New Technique for Data Hiding in Cover Images 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][0000-0001-6154-7139]

[1] V. N. Karazin Kharkiv National University, Kharkiv, Ukraine
kuznetsov@karazin.ua, dianakovalhyk@ukr.net,
kuznetsova.tatiana17@gmail.com
[2] Central Ukrainian National Technical University, Kropivnitskiy, Ukraine,
dr.smirnovoa@gmail.com

Abstract. The technology of direct spectrum spread is used in radio communication systems with multiple access. It is based on the use of pseudorandom (noise-like) discrete signals (sequences). In this paper steganography techniques based on spectrum spread are studied. Using noise-like signals, it is possible to hide information in cover images. We conduct experimental studies and show that the error rate in the restored informational messages is very high. This is due to the high correlation of discrete sequences and cover images. We offer a new technique when the statistical properties of cover images are taken into account when forming sequences. Our experiments show that the practical use of this approach can significantly reduce the error rate. The distortion of the image does not increase.

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

1 Introduction

The use of direct spectrum spread technology makes it possible to significantly improve the efficiency of multiple access radio communication systems [1-5]. In particular, the use of weakly correlated pseudorandom sequences (discrete signals) provides high noise immunity and mimic resistance of communication systems; to reduce the cost of communication, etc.

In [6-15], techniques for hiding data in digital images using direct spectrum spreading technology were studied. In this case, the cover image is interpreted as noise in the communication channel. As shown in [16-21], this allows one to hide informational communications using long pseudorandom sequences. At the same time, as shown in this paper, certain disadvantages are inherent in known techniques. In particular, we present the results of experimental studies and show that the bit error rate (BER) in the extracted messages is very high. This is due to the correlation of the applied spreading spectrum pseudorandom sequences and the cover image (or its

CybHyg-2019: International Workshop on Cyber Hygiene, Kyiv, Ukraine, November 30, 2019.

fragment). In this paper, we propose a new technique for hiding data based on specially formed pseudorandom sequences. When generating discrete signals, we take into account the statistical properties of the cover image (we call this method of generation adaptive). This can significantly reduce the BER in the extracted messages. We also show that cover images are not distorted significantly, both of the considered techniques are almost equivalent in this indicator.

2 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 [11, 12, 14, 15]. Let's consider it in more detail.

The method of concealing data using the direct spread spectrum, proposed in US patent [15], 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

$$m = \left(m_0, m_1, ..., m_{N-1}\right)$$

the blocks are modulated by noise-like discrete signals with the help of appropriate devices

$$\Phi_i = \left(\phi_{i_0}, \phi_{i_1}, ..., \phi_{i_{n-1}}\right),\ \Phi_i \in \Phi = \left\{\Phi_0, \Phi_1, ..., \Phi_{M-1}\right\},\ k \le M\ ,$$

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

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

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, 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 transmitting side:

$$\rho\left(S*_i, \Phi_j\right) = \frac{1}{n}\sum_{z=0}^{n-1} S*_{i_z}\,\phi_{j_z} \approx G \cdot \frac{1}{n}\sum_{z=0}^{n-1} E_{i_z}\phi_{j_z} + \frac{1}{n}\sum_{z=0}^{n-1} C_{i_z}\phi_{j_z}\ . \qquad (2)$$

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::

$$\rho\left(S*_i,\Phi_j\right)\approx G\cdot\frac{1}{n}\sum_{z=0}^{n-1}E_{i_z}\phi_{j_z}=G\cdot\frac{1}{n}\sum_{z=0}^{n-1}\left(\sum_{u=0}^{k-1}m*_{i_u}\ \phi_{u_z}\right)\phi_{j_z}=$$
$$=G\cdot\sum_{u=0}^{k-1}m*_{i_u}\ \sum_{z=0}^{n-1}\phi_{u_z}\phi_{j_z}=G\cdot\sum_{u=0}^{k-1}m*_{i_u}\ \rho\left(\Phi_u,\Phi_j\right). \qquad (3)$$

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:

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

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:

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

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 $m = (m_0, m_1, ..., m_{N-1})$ during steganographic conversions.

3 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 [11, 12, 14, 15]), 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.

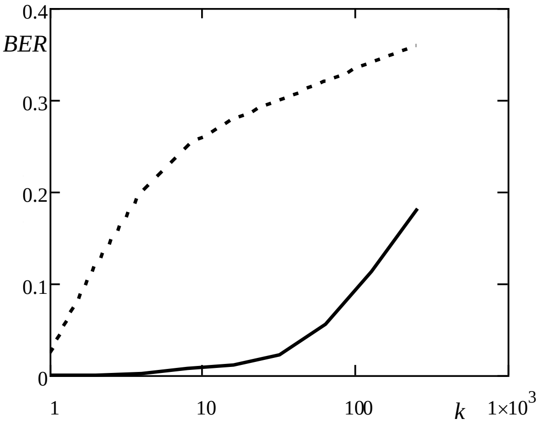


Fig. 1. *BER (k)* dependency

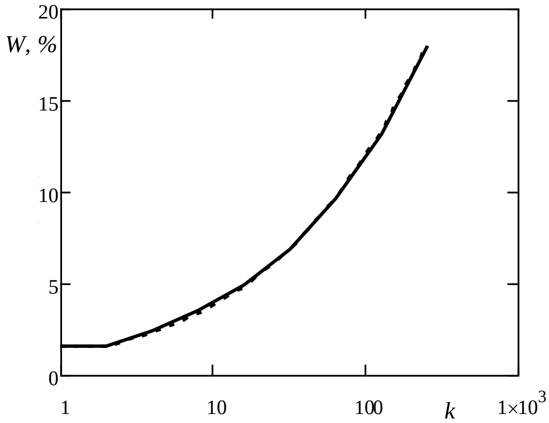


Fig. 2. *W(k)* dependency

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 $G \leq 6$ gain value, there is a large number of errors when extracting individual data bits from the spatial area of the image corresponding to $BER \geq 0,2$.

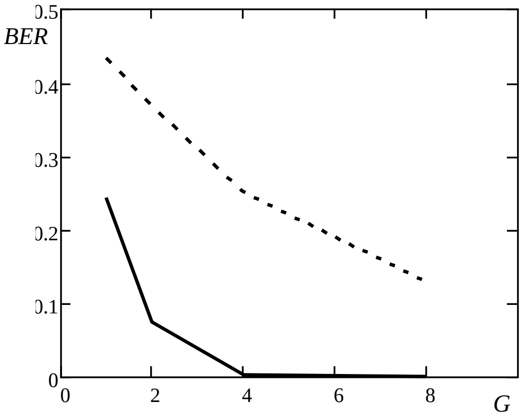


Fig. 3. *BER (G)* dependency

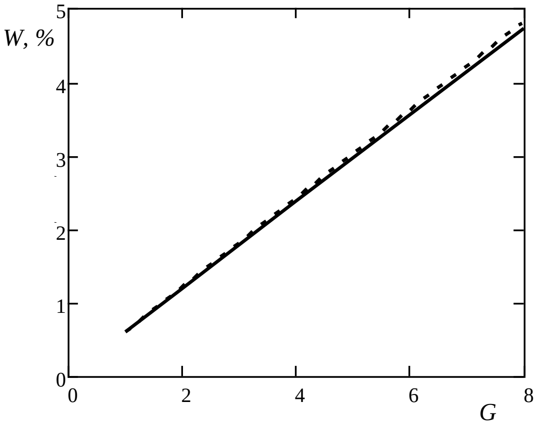


Fig. 4. *W(G)* dependency

Empirical estimates of the dependence of the probability of false recovery of individual bits of data on the average fraction of errors made in the cover image when changing the number of bits hidden in one element of the cover (from 1 to 255) or changing the value of the expansion signal gain (from 1 to 8) are shown in accordance with Fig. 5, 6. In the first case (Fig. 5) the dependencies are built according to the fixed $G = 4$, gain value, in the second case (Fig. 6) - according to the fixed value $k = 4$.

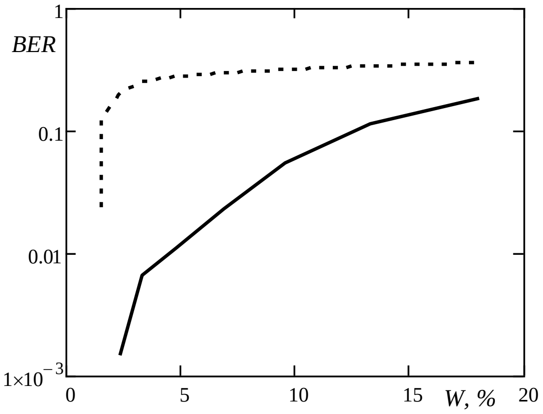


Fig. 5. *BER (W), k = 1, 2, ..., 255*

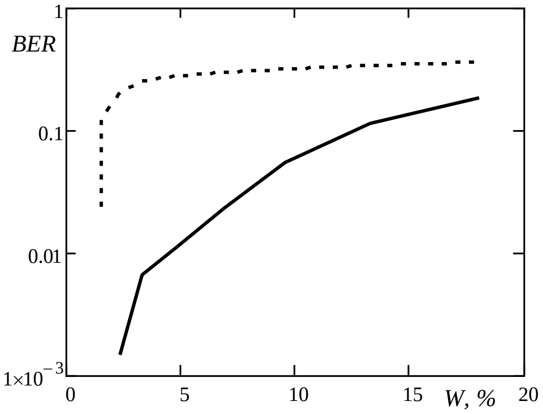


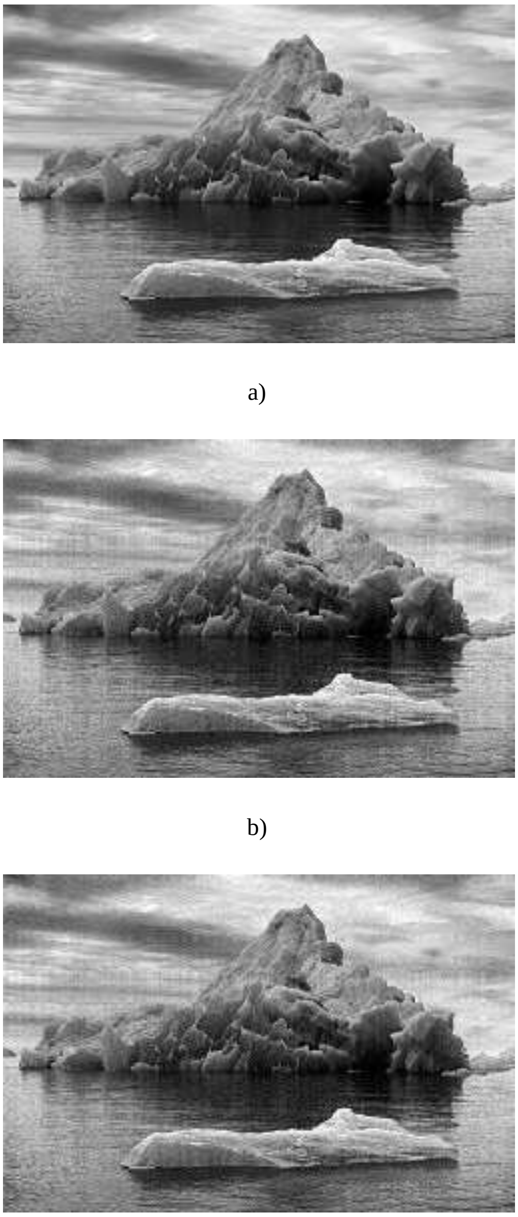
Fig. 6. *BER (W), G = 1, 2, ..., 8*

From the given dependences (interrupted line) it is visible, that practically in all cases at data embedding by means of a method-prototype there is a considerable quantity of errors at data recovery from images. Even with small values, the probability of mistaken deletion is 0,05..0,25 (see Fig.6).

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

- Fig. 7.a. – original image (empty cover);
- Fig. 7.b. – image with hidden messages using prototype method (filled cover);
- Fig. 7.c. – image with hidden messages using the proposed method (filled cover).

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



a)

b)

c)

Fig. 7. Examples of cover images

4 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):

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

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.

To confirm the conclusion in Fig. 1-6, the solid line shows empirical estimates of the probabilistic properties of steganographic hiding using the proposed method:

- Fig. 1 shows empirical estimates of dependence *BER (k)*;
- Fig. 2 shows empirical estimates of dependence *W(k)*;
- Fig. 3 shows empirical estimates of dependence *BER (G)*;
- Fig. 4 shows empirical estimates of dependence *W(G)*;
- Fig. 5 shows empirical estimates of *BER (W)* at $k = 1,...,255$ and at a fixed gain $G = 4$;
- Fig. 6 shows empirical estimates of *BER (W),* at $G = 1,...,8$ and $k = 4$.

The dependencies shown in Figs. 1-6 (solid line) are obtained using adapted (statistical properties of the cover) discrete signals formation, the value of the set threshold is equal to $\rho_{\max} = 3{,}9$.

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).

5 Conclusions

The use of direct spectrum spread technology is an interesting and hugely promising area of modern steganography. Indeed, if you use advanced mathematical apparatus and digital communication techniques, in particular pseudorandom (noise-like) discrete signals, you can get a safe and secure way to hide information messages in different cover images. We have looked at a number of technologies that are based on direct spectrum spread technology to hide information in images

Our research has shown that in addition to the traditional requirements of digital communication, steganographic applications should also take into account the specifics of the cover images used. In particular, images interpreted as noise in communication channels cannot be considered as implementation of random process. Because there are correlations between individual pixels of the image. Therefore, the use of pseudorandom sequences (extension signals) without taking into account the statistical properties of cover images can lead to a significant number of hidden data errors.

We have introduced a new data hiding technique with the use of direct spectrum spread technology. In particular, our approach is based on the special formation of discrete signals, that is, taking into account the statistical properties of cover images. We call this metod adaptive. Indeed, in this case, the extension signals applied are not correlate with the image, and the number of hidden data errors can be significantly reduced.

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 [22-26] to hide information in cover images.

The results can be used in various computer science applications. In particular, for modernization of various cryptographic algorithms, optimization of calculations, modeling and telecommunications [27-33].

References

1. V. P. Ipatov, “Spread Spectrum and CDMA”, Mar. 2005. DOI:10.1002/0470091800.
2. “Introduction to CDMA Wireless Communications,” 2007. DOI:10.1016/b978-0-7506-5252-0.x5001-7.
3. “The Generalized CDMA,” CDMA: Access and Switching, pp. 1–28. DOI:10.1002/0470841699.
4. S. Hara and R. Prasad, “DS-CDMA, MC-CDMA and MT-CDMA for mobile multi-media communications”, Proceedings of Vehicular Technology Conference - VTC, Atlanta, GA, USA, 1996, pp. 1106-1110 vol.2, DOI: 10.1109/VETEC.1996.501483.
5. “Digital Watermarking and Steganography”, 2008. DOI:10.1016/b978-0-12-372585-1.x5001-3.

6. F.Y. Shin, “Digital Watermarking and Steganography,” Dec. 2017. DOI:10.1201/ 9781315219783.
7. N. F. Johnson and S. Jajodia, “Exploring steganography: Seeing the unseen”, in Computer, vol. 31, no. 2, pp. 26-34, Feb. 1998. DOI: 10.1109/MC.1998.4655281.
8. I.V. S. Manoj, “Cryptography and Steganography,” International Journal of Computer Applications, vol. 1, no. 12, pp. 63–68, Feb. 2010. DOI:10.5120/257-414.
9. 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.
10. 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.
11. L.M. Marvel, C. G. Boncelet, R. Jr., and Charles T., “Methodology of Spread-Spectrum Image Steganography,” Jun. 1998. doi:10.21236/ada349102.
12. 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.
13. M. Kutter, “Performance Improvement of Spread Spectrum Based Image Watermarking Schemes through M-ary Modulation,” Lecture Notes in Computer Science, pp. 237–252, 2000. DOI:10.1007/10719724_17.
14. F.S. Brundick and L. M. Marvel, “Implementation of Spread Spectrum Image Steganography,” Mar. 2001. DOI:10.21236/ada392155.
15. 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.
16. Fan Zhang, Bin Xu and Xinhong Zhang, “Digital image watermarking algorithm based on CDMA spread spectrum”, 2006 12th International Multi-Media Modelling Conference, Beijing, 2006, pp. 4, DOI: 10.1109/MMMC.2006.1651359.
17. T. T. Nguyen and D. Taubman, “Optimal linear detector for spread spectrum based multidimensional signal watermarking”, 2009 16th IEEE International Conference on Image Processing (ICIP), Cairo, 2009, pp. 113-116. DOI: 10.1109/ICIP.2009.5414121.
18. E. Nezhadarya, Z. J. Wang and R. K. Ward, “Image quality monitoring using spread spectrum watermarking”, 2009 16th IEEE International Conference on Image Processing (ICIP), Cairo, 2009, pp. 2233-2236. DOI: 10.1109/ICIP.2009.5413955.
19. S. Ghosh, P. Ray, S. P. Maity and H. Rahaman, “Spread Spectrum Image Watermarking with Digital Design”, 2009 IEEE International Advance Computing Conference, Patiala, 2009, pp. 868-873. DOI: 10.1109/IADCC.2009.4809129.
20. H.O. Altun, A. Orsdemir, G. Sharma and M. F. Bocko, “Optimal Spread Spectrum Watermark Embedding via a Multistep Feasibility Formulation”, in IEEE Transactions on Image Processing, vol. 18, no. 2, pp. 371-387, Feb. 2009. doi: 10.1109/TIP.2008.2008222.
21. A. Samčović and M. Milovanović, “Robust digital image watermarking based on wavelet transform and spread spectrum techniques”, 2015 23rd Telecommunications Forum Telfor (TELFOR), Belgrade, 2015, pp. 811-814, DOI: 10.1109/TELFOR.2015.7377589.
22. Yu.V. Stasev, A.A. Kuznetsov, A.M. Nosik. “Formation of pseudorandom sequences with improved autocorrelation properties” Cybernetics and Systems Analysis, vol. 43, Issue 1, pp. 1-11, January 2007. DOI: 10.1007/s10559-007-0021-2

23. N.I.Naumenko, Yu.V.Stasev, A.A.Kuznetsov. “Methods of synthesis of signals with prescribed properties”, Cybernetics and Systems Analysis, vol. 43, Issue 3, pp. 321-326, May 2007. DOI: 10.1007/s10559-007-0052-8
24. O.Karpenko, A.Kuznetsov, V.Sai, Yu.Stasev. “Discrete Signals with Multi-Level Correlation Function.” Telecommunications and Radio Engineering, vol. 71, 2012 Issue 1. pp 91-98. DOI: 10.1615/TelecomRadEng.v71.i1.100
25. 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
26. 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
27. Chornei, R., Hans Daduna, V. M., & Knopov, P. (2005). “Controlled markov fields with finite state space on graphs. Stochastic Models”, 21(4), 847-874. DOI:10.1080/15326340500294520
28. Runovski, K., & Schmeisser, H. (2004). “On the convergence of fourier means and interpolation means”. Journal of Computational Analysis and Applications, 6(3), 211-227.
29. Bondarenko, S., Liliya, B., Oksana, K., & Inna, G. (2019). “Modelling instruments in risk management. International Journal of Civil Engineering and Technology”, 10(1), 1561-1568.
30. S. Gnatyuk, T. Zhmurko, P. Falat, “Efficiency Increasing Method for Quantum Secure Direct Communication Protocols”, Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS’2015), Warsaw, Poland, September 24-26, Vol. 1, 2015, pp. 468-472.
31. Tkach B. P., & Urmancheva L. B. (2009). “Numerical-analytic method for finding solutions of systems with distributed parameters and integral condition”. Nonlinear Oscillations, 12(1), 113-122. DOI:10.1007/s11072-009-0064-6.
32. S. Gnatyuk, V. Kinzeryavyy, M. Iavich, D. Prysiazhnyi, Kh. Yubuzova, “High-Performance Reliable Block Encryption Algorithms Secured against Linear and Differential Cryptanalytic Attacks”, CEUR Workshop Proceedings, Vol. 2104, pp. 657-668, 2018.
33. Hu Z., Gnatyuk S., Kovtun M., Seilova N. “Method of searching birationally equivalent Edwards curves over binary fields”, Advances in Intelligent Systems and Computing, Vol. 754, pp. 309-319, 2019.