sequences of length n cannot exceed n. Therefore, to hide a large number of bits in the same container, this generation method may not be sufficient.

3.5. Indicators of Effectiveness of Hiding Messages

In order to evaluate the efficiency of the steganosystem, it is necessary to evaluate the distortions in the recovered messages, as well as the distortions of the original container. Therefore, we experimentally estimated the bit error rate (BER) in recovered messages. We also estimated audio cover distortions by mean squared error (MSE) and peak signal-to-noise ratio (PSNR). We did not use other indicators of distortion of the audio cover (for example, percentage residual deviation, autocorrelation analysis of stegodata with original data, etc.), as this can be obtained after processing our results.

These are the most common metrics used in many related works.

1. Bit Error Rate, BER

The bit error rate is calculated using the equation:

$$BER = \frac{k_{error}}{k} \tag{12}$$

where k_{error} is the number of erroneously recovered bits, k is the total number of bits in the information message.

2. Mean squared error, MSE

In order to estimate the container distortion, the root mean square error (MSE) is used, i.e., the averaged square of the difference between the original multimedia data and the cover data obtained after the message was hidden. For an audio signal represented by a set of n discrete samples, MSE is calculated by the equation:

$$MSE = \frac{1}{n} \sum_{i=0}^{n-1} [Mix_i - N_i]^2 \tag{13}$$

3. Peak signal-to-noise ratio, PSNR

A more visual characteristic of cover distortion is the ratio of the maximum possible signal power to the power of the distorting noise. Usually, this characteristic is expressed on a logarithmic scale and calculated by the equation:

$$\begin{aligned} PSNR = 10 \cdot \log_{10}\left(\frac{N_{\max}^2}{MSE}\right) = 20 \cdot \log_{10}\left(\frac{N_{\max}}{\sqrt{MSE}}\right) = \\ = 20 \cdot \log_{10}(N_{\max}) - 10 \cdot \log_{10}(MSE), \end{aligned} \quad (14)$$

where $N_{\max}$ is the maximum possible value of the signal N.

In our case, by N we mean multimedia data, i.e., an audio signal represented by a set of discrete samples. If each discrete sample is coded in B bits, then (in linear pulse code modulation, PCM) the maximum possible value of $N_{\max} = 2^B - 1$. In our experiments, we used the simplest audio signals with $B = 8$, i.e., $N_{\max} = 255$. Equation (14) for this value takes the form:

$$PSNR = 20 \cdot \log_{10}(255) - 10 \cdot \log_{10}(MSE).$$

4. Results

4.1. Experimental Evaluation of Hidden Message Distortion

In Figures 2–6, the results of our experiments on BER estimation are shown for different methods of generating chip codes of length $n = 1024$. We changed the number k of hidden information bits and the coefficient P for amplifying the power of the spreading signals in (9).

The obtained results of experimental studies correspond to the points in the given diagrams. Each point corresponds to a value averaged over 5000 tests. For better perception, these and all subsequent figures also show trend lines.

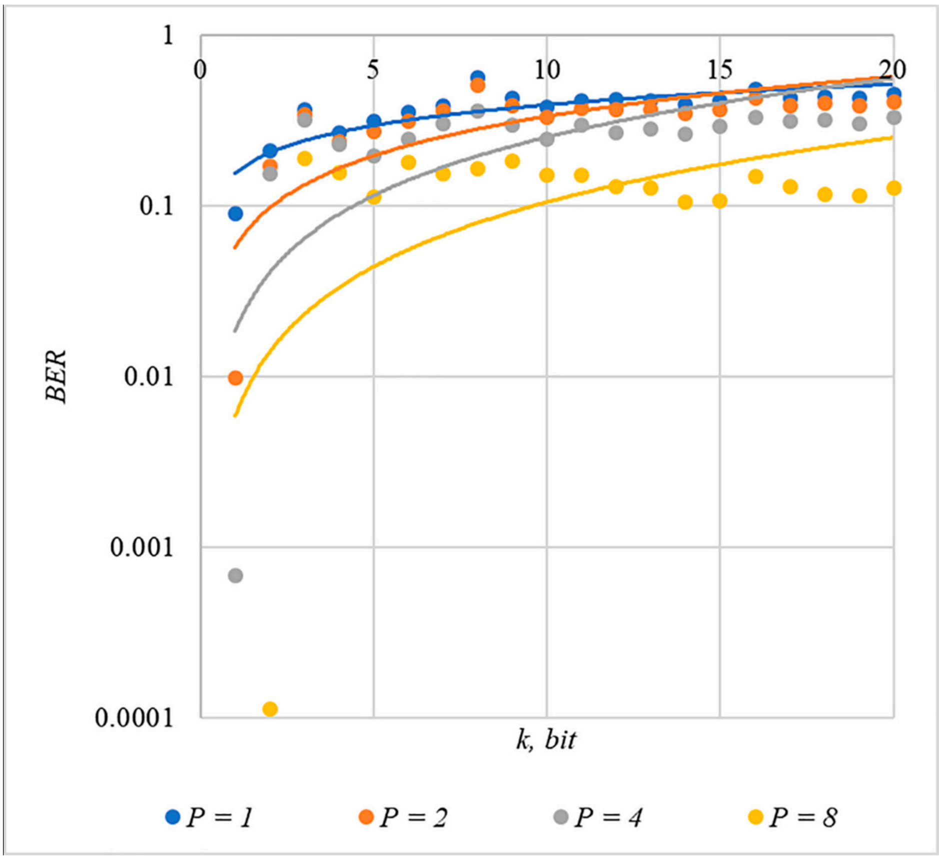

Figure 2. $BER(k)$ dependencies for different values of P rule for generating chip codes №1.

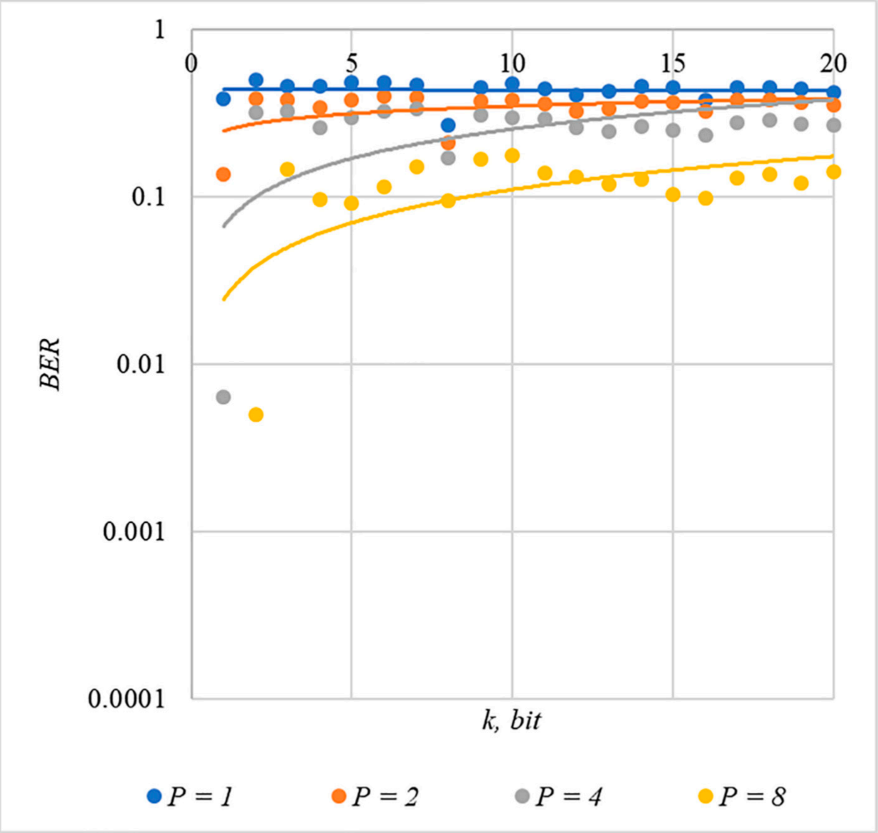

Figure 3. *BER*(*k*) dependencies for different values of *P* rule for generating chip codes №2.

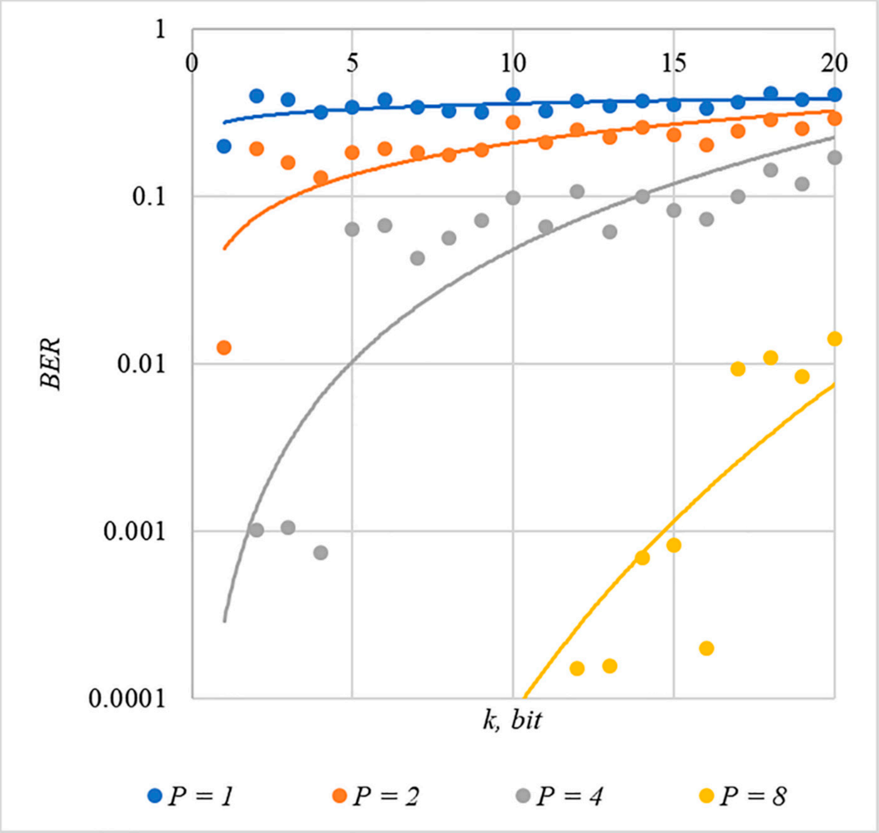

Figure 4. *BER*(*k*) dependencies for different values of *P* rule for generating chip codes №3.

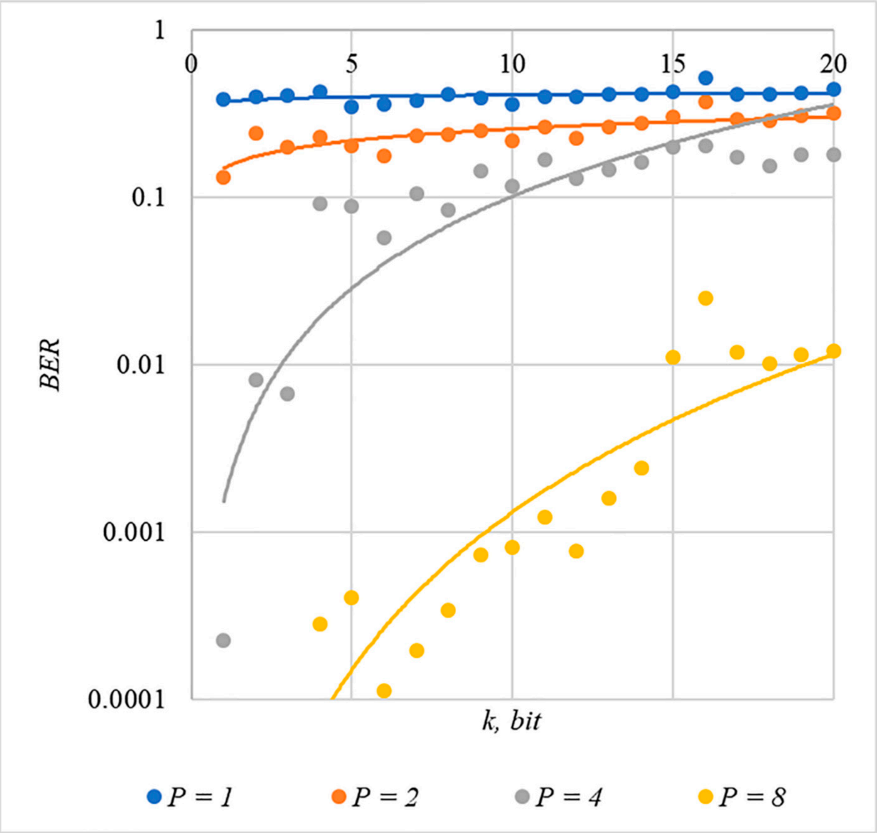

Figure 5. *BER*(*k*) dependencies for different values of *P* rule for generating chip codes №4.

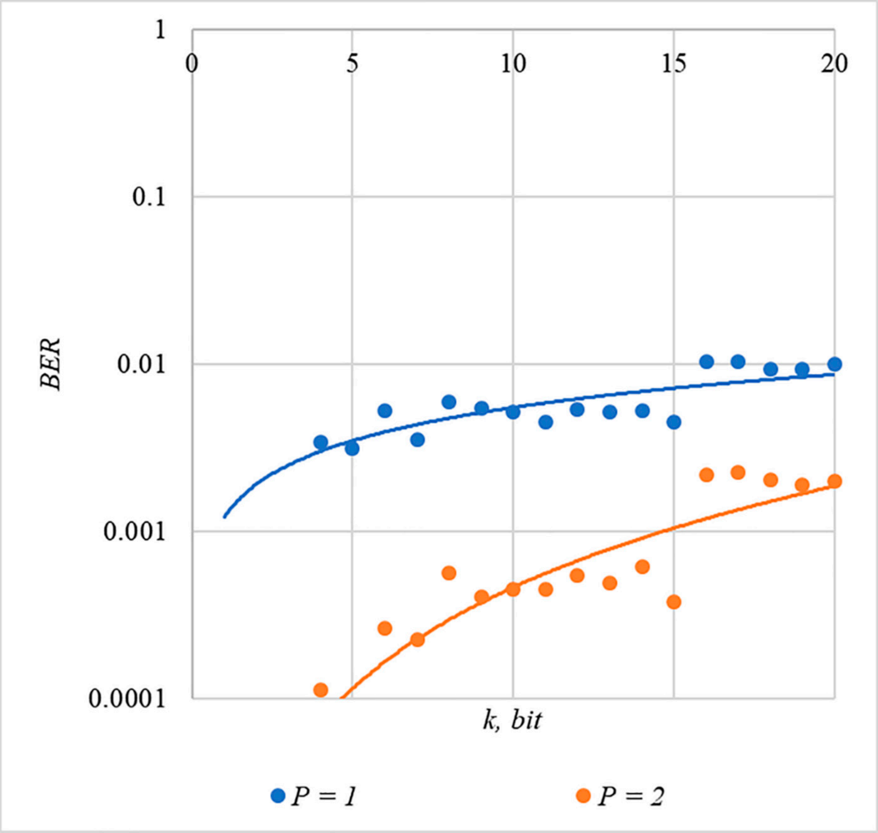

Figure 6. *BER*(*k*) dependencies for different values of *P* rule for generating chip codes №5.

The analysis of the results obtained (see Figures 2–6) enables us to make the following observations.

First, an increase in the coefficient P makes it possible to achieve low BER values for any of the considered classes of chip codes. At the same time, chip codes with generation rules №1, 2 and 3, 4 give similar BER values, i.e., for this indicator, such spreading sequences are equivalent to each other.

Walsh–Hadamard sequences give significantly better results in terms of error rates. Even at low values of P, these chip codes provide low BER.

The second observation is that the BER increases as the number of bits in the hidden message increases. However, different chip codes give different results. For example, spreading sequences №1 and №2 at $k = 10$ provide $BER < 10\%$ only at $P > 8$. For chip codes №3 and №4, the same is provided with a lower power gain, for example, for $P > 4$. The Walsh–Hadamard sequences even with $P = 1$ and $k = 20$ provide $BER < 1\%$.

In order to compare the BER dependences corresponding to different methods of forming chip codes, Figure 7 shows diagrams $BER(P)$. These are averaged over 5000 test results for $k = 20$ bits.

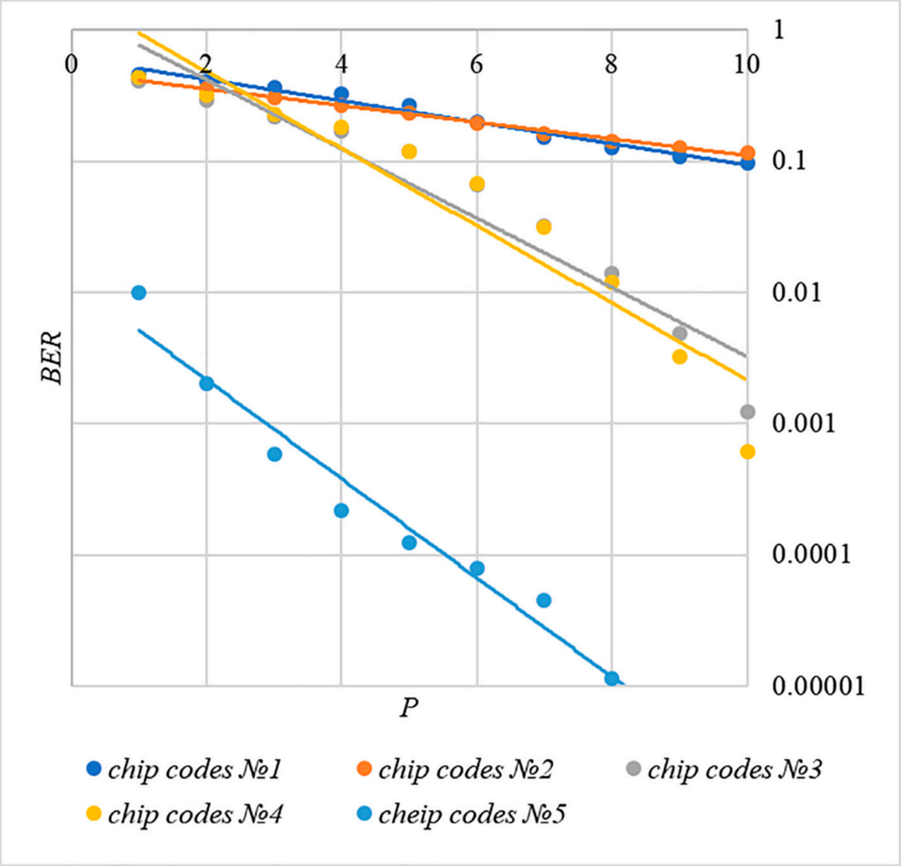

Figure 7. $BER(P)$ dependencies for different rules for generating chip codes, $k = 20$.

The analysis of the results shown in Figure 7 demonstrates that the techniques for generating chip codes №1 and №2, as well as №3 and №4, do indeed give similar BER values. However, such a difference in the BER value is observed only for large k values. With a small number of hidden bits, the BER values for chip codes №1–4 are practically the same. This is clearly seen in Figure 8. Thus, for small values of k, it is really possible to achieve a low error rate for practically any method of forming chip codes.

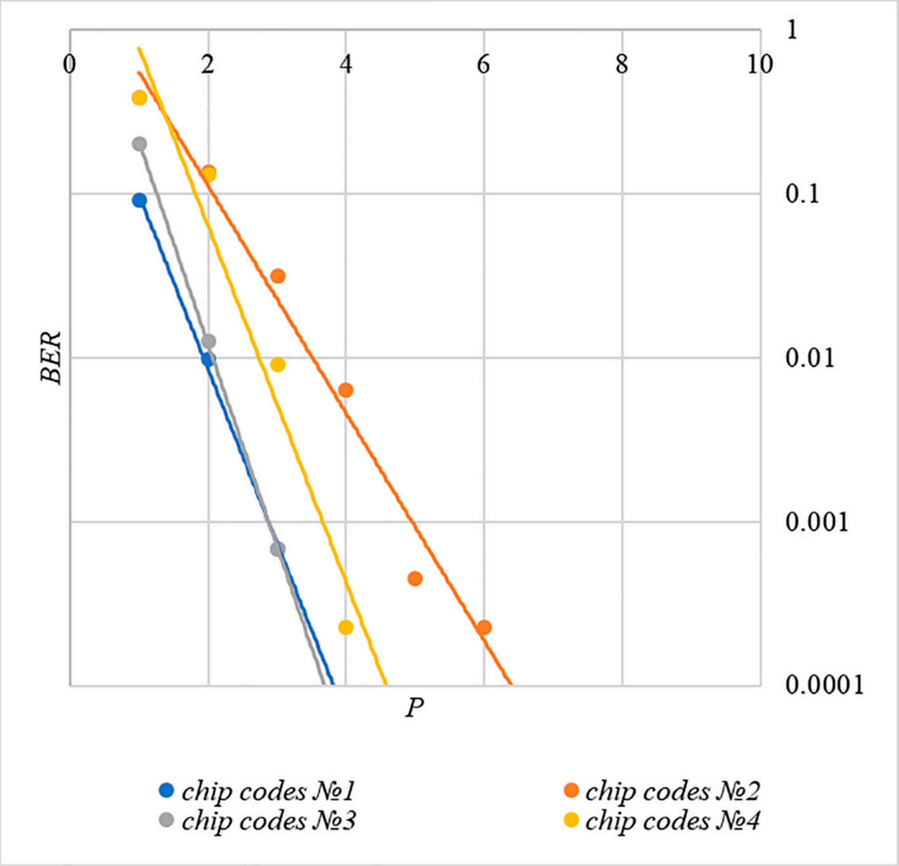

Figure 8. $BER(P)$ dependencies for different rules for generating chip codes, $k = 1$.

Walsh–Hadamard sequences show significantly better BER results. For this family of chip codes, the error rate, other things being equal, is one to two orders of magnitude lower. At the same time, BER can be significantly reduced only for large P values, and this will inevitably lead to container distortion.

4.2. Experimental Evaluation of Container Distortion

We used MSE and PSNR to assess container distortion. The obtained experimental results indicate that using chip codes generated according to rules 1, 3, 4, and 5 leads to approximately equal distortions of containers. The corresponding dependences of $MSE(k)$ and $PSNR(k)$ for different values are shown in Figures 9 and 10.

Somewhat less distortion of the container is provided by using the rule for generating chip codes №2; the corresponding dependencies are shown in Figures 11 and 12.

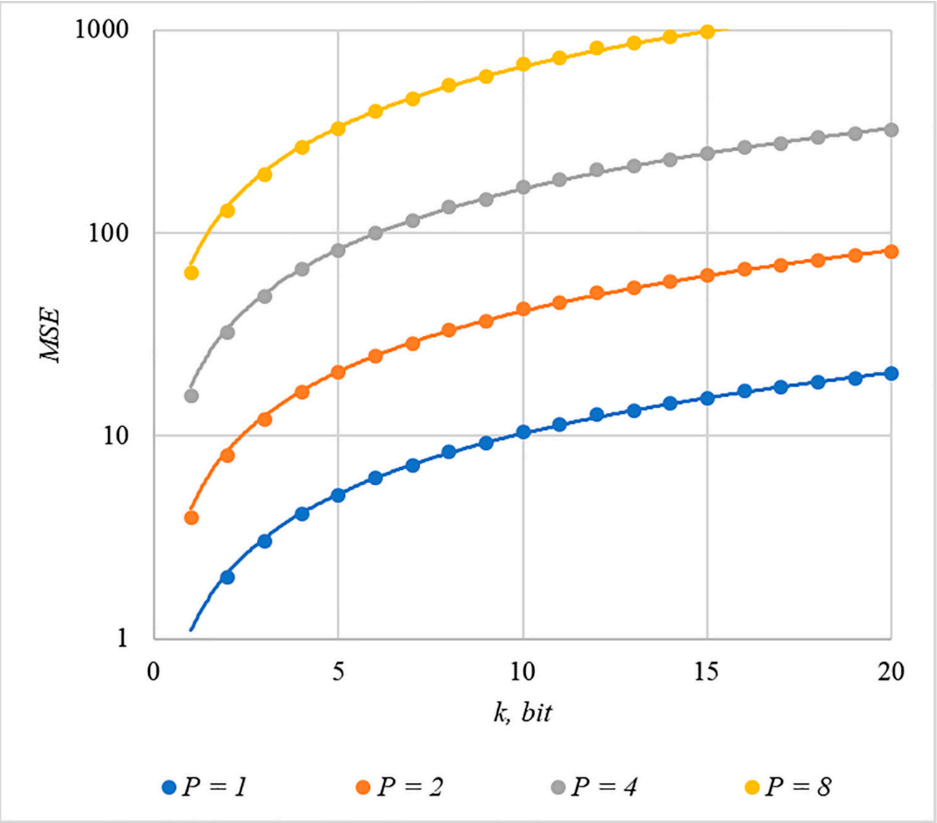

Figure 9. *MSE*(*k*) dependencies for different values of *P* rules for generating chip codes №1, 3, 4, and 5.

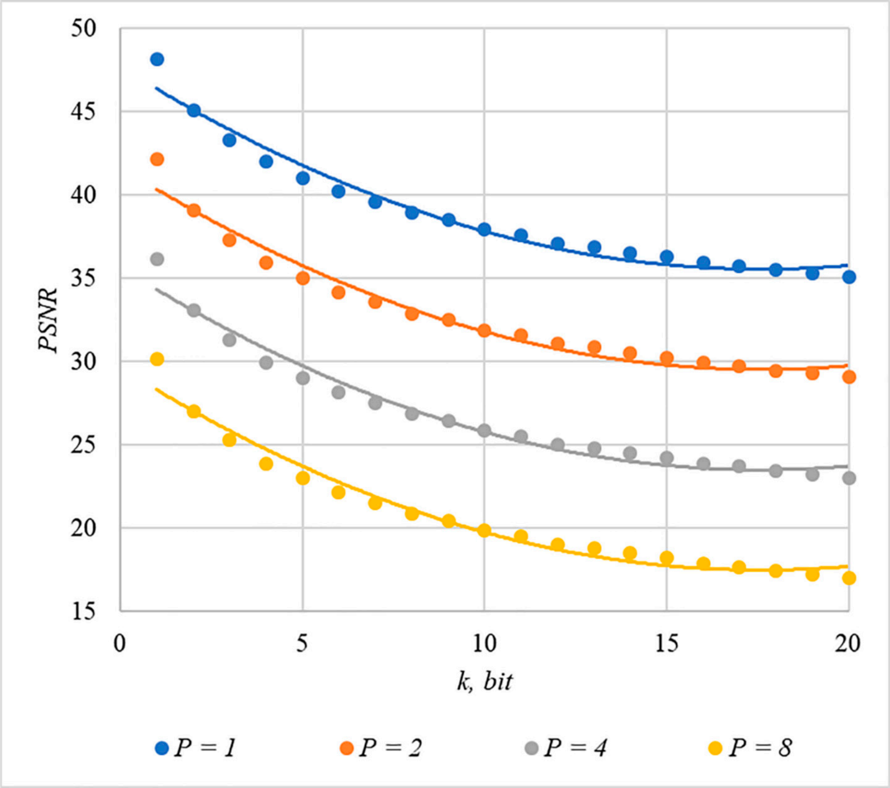

Figure 10. *PSNR*(*k*) dependencies for different values of *P* rules for generating chip codes №1, 3, 4, and 5.

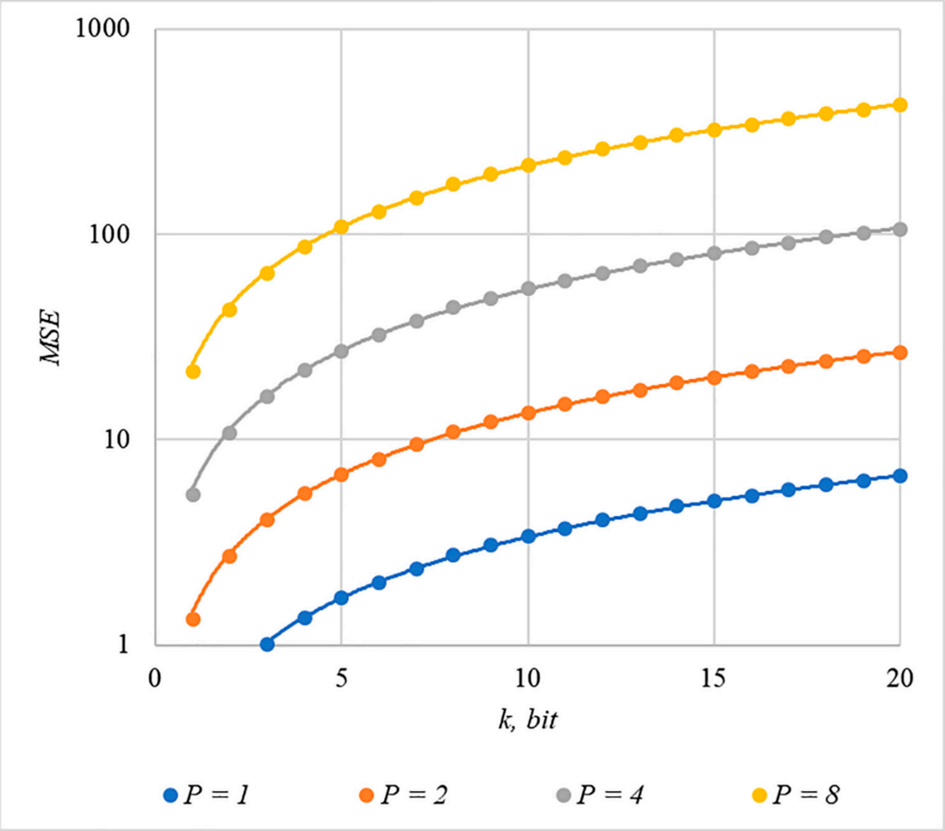

Figure 11. *MSE*(*k*) dependencies for different values of *P* rule for generating chip codes №2.

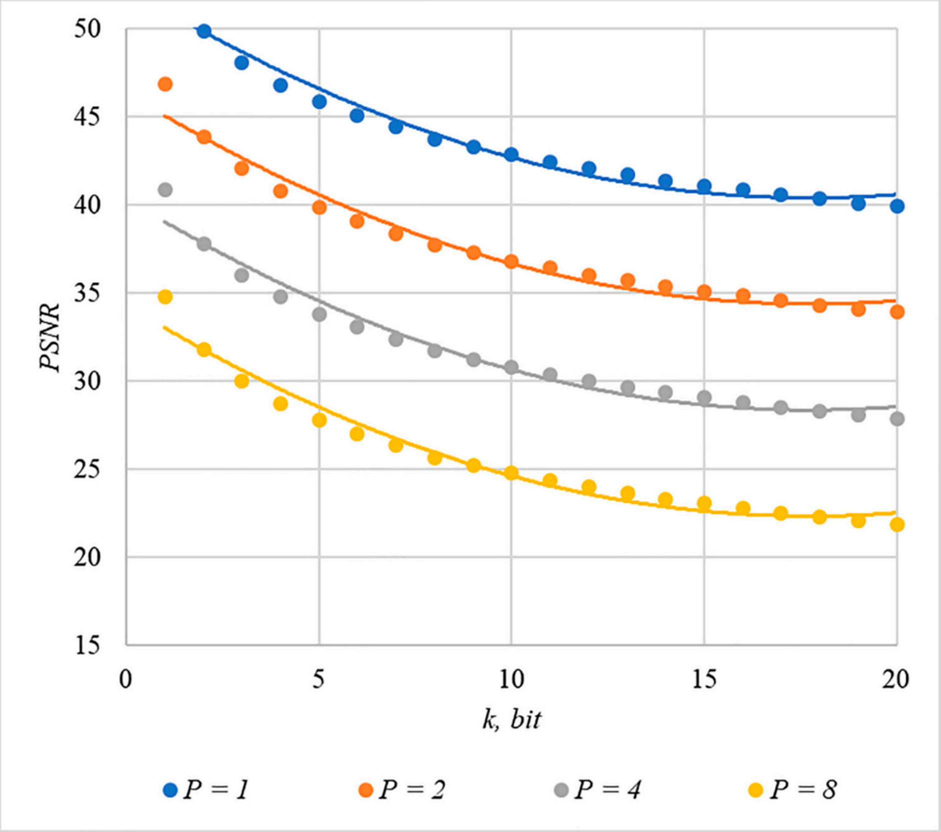

Figure 12. *PSNR*(*k*) dependencies for different values of *P*, rule for generating chip codes №2.

The analysis of Figures 9–12 enables us to make the following observations.

First, an increase in the number of hidden information bits leads to an inevitable increase in container distortion. Usually, PSNR values of about 30–40 dB are considered acceptable quality. If you focus on these values, then you can effectively hide no more than 10–20 information bits.

Secondly, an increase in the power gain P also leads to an increase in container distortion. If we focus on PSNR of about 30.40 dB, then the values of $P < 8$ are acceptable (with $k < 4$).

Thus, the obtained results of experimental studies show that by increasing the length k of the hidden message, we inevitably distort the container. Raising P in order to reduce BER also leads to an increase in container distortion. Thus, there are several conflicting factors that directly affect the efficiency of the steganosystem. In order to find a compromise, it is necessary to study the influence of these factors on each other.

4.3. *Correlation of Error Rate and Container Distortion, Finding a Compromise*

In order to find a compromise solution, let us study the relationship between BER and PSNR.

In Figures 13–17 the dependences obtained as a result of averaging over 5000 tests are shown.

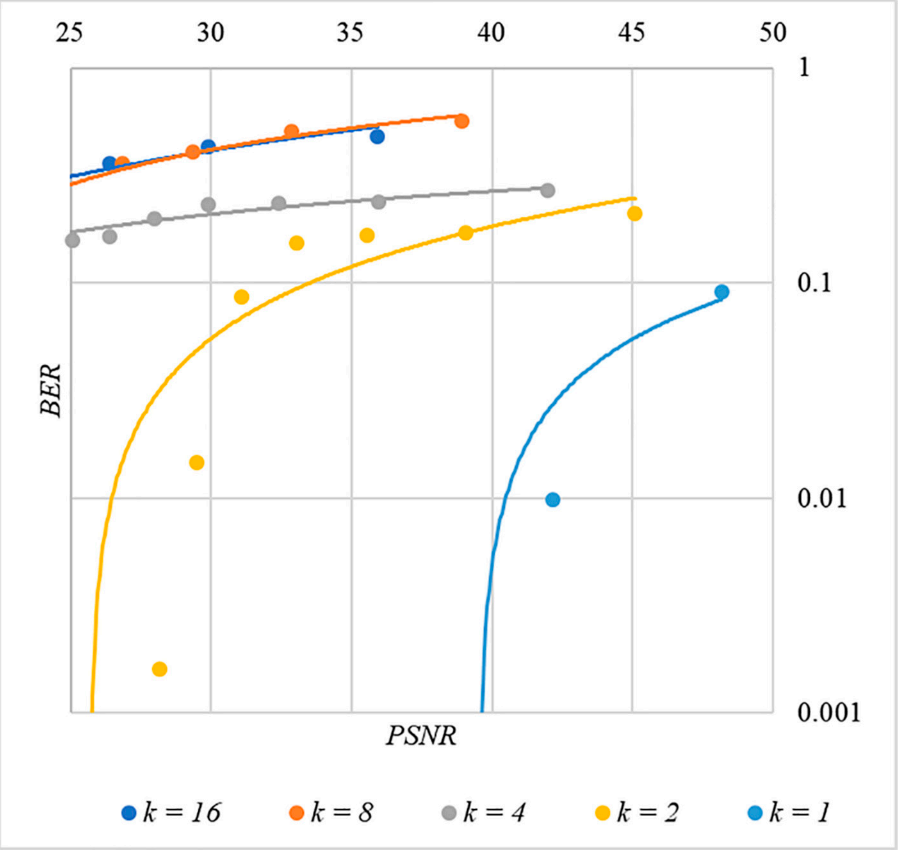

Figure 13. *BER*(*PSNR*) dependencies for different values k rule for generating chip codes №1.

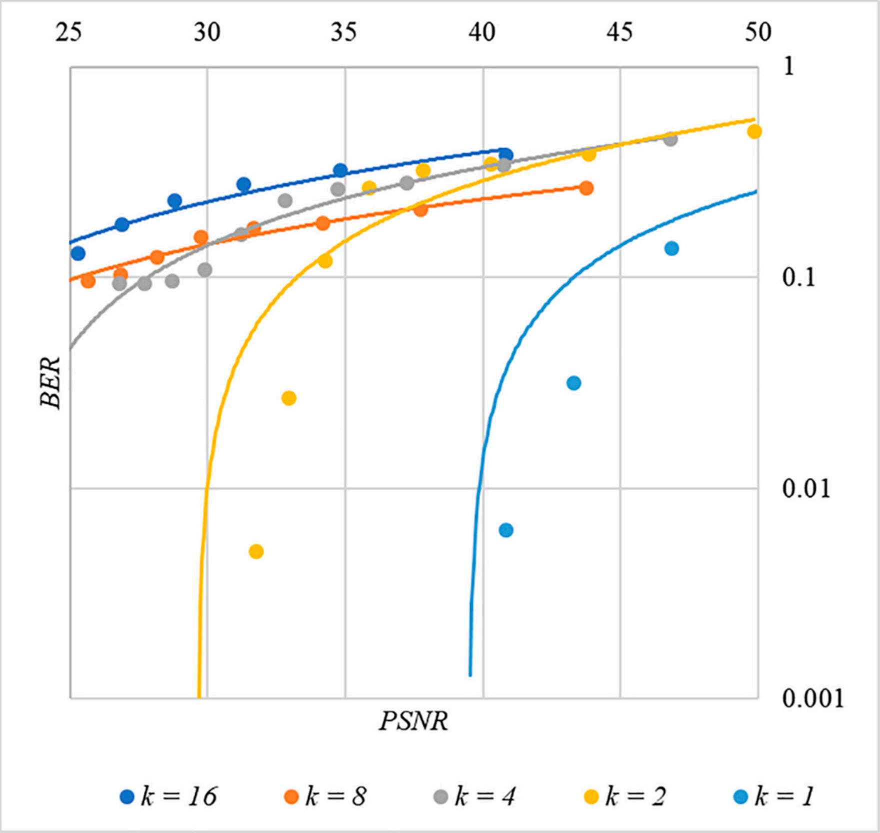

Figure 14. *BER*(*PSNR*) dependencies for different values *k* rule for generating chip codes №2.

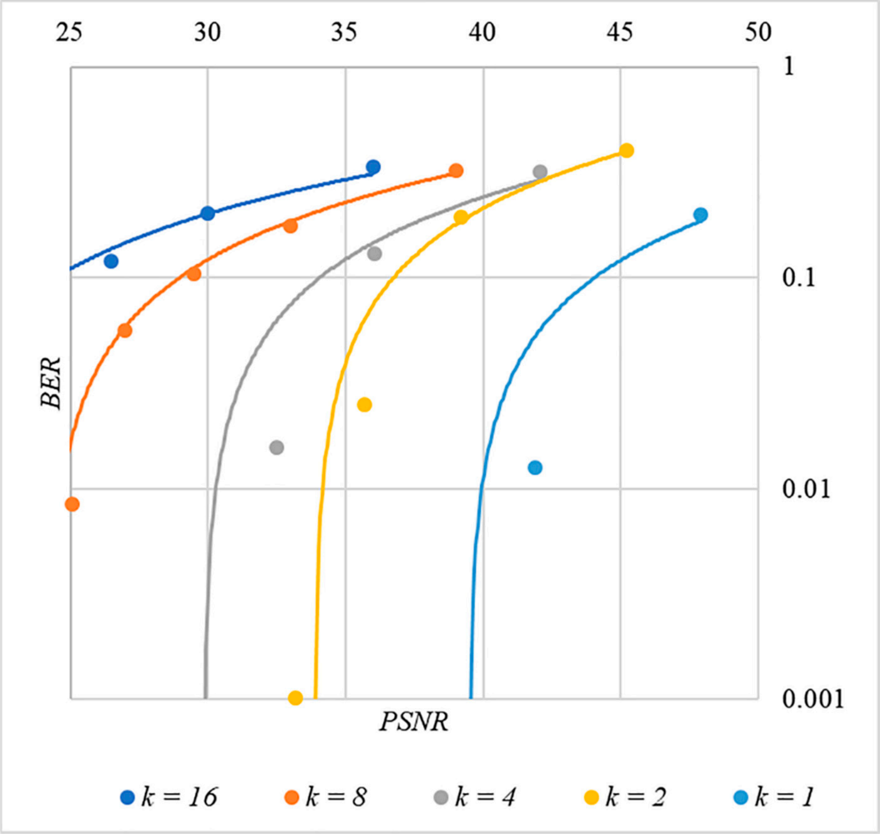

Figure 15. *BER*(*PSNR*) dependencies for different values *k* rule for generating chip codes №3.

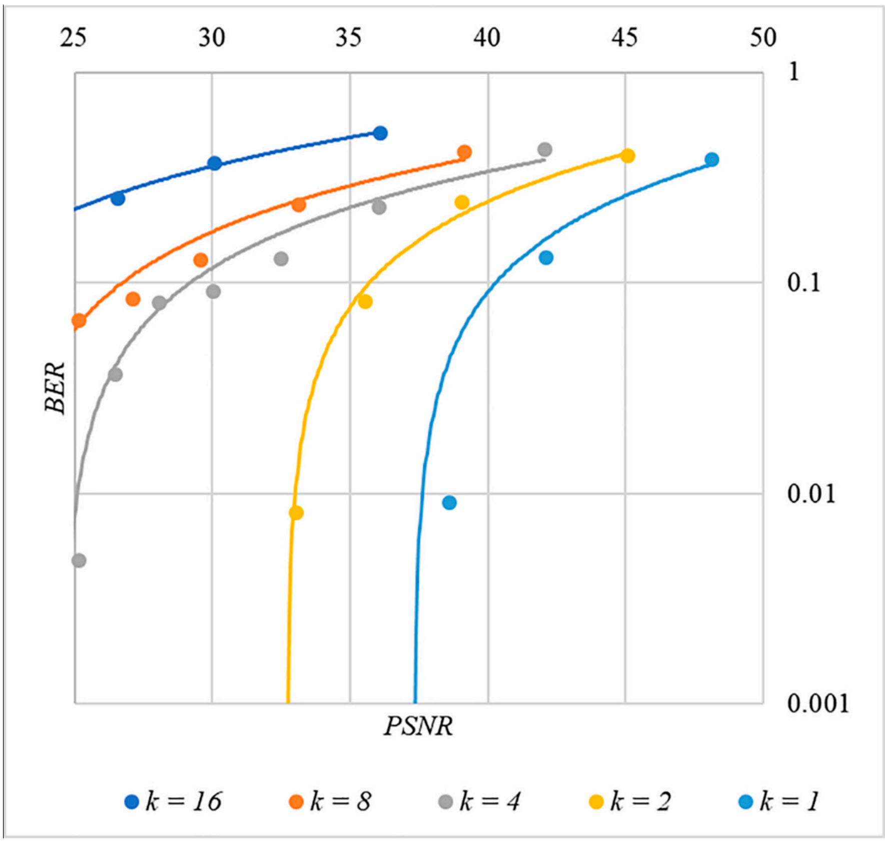

Figure 16. *BER*(*PSNR*) dependencies for different values *k* rule for generating chip codes №4.

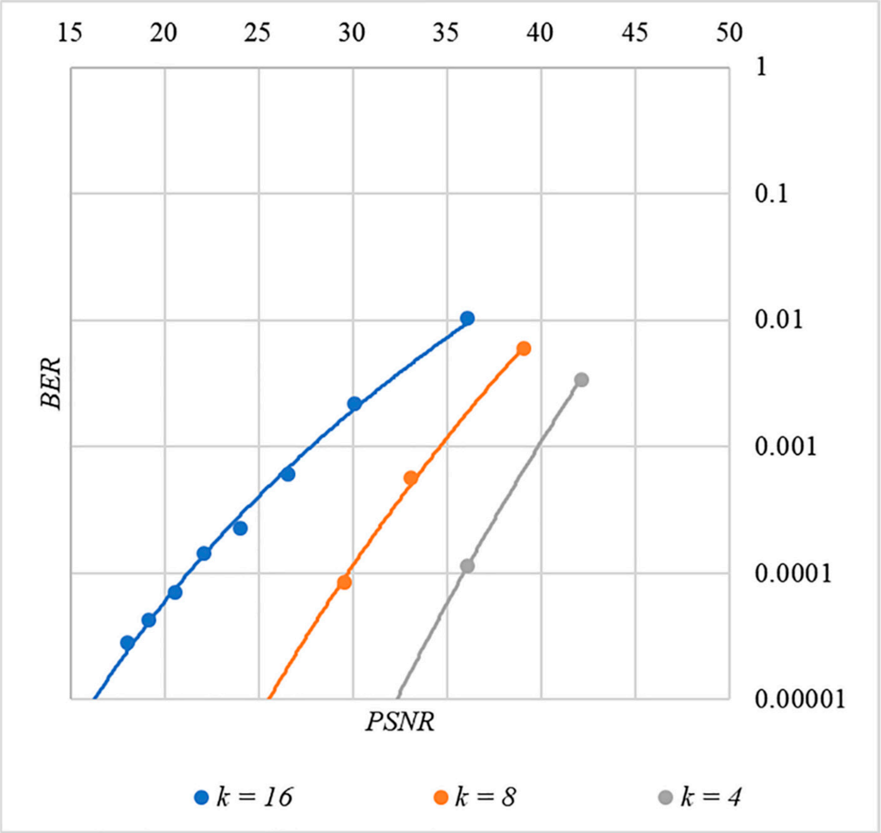

Figure 17. *BER*(*PSNR*) dependencies for different values *k* rule for generating chip codes №5.

5. Discussion

The analysis of the data shown in Figures 2–17 results enables us to draw the following conclusions.

First, it is difficult to implement information hiding without significant container distortion. The above dependences of $BER(PSNR)$ clearly demonstrate this. By increasing the volume of the hidden message k and/or the power amplification factor P, we certainly distort the container, i.e., decrease PSNR. For example, chip codes №1 and №2 allow hiding only 1–2 bits of the message when $PSNR > 30$ dB and $BER < 10\%$. Spreading sequences №3 and №4 are somewhat better; they make it possible to hide 1–2 message bits when $PSNR > 35$ dB and $BER < 10\%$. However, this is still not enough. Finally, the Walsh–Hadamard signals perform well. If they are used, it is possible to hide 16 or more message bits and provide $PSNR > 30$ dB and $BER < 1\%$. This confirms the earlier conclusion about the preference of such chip codes for hiding information. This is also consistent with our findings from Spread Spectrum Image Steganography [23,24].

The second conclusion is a possible trade-off between the amount of hidden data and the introduced distortion of the audio container. For example, as follows from Figure 17, halving the k value leads to an increase in PSNR by about 5 dB. This can be used to configure the desired stegosystem parameters in a specific practical application.

The third and probably the most important conclusion is that it is almost impossible to achieve high volumes of hidden information with the known techniques. For example, even for the best case shown in Figure 17, with $PSNR = 35$ dB and $BER < 1\%$, only $k \leq 16$ bits of information can be hidden. It is possible to improve these values by traditional techniques only by increasing the length of the chip codes, which inevitably leads to an increase in the computational complexity of the transformations. This could, however, become a problem. Indeed, to restore each closed beta according to rule (8), it is necessary to calculate the correlation according to Equation (5). Therefore, you need to perform n additions and n multiplications, where n is the length of the chip codes. Our experiments correspond to the case of $n = 1024$, and we had a performance comparable to other modern data hiding techniques. However, as n increases, performance decreases, which can significantly complicate practical implementation.

Another way is the implementation of adaptive techniques, for example, as in [55,56], or the use of new, advanced methods of hiding information, for example, based on addressing chip codes [58]. These and other methods are a promising direction for our further research.

6. Conclusions

In the present paper, we explored techniques for hiding information in audio containers using a direct spread spectrum. We considered various spreading sequences (chip codes) and studied their influence on the error rate in recovered messages. We also investigated the distortion of the audio container in terms of MSE and PSNR.

The results clearly demonstrate the promising characteristics of this direction. Precisely, in each segment of the container, we managed to hide a part of the information message reliably. At the same time, the BER, MSE, and PSNR values are within an acceptable range. The best characteristics were shown by Walsh–Hadamard chip codes, which showed the lowest error rate (with comparable container distortions).

At the same time, it should be noted that there exist objectively conflicting factors that negatively affect one another. For example, by increasing the volume of hidden messages, we inevitably increase the BER and distort the container. By increasing the power of the chip codes, it is possible to reduce the BER. However, this distorts the container even more. This is consistent with known results in steganography based on direct spectrum expansion. For example, in [41,53], it is shown that by increasing the power of chip codes, it is really possible to reduce BER, but the distortion of the covers becomes very significant. We managed to present the availability of compromise solutions. This is especially true for Walsh–Hadamard chip codes, for which the range of possible solutions is much wider than for other spreading sequences. Nevertheless, it should be noted that when using traditional data hiding techniques, the volume of hidden messages cannot be large. The search for new ways of hiding information is promising, e.g., based on the adaptive formation of spreading sequences [56], advanced techniques for addressing chip codes [58], etc.

Author Contributions: Conceptualization and methodology, A.K.; software and validation, A.O. and T.G.; writing—review and editing, O.P. and R.Z.; visualization, K.W. All authors have read and agreed to the published version of the manuscript.

Funding: The research work reported in this paper was in part supported by the National Centre for Research and Development, Poland, under project no. POIR.04.01.04-00-0048/20.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Li, R.; Xu, S.; Rong, B.; Yang, H. Host Cancelation-Based Spread Spectrum Watermarking for Audio Anti-Piracy over Internet. *Secur. Commun. Netw.* **2016**, *9*, 4691–4702. [CrossRef]
2. Manoj, I.V.S. Cryptography and Steganography. *Int. J. Comput. Appl.* **2010**, *1*, 63–68. [CrossRef]
3. Moulin, P.; O'Sullivan, J.A. Information-Theoretic Analysis of Information Hiding. *IEEE Trans. Inf. Theory* **2003**, *49*, 563–593. [CrossRef]
4. Aroua, S.; Champagnat, R.; Coustaty, M.; Falquet, G.; Ghadfi, S.; Ghamri-Doudane, Y.; Gomez-Kramer, P.; Howells, G.; McDonald-Maier, K.D.; Murphy, J.; et al. Security and PrIvacy foR the Internet of Things: An Overview of the Project. In Proceedings of the 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), Bari, Italy, 6–9 October 2019; pp. 3993–3998.
5. Fazzat, A.; Khatoun, R.; Labiod, H.; Dubois, R. A Comparative Performance Study of Cryptographic Algorithms for Connected Vehicles. In Proceedings of the 2020 4th Cyber Security in Networking Conference (CSNet), Lausanne, Switzerland, 21–23 October 2020; pp. 1–8.
6. Levi, I.; Rudin, Y.; Fish, A.; Keren, O. Embedded Randomness and Data Dependencies Design Paradigm: Advantages and Challenges. In Proceedings of the 2018 Design, Automation Test in Europe Conference Exhibition (DATE), Dresden, Germany, 19–23 March 2018; pp. 395–400.
7. Menezes, A.J.; van Oorschot, P.C.; Vanstone, S.A.; van Oorschot, P.C.; Vanstone, S.A. *Handbook of Applied Cryptography*; CRC Press: Boca Raton, FA, USA, 2018; ISBN 978-0-429-46633-5.
8. Yahya, A. Steganography Techniques. In *Steganography Techniques for Digital Images*; Yahya, A., Ed.; Springer International Publishing: Cham, Switzerland, 2019; pp. 9–42, ISBN 978-3-319-78597-4.
9. Fridrich, J. *Steganography in Digital Media: Principles, Algorithms, and Applications*; Illustrated Edition; Cambridge University Press: Cambridge, MA, USA; New York, NY, USA, 2009; ISBN 978-0-521-19019-0.
10. WAV File Extension-What Is It? How to Open a WAV File? Available online: https://filext.com/file-extension/WAV (accessed on 25 April 2021).
11. Fleischman, E. WAVE and AVI Codec Registries. Available online: https://tools.ietf.org/html/rfc2361 (accessed on 25 April 2021).
12. Song, T.; Zhou, K.; Li, T. CDMA System Design and Capacity Analysis Under Disguised Jamming. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 2487–2498. [CrossRef]
13. Wang, X.; Liu, X.; Chen, H.-H.; Meng, W. Complementary Coded CDMA Systems With CP-Free OFDM. *IEEE Trans. Veh. Technol.* **2020**, *69*, 11515–11528. [CrossRef]
14. Sedaghat, M.A.; Müller, R.R.; Marvasti, F. On Optimum Asymptotic Multiuser Efficiency of Randomly Spread CDMA. *IEEE Trans. Inf. Theory* **2015**, *61*, 6635–6642. [CrossRef]
15. Khalife, J.; Kassas, Z.M. Navigation with Cellular CDMA Signals—Part II: Performance Analysis and Experimental Results. *IEEE Trans. Signal Process.* **2018**, *66*, 2204–2218. [CrossRef]
16. Stüber, G.L. Spread Spectrum Techniques. In *Principles of Mobile Communication*; Stüber, G.L., Ed.; Springer International Publishing: Cham, Switzerland, 2017; pp. 449–499, ISBN 978-3-319-55615-4.
17. Torrieri, D. Chapter 2 Direct-Sequence Systems. In *Principles of Spread-Spectrum Communication Systems*; Torrieri, D., Ed.; Springer International Publishing: Cham, Switzerland, 2015; pp. 79–145, ISBN 978-3-319-14096-4.
18. Ipatov, V.P. *Spread Spectrum and CDMA: Principles and Applications*; John Wiley & Sons, Ltd.: Chichester, UK, 2005; ISBN 978-0-470-09180-7.
19. Torrieri, D. *Principles of Spread-Spectrum Communication Systems*; Springer International Publishing: Cham, Switzerland, 2018.
20. Smith, J.R.; Comiskey, B.O. Modulation and Information Hiding in Images. In *International Workshop on Information Hiding*; Anderson, R., Ed.; Springer: Berlin/Heidelberg, Germany, 1996; pp. 207–226.

21. Marvel, L.M.; Boncelet, C.G.; Retter, C.T. *Methodology of Spread-Spectrum Image Steganography*; Army Research Lab Aberdeen Proving: Ground, MD, USA, 1998.
22. Wang, Y.-G.; Zhu, G.; Kwong, S.; Shi, Y.-Q. A Study on the Security Levels of Spread-Spectrum Embedding Schemes in the WOA Framework. *IEEE Trans. Cybern.* **2018**, *48*, 2307–2320. [CrossRef] [PubMed]
23. Kuznetsov, A.; Smirnov, O.; Arischenko, A.; Chepurko, I.; Onikiychuk, A.; Kuznetsova, T. Pseudorandom Sequences for Spread Spectrum Image Steganography. In Proceedings of the International Workshop on Cyber Hygiene (CybHyg-2019) Co-Located with 1st International Conference on Cyber Hygiene and Conflict Management in Global Information Networks (CyberConf 2019), Kyiv, Ukraine, 30 November 2019; CEUR-WS.org: Tilburg, The Netherlands, 2020; Volume 2654, pp. 122–131.
24. Kuznetsov, A.; Smirnov, A.; Gorbacheva, L.; Babenko, V. Hiding Data in Cover Images Using a Pseudo-Random Sequences. In Proceedings of the Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020), Zaporizhzhia, Ukraine, 27 April–1 May 2020; Subbotin, S., Ed.; CEUR-WS.org: Tilburg, The Netherlands, 2020; Volume 2608, pp. 646–660.
25. Avci, D.; Tuncer, T.; Avci, E. A New Information Hiding Method for Audio Signals. In Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22–25 March 2018; pp. 1–4.
26. Rajput, S.P.; Adhiya, K.P.; Patnaik, G.K. An Efficient Audio Steganography Technique to Hide Text in Audio. In Proceedings of the 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, 17–18 August 2017; pp. 1–6.
27. Nassrullah, H.A.; Flayyih, W.N.; Nasrullah, M.A. Enhancement of LSB Audio Steganography Based on Carrier and Message Characteristics. *J. Inf. Hiding Multimed. Signal Process.* **2020**, *11*, 126–137.
28. Ramya, G.; Janarthanan, P.P.; Mohanapriya, D. Steganography Based Data Hiding for Security Applications. In Proceedings of the 2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW), Erode, India, 14–15 December 2018; pp. 131–135.
29. Lee, M.C.; Lau, C.Y. Three Orders Mixture Algorithm of Audio Steganography Combining Cryptography. *J. Inf. Hiding Multimed. Signal Process.* **2018**, *9*, 959–969.
30. Akbay, K.; Konyar, M.Z.; İlkın, S.; Sondaş, A. Data Hiding Using Shuffle Algorithm and LSB Method. In Proceedings of the 2018 26th Signal Processing and Communications Applications Conference (SIU), Izmir, Turkey, 2–5 May 2018; pp. 1–4.
31. Gopalan, K. Audio Steganography for Information Hiding and Covert Communication–a Tutorial. In Proceedings of the 2018 IEEE International Conference on Electro/Information Technology (EIT), Rochester, MI, USA, 3–5 May 2018; pp. 0242–0243.
32. Unoki, M.; Imabeppu, K.; Hamada, D.; Haniu, A.; Miyauchi, R. Embedding Limitations with Digital-Audio Watermarking Method Based on Cochlear Delay Characteristics. *J. Inf. Hiding Multimed. Signal Process.* **2011**, *2*, 1–23.
33. Altinbaş, A.E.; Yalman, Y. Bit Reduction Based Audio Steganography Algorithm. In Proceedings of the 2021 6th International Conference on Computer Science and Engineering (UBMK), Ankara, Turkey, 15–17 September 2021; pp. 703–706.
34. Tabara, B.; Wojtuń, J.; Piotrowski, Z. Data Hiding Method in Speech Using Echo Embedding and Voicing Correction. In Proceedings of the 2017 Signal Processing Symposium (SPSympo), Debe, Poland, 12–14 September 2017; pp. 1–6.
35. Wang, S.; Yuan, W.; Unoki, M. Multi-Subspace Echo Hiding Based on Time-Frequency Similarities of Audio Signals. *IEEE/ACM Trans. Audio Speech Lang. Process.* **2020**, *28*, 2349–2363. [CrossRef]
36. Latypov, R.K.; Stolov, E.L. Ternary Echo Hiding in Audio Files. In Proceedings of the 2020 28th Telecommunications Forum ($^{\mathrm{TEL}}$FOR), Belgrade, Serbia, 24–25 November 2020; pp. 1–4.
37. Cho, K.; Bae, S.H.; Choi, I.K.; Kim, N.S.; Unoki, M. Robust Audio Data Hiding Method Based on Phase of Modulated Complex Lapped Transform. In Proceedings of the 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Beijing, China, 16–18 October 2013; pp. 263–266.
38. Manunggal, T.T.; Arifianto, D. Data Protection Using Interaural Quantified-Phase Steganography on Stereo Audio Signals. In Proceedings of the 2016 IEEE Region 10 Conference (TENCON), Singapore, 22–25 November 2016; pp. 3817–3821.
39. Ginanjar, R.R.; Bhardwaj, S.; Kim, D.-S.; Lee, J.-M. Rounding Modulation for Transparent Data-Hiding Scheme in High-Quality Audio File. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 11–13 January 2019; pp. 1–2.
40. Marvel, L.M.; Boncelet, C.G.; Retter, C.T. Spread Spectrum Image Steganography. *IEEE Trans. Image Process.* **1999**, *8*, 1075–1083. [CrossRef] [PubMed]
41. Marvel, L.M. *Image Steganography for Hidden Communication*; Army Research Lab Aberdeen Proving: Ground, MD, USA, 2000.
42. Youail, R.S.; Samawi, V.W.; Kadhim, A.-K.A.-R. Combining a Spread Spectrum Technique with Error-Correction Code to Design an Immune Stegosystem. In Proceedings of the Security and Identification 2008 2nd International Conference on Anti-counterfeiting, Guiyang, China, 20–23 August 2008; pp. 245–248.
43. Agrawal, N.; Gupta, A. DCT Domain Message Embedding in Spread-Spectrum Steganography System. In Proceedings of the 2009 Data Compression Conference, Washington, DC, USA, 16–18 March 2009; p. 433.
44. Lu, L.; Sun, X.; Cai, L. A Robust Image Watermarking Based on DCT by Arnold Transform and Spread Spectrum. In Proceedings of the 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Chengdu, China, 20–22 August 2010; Volume 1, pp. V1-198–V1-201.
45. Satish, K.; Jayakar, T.; Tobin, C.; Madhavi, K.; Murali, K. Chaos Based Spread Spectrum Image Steganography. *IEEE Trans. Consum. Electron.* **2004**, *50*, 587–590. [CrossRef]

46. Kumar, A.; Albagul, A.; Ghose, M.; Negrat, K. Improved Chaos Based Spread Spectrum Image Steganography. In Proceedings of the 10th IASTED International Conference, Beijing China, 8–10 October 2008; pp. 18–20.
47. Weihua, X.; Yongbing, W.; Shuiyuan, Y.H. 264 Video Watermark Algorithm Using DCT Spread Spectrum. In Proceedings of the 2015 3rd International Conference on Applied Computing and Information Technology/2nd International Conference on Computational Science and Intelligence, Okayama, Japan, 12–16 July 2015; pp. 447–450.
48. Zarmehi, N.; Akhaee, M.A. Video Steganalysis of Multiplicative Spread Spectrum Steganography. In Proceedings of the 2014 22nd European Signal Processing Conference (EUSIPCO), Lisbon, Portugal, 1–5 September 2014; pp. 2440–2444.
49. Nugraha, R.M. Implementation of Direct Sequence Spread Spectrum Steganography on Audio Data. In Proceedings of the 2011 International Conference on Electrical Engineering and Informatics, Bandung, Indonesia, 17–19 July 2011; pp. 1–6.
50. Li, X.; Yu, H.H. Transparent and Robust Audio Data Hiding in Subband Domain. In Proceedings of the International Conference on Information Technology: Coding and Computing (Cat. No.PR00540), Las Vegas, NV, USA, 27–29 March 2000; pp. 74–79.
51. Hernandez-Garay, S.; Vazquez-Medina, R.; Nino de Rivera, L.; Ponomaryov, V. Steganographic Communication Channel Using Audio Signals. In Proceedings of the 2008 12th International Conference on Mathematical Methods in Electromagnetic Theory, Odessa, Ukraine, 29 June–2 July 2008; pp. 427–429.
52. Sklar, B. *Digital Communications: Fundamentals and Applications*, 2nd ed.; Prentice Hall: Upper Saddle River, NJ, USA, 2017; ISBN 978-0-13-472405-8.
53. Brundick, F.S.; Marvel, L.M. *Implementation of Spread Spectrum Image Steganography*; Defense Technical Information Center: Fort Belvoir, VA, USA, 2001.
54. Boncelet, J.C.G.; Marvel, L.M.; Retter, C.T. Spread Spectrum Image Steganography/Unified Patents. Patents US6557103B1, 29 April 2003.
55. Kuznetsov, A.; Smirnov, O.; Kovalchuk, D.; Kuznetsova, T. New Technique for Data Hiding in Cover Images Using Adaptively Generated Pseudorandom Sequences. In Proceedings of the International Workshop on Cyber Hygiene (CybHyg-2019) co-located with 1st International Conference on Cyber Hygiene and Conflict Management in Global Information Networks (CyberConf 2019), Kyiv, Ukraine, 30 November 2019; CEUR-WS.org: Tilburg, The Netherlands, 2020; Volume 2654, pp. 1–14.
56. Kuznetsov, A.; Smirnov, O.; Onikiychuk, A.; Makushenko, T.; Anisimova, O.; Arischenko, A. Adaptive Pseudo-Random Sequence Generation for Spread Spectrum Image Steganography. In Proceedings of the 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 14–18 May 2020; pp. 161–165.
57. Gaudeamus Igitur. Available online: http://graecolatini.bsu.by/texts/gaudeamus/gaudeamus-data/gaudeamus03.mp3 (accessed on 7 May 2021).
58. Kuznetsov, A.; Kiian, A.; Kuznetsova, K.; Smirnov, A. Data Hiding Scheme Based on Spread Sequence Addressing. In Proceedings of the 1st International Workshop on Computational & Information Technologies for Risk-Informed Systems (CITRisk 2020) co-located with XX International scientific and technical conference on Information Technologies in Education and Management (ITEM 2020), Kherson, Ukraine, 15–16 October 2020; pp. 44–58.