New Technique for Hiding Data Using Adaptively Generated Pseudorandom Sequences

Alexandr Kuznetsov [1 [0000-0003-2331-6326]], Oleksii Smirnov [2[0000-0001-9543-874X]], Diana Kovalchuk [1[0000-0002-4499-3732]] and Tetiana Kuznetsova [1[0000-0002-5605-9293]]

[1]V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkiv, 61022, Ukraine
kuznetsov@karazin.ua, dianakovalhyk@ukr.net
[2]Central Ukrainian National Technical University, avenue University, 8, Kropivnitskiy, 25006, Ukraine, dr.smirnovoa@gmail.com

Abstract. This article explores the steganographic techniques of hiding information using direct spectrum expansion technology. Using noise-like pseudorandom sequences (discrete signals), it is possible to reliably hide information messages in redundant digital data (cover files), for example, images, video and audio files, etc. However, the correlation of discrete signals and cover files can be a problem; the extracted information messages can cover a lot of the number of errors. Our experiments (on still images) show that the error rate in the reconstructed information messages is very high. We offer a new technique when the statistical properties of covers are taken into account when generating discrete signals. In this case, it is possible to significantly reduce the error rate without introducing additional distortion in-to the cover.

Keywords: pseudorandom sequence, hidden information, direct spectrum spread technology, steganography

1 Introduction

Direct spread spectrum technology has traditionally been used in code division multiple access radio communication systems (CDMA). These techniques are used for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference, noise, and jamming, to prevent detection, to limit power flux density (e.g., in satellite down links), and to enable multiple-access communications [1-3].

The technology of direct spectrum expansion uses discrete noise-like sequences (discrete signals) to expand a usually narrowband information signal over a relatively wideband (radio) frequency range. The receiver correlates received signals to extract the original information signal.

Thus, the basic principle of direct spectrum spreading is the use of noise-like carriers and the bandwidth is much wider than that required for simple point-to-point communication with the same data rate. This allows you to get significant advantages in the organization of communication, for example [1-3]:

- Resistance to jamming (interference). High resistance to narrowband interference is provided;
- Resistance to eavesdropping. The selection of a particular pseudo-random sequence can be saved as a secret key. In this case, it is very difficult to find the right key and eavesdrop on the negotiations. In addition, when using very long pseudorandom sequences, it is possible to arrange communication at very low signal to noise ratios, which does not even allow the secret transmission of information to be detected;
- Resistance to fading. The expansion of the frequency band leads to an increase in the quality of communication, even in conditions of fading (attenuation) of the signal;
- Multiple access capability. A large number of sequences allows to increase the subscriber capacity of the communication system, i.e. after all, makes communication much cheaper.

Direct spectrum spreading technology can also be used for steganographic purposes, i.e. to hide information messages in redundant digital data (cover files), for example, in images, video and audio files, etc. Moreover, cover files are interpreted as noise in communication channels, and the number of different discrete signals determines the channel capacity of the steganosystem (similar to multiple access to CDMA).

This article explores the steganographic techniques of hiding information using direct spectrum expansion technology. We offer a new technique when the statistical properties of cover files are taken into account when generating discrete signals. This allows you to significantly improve individual performance indicators of the steganosystem. In particular, we manage to significantly reduce the bit error rate in the extracted informational messages.

2 Literature review

In the first works [4-7] on steganographic systems based on direct spectrum expansion, the fundamental possibility of hiding data in various cover files was shown, the main advantages of using pseudorandom sequences, as well as some dependences of the error rate in the restored messages and cover file distortions are shown. Subsequently, many techniques were finalized and improved. In particular, in [8], combined methods combining error correction, random positioning in pixels of a cover image, and direct-sequence spread spectrum (DSSS) spectrum expansion were investigated. In [9], concealment is implemented in the frequency domain, i.e. spreading modulation was applied to discrete cosine transform (DCT) coefficients. In [10], the implementation of the steganosystem was supplemented by several levels of security, including cryptographic transformations. In [11], aspects of the practical implementation of steganosystems when hiding information in audio files by the method of direct spectrum expansion are considered. In [12], steganoanalysis methods using video files and direct spectral expansion methods were studied. The work [13] is devoted to the use of steganographic security techniques for transmitting medical images and elec-

tronic medical records in teleradiology. Article [14] is devoted to a theoretical panalysis of the safety of steganosystems based on direct sequence spreading of the spectrum.

Thus, methods of direct expansion of the spectrum are used to conceal data in various multimedia files (images, video, audio, etc.). Moreover, transformations can be used both in the spatial domain [4-7] and in the field of orthogonal transformations, for example, in DCT [9]. At the same time, the main problem of using DSSS in steganography is the high level of errors in the restored messages.

3 Purpose and objectives of the article

The main goal of this work is to introduce a new technique for hiding informational messages in cover files using direct spectrum expansion and adaptively generated pseudorandom sequences. We propose a new approach consisting in the formation of noise-like sequences taking into account the statistical properties of cover files. The task is to ensure that each sequence does not correlate with the cover file used. This can significantly reduce the bit error rate in the extracted informational messages. Our experiments clearly confirm this.

The article is organized as follows. First, we briefly present the known information on the use of direct spectrum spreading technology in steganography (we use basic information from several articles and US patents), and also show that the practical failure to fulfill certain theoretical assumptions will lead to the guaranteed occurrence of errors in the restored information data. Our experiments on still images clearly demonstrate this, and the error rate remains very high even with amplification of the spreading signal and with a small number of hidden data. We also show examples of specific images of covers, as well as an assessment of their distortions at various parameters of the steganosystem. Finally, we propose a new technique for hiding information, which is based on the obligatory fulfillment of the theoretical assumption about the uncorrelatedness of extension sequences and cover files. The experiments presented in the article show that in practical implementation it is really possible to significantly reduce the bit error rate. Preliminary results were abridged at the conference [15].

4 Hiding data in images using direct spread spectrum technology

As a prototype of an improved method of hiding data in cover images, the technique proposed in the dissertation by L. Marvel was selected, described in detail and studied in [6, 7, 16, 17]. Let's consider it in more detail.

The method of concealing data using the direct spread spectrum, proposed in US patent [17], based on the fact that (on the transmission side after encryption and noise immunity coding) separate blocks $m_i = \left(m_{i_0}, m_{i_1}, ..., m_{i_{k-1}}\right)$, $i = 0, ..., N-1$ of data of

information message $m=(m_0,m_1,...,m_{N-1})$ the blocks are modulated by noise-like discrete signals with the help of appropriate devices $\Phi_i=(\phi_{i_0},\phi_{i_1},...,\phi_{i_{n-1}})$, $\Phi_i\in\Phi=\{\Phi_0,\Phi_1,...,\Phi_{M-1}\}$, $k\le M$, with a base $B=TF$, where T is the duration of the signal element ϕ_{i_j}, F is the frequency band of the signal Φ_i. Since $F=n\frac{1}{T}$ we have $B=n>>1$ and the signal base sets the frequency spread of the frequency band of signal Φ_i with respect to elementary signals ϕ_{i_j} and / or m_{i_j}. As a result, a modulated information signal block is generated for each m_i information block

$$E_i=\sum_{j=0}^{k-1} m^*_{i_j}\,\Phi_j\,, \tag{1}$$

where

$$m^*_{i_j}=\begin{cases}+1, m_{i_j}=1;\\ -1, m_{i_j}=0;\end{cases}$$

which, according to statistical properties, takes the form of a random (noise-like) sequence

$$E_i=\left(\sum_{j=0}^{k-1} m^*_{i_j}\,\phi_{j_0},\sum_{j=0}^{k-1} m^*_{i_j}\,\phi_{j_1},...,\sum_{j=0}^{k-1} m^*_{i_j}\,\phi_{j_{n-1}}\right),$$

and due to the large base of discrete signals, the frequency spectrum is spreaded by $B=n$ times.

The resulting modulated message E_i is supplied to an alternationing device on which the elements of E_i are mixed with the corresponding rule f by means of a secret key K_1. The obtained data $\overline{E_i}=f(E_i,K_1)$ з using the appropriate device is added to the data of the image C_i (digital image data in the spatial domain) according to the rule: $S_i=C_i+\overline{E_i}\cdot G$, where $G>0$ is the gain of the expansion signal, which sets the "power" of the hidden blocks of information messages.

The obtained data S_i is supplied to the quantization device, which performs a certain transformation to store the primary dynamic range of the cover image, resulting in the formation of separate blocks of the steganogram $\overline{S_i}$ and the cover $\overline{S}=\overline{S_0}\cup\overline{S_1}\cup...\cup\overline{S_{N-1}}$, which is transmitted to the receiving side.

On the receiving side, the resulting steganogram blocks $\overline{S_i}$ after filtration, are, supplied to a reverse interleaving device, on which the elements of the filtered blocks

of the stegogram $\overline{\overline{S_i}}$ are mixed by rule f^{-1}, which is an inverse rule of alternation f on the transmitting side. The extraction of blocks of information data is carried out using a correlation receiver, which calculates the value of the correlation coefficient obtained after the reverse alternation of data $S^*_i = f^{-1}(\overline{\overline{S_i}}, K_1)$ and corresponding discrete Φ_j, signals identical to those used on the transmitting side:

$$\rho\left(S^*_i, \Phi_j\right) = \frac{1}{n}\sum_{z=0}^{n-1} S^*_{i_z}\, \phi_{j_z}\ . \tag{2}$$

Since $S_i = C_i + \overline{E_i}\cdot G$ we have:

$$\frac{1}{n}\sum_{z=0}^{n-1} S^*_{i_z}\, \phi_{j_z} \approx G\cdot\frac{1}{n}\sum_{z=0}^{n-1} E_{i_z}\phi_{j_z} + \frac{1}{n}\sum_{z=0}^{n-1} C_{i_z}\phi_{j_z}$$

Suppose that the data block of the image block C_i has a random statistical structure, that is, suppose that the second term on the right side of expression (2) is close to zero and can be ignored. Then we have:

$$\rho\left(S^*_i, \Phi_j\right) \approx G\cdot\sum_{u=0}^{k-1} m^*_{i_u}\ \rho\left(\Phi_u, \Phi_j\right). \tag{3}$$

Since all sequences of the set Φ are formed by a pseudorandom sequence generator initiated by a secret key K_2, the corresponding discrete signals are weakly correlated, that is, at $u \neq j$ we have $\rho\left(\Phi_u, \Phi_j\right) \approx 0$.

According to this, all terms, except case $u = j$, in the right-hand side of equation (3) can be ignored. Where do we have:

$$\rho\left(S^*_i, \Phi_j\right) \approx G\cdot m^*_{i_j}\cdot\frac{1}{n}\sum_{z=0}^{n-1}\left(\phi_{j_z}\right)^2 = G\cdot m^*_{i_j} = \begin{cases} +G; \\ -G. \end{cases} \tag{4}$$

The corresponding value of the seized data is taken with a threshold device according to the calculated correlation coefficient.

Since $G > 0$ and $n > 0$ of $\rho\left(S^*_i, \Phi_j\right)$ character in (4) depends only on $m^*_{i_j}$, from where we have:

$$m^*_{i_j} = sign\left(\rho\left(S^*_i, \Phi_j\right)\right) = \begin{cases} -1,\ \rho\left(S_i, \Phi_j\right) < 0; \\ +1,\ \rho\left(S_i, \Phi_j\right) > 0. \end{cases} \tag{5}$$

If $\rho\left(S^*_i, \Phi_j\right) = 0$ in (5) we will assume that the hidden information has been lost (erased). Separate blocks of data are formed from the extracted data on the receiving side $m_i = \left(m_{i_0}, m_{i_1}, ..., m_{i_{k-1}}\right)$, $i = 0, ..., N-1$ of information messages $m = \left(m_0, m_1, ..., m_{N-1}\right)$, where $m_{i_j} = \begin{cases} 1, m^*_{i_j} = +1; \\ 0, m^*_{i_j} = -1; \end{cases}$ of which information messages are generated after noise immunity decoding and decryption of the extracted data.

The secret key K_2 sets the rule for the formation of pseudorandom sequences $\Phi_i = \left(\phi_{i_0}, \phi_{i_1}, ..., \phi_{i_{n-1}}\right)$, which are formed by the corresponding generator and are used as noise-like discrete signals $\Phi_i \in \Phi = \left\{\Phi_0, \Phi_1, ..., \Phi_{M-1}\right\}$ from the ensemble (set) Φ of power M.

The encryption and decryption rule on the transmitting and receiving side is initiated by the secret key K_3.

The use of encryption and alternation devices in the process of hiding and retrieving data can improve the statistical properties of the modulated message E_i, ie to bring it closer to a random sequence. The use of noise immunity coding devices can improve the reliability of the transmission of information messages $m = \left(m_0, m_1, ..., m_{N-1}\right)$ during steganographic conversions.

5 Experimental researches

The disadvantage of the prototype under consideration is that in the process of steganographic hiding, the statistical properties of the blocks of the image C_i, are not taken into account, that is, the digital image data can be correlated with the applied discrete signals, which will lead to an error when extracting information data on the receiving side.

So, for example, if the correlation coefficient of the i-th block C_i of the image will be higher behind the module and opposite in value of sign $G \cdot m^*_{i_j}$, that is, when the second summand in the right part of expression (2) will be higher in module and opposite in value of sign of the first summand (and the condition of mutual orthogonality of applied discrete signals will be fulfilled), it is guaranteed that an error will the result at data extract according to rule (5). In practice, as our researches have shown, such cases occur very often. This is due to the fact that the digital data of real images used to hide information messages do not have a random statistical structure, that is, the applied assumption in the transition from formula (2) to formula (3) is not fulfilled in practice and is false. Typically, steganographic hiding uses realistic images and the corresponding digital data is not a random process, and even in its statistical properties are not similar to pseudorandom sequences. The

corresponding values of the correlation coefficient $\rho\left(C_i,\Phi_j\right)=\frac{1}{n}\sum_{z=0}^{n-1}C_{i_z}\phi_{j_z}\neq 0$, and can take large amplitude ($\left|\rho\left(C_i,\Phi_j\right)\right|>>1$) and random values. In this case, it is possible to increase the reliability of the extracted data only by applying low-speed noise immunity codes (as in the prototype discussed above [6, 7, 16, 17]), which leads to a decrease in the relative transmission rate of information, or an increase in the gain G, which leads to an increase in the introduced errors.

To confirm this fact, Fig. 1 shows the empirical estimates of BER dependence in message recovery using the considered prototype method (interrupted line). The $G=4$ gain was applied, and the number of bits k, hidden in one block C_i of the cover image varied from 1 to 255. Fig. 2. shows empirical estimations of dependence of the average proportion of introduced errors (in relation to the dynamic range of 256 levels) in the cover image with respect to the number of bits embedded in one element of the cover. From the given dependencies (Fig. 1, 2, interrupted line) it is visible, that at entering errors in the cover image below a visual threshold of human sensitivity (2-3%) it is possible to hide no more than 10 bits of data in one block of the image C_i. But even with such an insignificant amount of hidden data, BER takes the value 0.05..0.25, which requires the use of low-speed noise immunity codes with the permission to correct multiple errors.

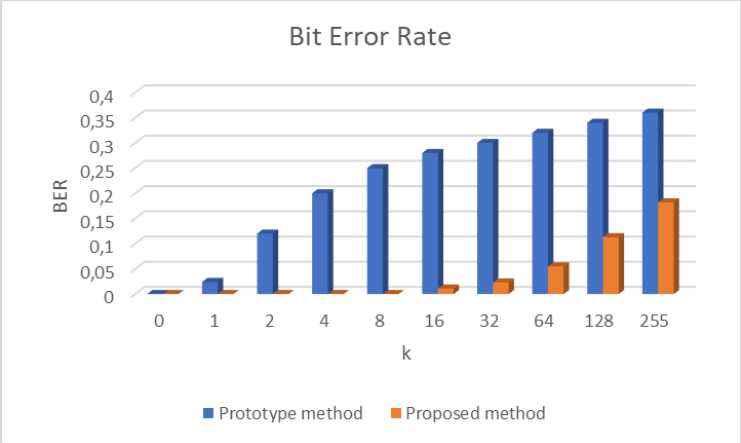

Fig. 1. Bit error rate in recovered messages depending on message size

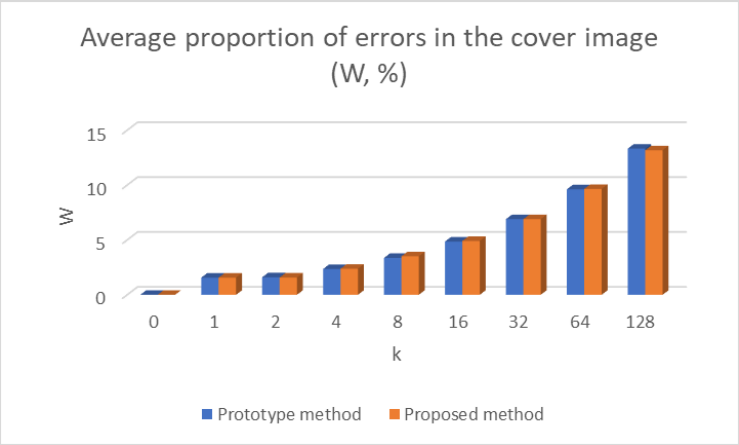

Fig. 2. The proportion of distortion introduced into the cover image depending on the size of the message

In Fig. 3, 4 show, accordingly, the obtained empirical estimates of the BER dependence when restoring the messages and the dependence of the average fraction of the input errors on the G gain values using the considered prototype method (intermittent lines). At the same time, $k = 4$ bits of information data were embedded in one block C_i of the cover, and the gain G changed from 1 to 8. From the given dependencies (Fig. 3, 4, interrupted line) it is visible, that at value of gain $G > 6$ hiding of the information data leads to entering of errors, part of which (relative to a dynamic range) is above a visual threshold of human sensitivity (2-3 %). That is, the fact of hiding data in the image turns out to be a visual observation and steganographic hiding with these parameters is not reasonable But at $G \le 6$ gain value, there is a large number of errors when extracting individual data bits from the spatial area of the image corresponding to $BER \ge 0,2$.

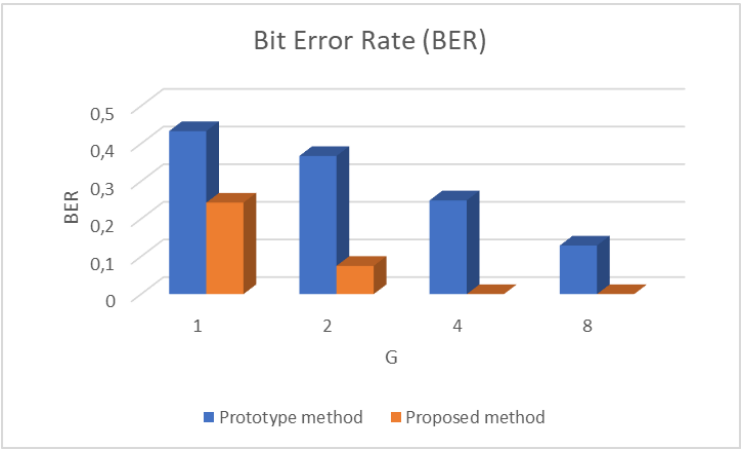

Fig. 3. Rate of bit errors in recovered messages depending on the gain factor

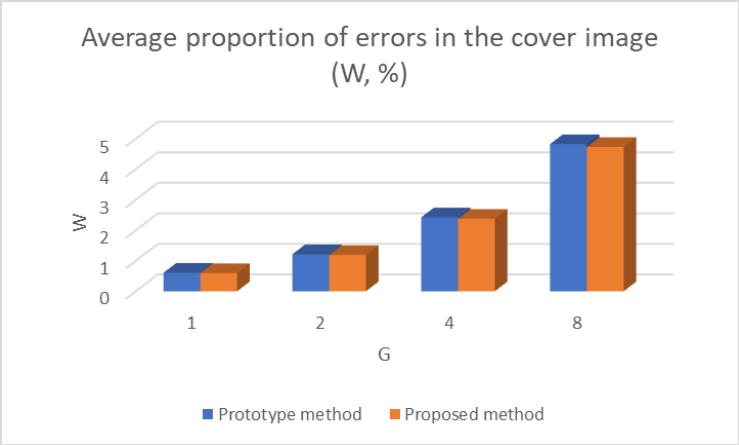

Fig. 4. The proportion of introduced distortion in the cover image depending on the gain factor

In Fig. 5-7 shows examples of images used in research:

- Fig. 5 – original image;
- Fig. 6 – image with hidden messages using prototype method;
- Fig. 7 – image with hidden messages using the proposed method.

Data hiding is done with the following parameters: $G = 4$, $k = 4$.

Fig. 5. Original image

Fig. 6. Example of cover image (using prototype method)

Fig. 7. Example of cover image (using the proposed method)

6 Proposed data hiding technique

Our task is based on the following: by taking into account the statistical properties of cover C_i, significantly reduce the BER of hidden data. Indeed, the introduction of additional constraints on the correlation coefficient of the discrete signals used and

individual fragments of the image can significantly reduce the number of errors when recovering the message on the receiving side.

This problem is solved due to the special (we call adaptive) formation of pseudorandom sequences $\Phi_j = \left(\phi_{j_0}, \phi_{j_1}, ..., \phi_{j_{n-1}}\right)$, taking into account the statistical properties of these blocks of cover C_i. That is, the value of the correlation coefficient $\rho\left(C_i, \Phi_j\right)$ for all $i = 0,..,N-1$ and for all $j = 0,..,M-1$ by the module should not exceed some predetermined value $\rho_{\max}$ (value of the set threshold):

$$\left|\rho\left(C_i, \Phi_j\right)\right| = \left|\frac{1}{n}\sum_{z=0}^{n-1} C_{i_z}\phi_{j_z}\right| \le \rho_{\max}. \quad (6)$$

Thus, the formation of $\Phi_j \in \Phi = \left\{\Phi_0, \Phi_1, ..., \Phi_{M-1}\right\}$ sequences is performed by a pseudo-random rule, which is initiated by the secret key K_2, and taking into account conditions (6) for all $i = 0,..,N-1$ and all $j = 0,..,M-1$.

In this formation of discrete signals, each sequence of the set of $\Phi = \left\{\Phi_0, \Phi_1, ..., \Phi_{M-1}\right\}$ will not be correlated (up to the set limit) with any block of the cover image, and, accordingly, the correlation coefficient of the i-th block C_i of the cover on the module will never be higher than the module and the opposite in sign $\rho_{\max}$. In accordance with this (and when the conditions of mutual orthogonality of the applied discrete signals) the second term in the right part of expression (2) may exceed in module and be opposite in sign to the first term only when $\left|G \cdot m^*_{i_j}\right| < \rho_{\max}$. It is in this case that an error of data extraction will happen, but the probability of such an event will be much less than in case of an error of data extraction in the prototype method. If the value of the $\rho_{\max}$ threshold is lower than the G gain value, i.e. when the unequal is performed $\left|G \cdot m^*_{i_j}\right| > \rho_{\max}$ the error will not occur at all, i.e. an unmistakable transfer of secret information will be achieved.

In Figs. 1-6, solid lines show empirical estimates of the probability properties of steganographic concealment using the proposed method, which confirms our conclusion:

- in Fig. 1 shows the bit error rate in the recovered messages depending on the size of the message;
- in Fig. 2 shows the proportion of distortion introduced into the cover image depending on the size of the message;
- in Fig. 3 shows bit error rate in the recovered messages depending on the gain factor;
- in Fig. 4 shows the proportion of distortion introduced into the cover image depending on the gain factor.

7 Discussion of the results

From the above dependencies in Fig. 1, 2 (solid line) shows that when making errors in the cover image lower than the visual threshold of human sensitivity (2-3%) manages to embed no more than 10 bits of data in one block of the C coniner (as in the prototype method). But with so a number of hidden data, the BER value is much less than 0.1 and several dozen times less than in the prototype method.

From the given dependencies in the fig. 3, 4 (solid line) can be seen that at the value of gain hiding information data in the cover image leads to the introduction of errors whose fate (in relation to the dynamic range) is higher than the visual threshold of human sensitivity (2-3%) as well as in the method prototype. At $G \le 6$ values, the errors introduced into the cover image are lower than the human visual sensitivity threshold, i.e. they are invisible. In compared with the method-prototype, there is a significant reduction in the number of errors when extracting individual data bits from the spatial area of the image. In addition, at the H gain value, there is a total non occurrence of errors in remote data, which confirms the above conclusion about the error-free transmission of hidden information. Indeed, if $G = 4$ then the inequality is being realized $\left| G \cdot m^*_{i_j} \right| > \rho_{\max}$, that is, assuming the validity of the mutual orthogonality of the applied discrete error signals, no errors occur at all and an error-free transmission of hidden information is achieved.

From the given dependencies in the fig. 5, 6 (solid line) shows that in almost all cases, when hiding data the proposed method is a gain in relation to the method-prototype (interrupted line). Thus, when the number of k bits hidden in one element of the cover image increases, as well as in the prototype method, there is an increase in the probability of false data extracted on the receiving side. However, this increase is much slower than in the prototype method. As the G gain increases, the probability of false data extraction decreases, but the proposed method (solid line) has significantly improved probabilistic properties than the prototype method (interrupted line).

8 Conclusions

Spread spectrum technologies are traditionally used in multiple access radio communication systems. Direct-sequence modulation makes the transmitted signal wider in bandwidth than the information signal. The resulting transmitted signal resembles white noise limited in bandwidth. This noiselike signal is used to accurately restore the source data on the host side by multiplying it by the same expansion sequence. This process is mathematically a correlation, i.e. on the receiving side the recovery of information data is performed by calculating the correlation coefficient of the accepted sequence and the spreading sequence.

Application of the technology of direct spread-spectrum in radio communication systems allows obtaining specific advantages: resistance to jamming (interference); resistance to eavesdropping; resistance to fading; multiple access capabilities. Some

radiocommunication industry standards take advantage of these advantages. However, this technology can also be successfully applied in steganography. Excess data (images, audio and video files, text documents, etc.) are interpreted as noise in a communication channel. The task is to hide information data in such a way that redundant data (cover files) are not distorted, i.e., photo or video images are visually indistinguishable from the original data. The technology of direct spread-spectrum is suitable for this very well.

The main theoretical assumption that explains the operation of this technology is the uncorrelation of the spreading sequence and noise in the communication channel. In radio communications systems with white noise, this assumption is fulfilled and there are few errors on the receiving side. In steganographic systems, however, this assumption may not work. Noise is understood here to be excess digital data, for example, it can be realistic images. And such cover files can strongly correlate with the spreading sequence. As a result of the correlation reception, a large number of errors occur when restoring information messages. We offer an effective way to reduce such errors. In fact, we offer a new way to form spreading sequences that takes into account the statistical properties of cover files. We call this method adaptive. As a result, we have a set of spreading sequences that do not correlate with cover files and almost no errors occur when restoring information messages. Experiments show that this is indeed the case. Our approach is much more efficient. Thus, a specific technical result is achieved, namely: by taking into account the statistical properties of the digital data of the cover images (in the adaptive formation of pseudorandom sequences) it is possible to significantly reduce the number of errors in the recovery of information data on the receiving side.

A promising trend is to study the properties of steganosystems using complex discrete signals with special correlation properties. For example, we want to use sequences from our previous work [18-19] to hide information in cover images.

References

1. Torrieri, D.: Principles of Spread-Spectrum Communication Systems. Springer International Publishing (2018)
2. Yang, S.-M.M.: Modern Digital Radio Communication Signals and Systems. Springer International Publishing (2019)
3. CDMA. TelecomSpace, (2020). http://www.telecomspace.com/cdma.html
4. A. Z. Tirkel, C. F. Osborne and R. G. Van Schyndel, "Image watermarking-a spread spectrum application," Proceedings of ISSSTA'95 International Symposium on Spread Spectrum Techniques and Applications, Mainz, Germany, 1996, pp. 785-789 vol.2. doi: 10.1109/ISSSTA.1996.563231.
5. J. R. Smith and B. O. Comiskey, “Modulation and information hiding in images,” Lecture Notes in Computer Science, pp. 207–226, 1996. doi:10.1007/3-540-61996-8_42.
6. L. M. Marvel, C. G. Boncelet, R. Jr., and Charles T., “Methodology of Spread-Spectrum Image Steganography,” Jun. 1998. doi:10.21236/ada349102.
7. L. M. Marvel, C. G. Boncelet and C. T. Retter, "Spread spectrum image steganography," in IEEE Transactions on Image Processing, vol. 8, no. 8, pp. 1075-1083, Aug. 1999. doi: 10.1109/83.777088.

8. 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: Security and Identification 2008 2nd International Conference on Anti-counterfeiting. pp. 245–248 (2008)
9. Agrawal, N., Gupta, A.: DCT Domain Message Embedding in Spread-Spectrum Steganography System. In: 2009 Data Compression Conference. pp. 433–433 (2009)
10. 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. pp. 1–6 (2011)
11. Yadav, P., Dutta, M.: 3-Level security based spread spectrum image steganography with enhanced peak signal to noise ratio. In: 2017 Fourth International Conference on Image Information Processing (ICIIP). pp. 1–5 (2017)
12. Zarmehi, N., Akhaee, M.A.: Video steganalysis of multiplicative spread spectrum steganography. In: 2014 22nd European Signal Processing Conference (EUSIPCO). pp. 2440–2444 (2014)
13. Eze, P.U., Parampalli, U., Evans, R.J., Liu, D.: Spread Spectrum Steganographic Capacity Improvement for Medical Image Security in Teleradiology*. In: 2018 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC). pp. 1–4 (2018)
14. 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 Transactions on Cybernetics. 48, 2307–2320 (2018). https://doi.org/10.1109/TCYB.2017.2735989
15. Kuznetsov, A., Smirnov, O., Onikiychuk, A., Makushenko, T., Anisimova, O., Arischenko, A.: Adaptive Pseudo-Random Sequence Generation for Spread Spectrum Image Steganography. In: 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT). pp. 161–165 (2020)
16. F. S. Brundick and L. M. Marvel, “Implementation of Spread Spectrum Image Steganography,” Mar. 2001. doi:10.21236/ada392155.
17. Patent No.: US 6,557,103 B1, Int.Cl. G06F 11/30. Charles G. Boncelet, Jr., Lisa M. Marvel, Charles T. Retter. Spread Spectrum Image Steganography. Patent No.: US 6,557,103 B1, Int.Cl. G06F 11/30. – № 09/257,136; Filed Feb. 11, 1999; Date of Patent Apr. 29, 2003
18. A. Kuznetsov, S. Kavun, V. Panchenko, D. Prokopovych-Tkachenko, F. Kurinniy and V. Shoiko, "Periodic Properties of Cryptographically Strong Pseudorandom Sequences," 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2018, pp. 129-134. doi: 10.1109/INFOCOMMST.2018.8632021
19. A. Kuznetsov, O. Smirnov, D. Kovalchuk, A. Averchev, M. Pastukhov and K. Kuznetsova, "Formation of Pseudorandom Sequences with Special Correlation Properties," 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), Lviv, Ukraine, 2019, pp. 395-399. doi: 10.1109/AIACT.2019.8847861