Data Hiding Scheme Based on Spread Sequence Addressing

Alexandr Kuznetsov [1[0000-0003-2331-6326]], Anastasiia Kiian [1[0000-0003-2110-010X]], Kateryna Kuznetsova [1[0000-0002-5605-9293]] and Oleksii Smirnov [2[0000-0001-9543-874X]]

[1]V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkiv, 61022, Ukraine,
[2]Central Ukrainian National Technical University, avenue University, 8, Kropivnitskiy, 25006, Ukraine

kuznetsov@karazin.ua, nastyak931@gmail.com,
kate.kuznetsova.2000@gmail.com, dr.smirnovoa@gmail.com

Abstract. Modern information technologies are constantly being evolved. On the one hand, this leads to the qualitative improvement in the services provided. On the other hand, this fact leads to the emergence of new threats to information security. In particular, new technologies for hiding data carry additional risks of computer security, for example, through the possible introduction of malicious computer programs. This article discusses the techniques for hiding data in cover images using direct spread spectrum. We propose a new technique that implies directly addressing to the propagation sequence. On the one hand, it significantly reduces cover file distortion. But on the other hand, the error rate in recovered messages does not increase. Our experiments have shown, that Spread Spectrum Steganography technique indeed reduce the distortion in cover images compared to other techniques. We give some illustrative examples and show the advantages of the proposed method. Even with a significant increase in encoding density, the quality of cover images does not degrade. We also conduct experiments and evaluate image quality based on Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). The obtained results of experimental studies confirm the adequacy and reliability of the research results. The main disadvantage of the proposed data hiding technique is the high computational complexity. To recover messages, it is necessary to sequentially calculate the correlation coefficients with a large number of pseudo-random sequences.

Keywords: Steganographic Spread Spectrum, Data Hiding, Cover Images, Direct Spread Spectrum, Pseudo-Random Sequence.

1 Introduction

There are various computing techniques (methods) [1–4] to transmit secret messages. For example, cryptographic techniques hide the semantic content of transmitted messages, presenting them in the form of noise-like minor data [1, 5]. Steganographic techniques hide the existence of information messages itself [3, 6]. In this case, mes-

sages are hidden inside cover files - redundant data that are transmitted in an open way and do not cause suspicion in anyone [2, 3]. An outside observer can intercept cover files, analyze and examine them. However, it is very difficult or even impossible to detect and recover hidden data.

Today steganographic methods are very well developed. The literature describes various ways of hiding information messages in redundant cover files [7–10]: in images, sound, text documents, videos, etc. The most common examples are described for cover images. In this case, various computing techniques are used.

The most promising direction in data hiding is Spread Spectrum Steganography [6, 11–14]. These techniques use the advances in sophisticated discrete signal theory to provide broadband and high-speed digital communications. For example, modern 4G and 5G mobile communication systems use broadband signals (specially formed pseudo-random sequences), providing high noise immunity, safety and environmental friendliness of communication [15–17]. These positive properties can also be used to hide data inside cover files, for example, in images [18–24].

It should be noted that the introduction of new technologies for hiding data creates additional risks of computer security, for example, through the possible introduction of malicious computer programs. In this sense, the development and research of modern data hiding techniques is especially relevant, including in the context of ensuring the cybersecurity of critical information systems.

This paper discusses the techniques for hiding data in cover images using direct spread spectrum. We show that some of the basic assumptions and hypotheses adopted for broadband high-speed digital communications may not be met when data is hidden within cover files. This leads to negative effects:

- cover files are heavily distorted;
- error rate in the recovered messages is very high.

We propose a new technique that implies directly address the propagation sequence. It significantly reduces cover file distortion. At the same time, the error rate in recovered messages does not increase. We give the illustrative examples and show the advantages of the proposed method. We also conduct experiments and evaluate image quality based on MSE and PSNR.

2 Related Works

The first works on Spread Spectrum Steganographic introduced basic concepts and definitions, and also showed the fundamental possibility of hiding data in cover files using complex discrete signals and direct spread spectrum [18–20, 25]. At the same time, the considered techniques have certain disadvantages:

- The bit error rate (BER) in recovered messages is very high. For example, in [18] it is shown (table 2, p. 12) that in most cases the BER takes values of 15% -30%. Even with very high "energy" of the latent message, the BER cannot be reduced below 10%;

- The distortion of cover images is very high. For example, in [18] it is shown that by increasing the "energy" of the hidden message, it is possible to reduce BER to 12% -15%, but the cover image quality is significantly reduced.

Thus, the main problem with Spread Spectrum Steganography is to reduce BER while maintaining acceptable cover image quality. For example, [18], page 22 states: “The BER is always higher than the desired value of 12%. A power of 150 has an error rate of 16% + and the picture quality is becoming unacceptable. Increasing the stegopower results in smaller improvements of the BER, approaching a limit of just under 16%.”.

Further research has focused on lowering BER and improving cover image quality. For this, various techniques were used [23, 26]: noise-immune coding, filtering, etc. In works [22, 27] variants of Spread Spectrum Steganography are investigated while using audio and video cover files. In [28–31], message hiding is implemented in the DCT-domain. These methods make it possible to implement message hiding that is resistant to compression attacks. For example, the most common JPEG compression method uses DCT. Hiding data in the DCT-domain reduces the BER, i.e. the number of errors in recovered messages decreases.

Another possible way to reduce BER is to select the spreading sequences [32], [33]. For instance, in [32], we have proposed to form expanding sequences taking into account the statistical properties of cover files. This allowed us to significantly reduce the BER. In some cases, it is possible to achieve BER≈0, however, in this case, the formation time of the spreading sequences is very long. In addition, the receiving side needs a list of spreading sequences (or a compact rule for their generation) to recover a message. Image quality remains the same. As the volume of the hidden message increases, the quality of the images inevitably decreases.

In this paper, we propose a new way to hide data in cover files. Our approach allows minimizing distortion of cover files, even with a large volume of simultaneously hidden messages. We show examples of images with different hiding methods. The proposed method has benefit in the quality of the cover image. On the contrary, the computational complexity of our method is much higher: the complexity of message recovery grows exponentially as the encoding density increases. This is the main disadvantage of the proposed method. However, you can always find a compromise between computational complexity and quality of cover files..

3 Used Data Hiding Technique

Notable examples of Spread Spectrum Steganography use pseudo-random sequences to hide messages. In this case, various data can be used as cover files: images, audio, video, etc. In addition, hiding can be implemented both in the spatial domain and in the DCT domain. We will not focus on this, since the method proposed below can also be applied in various ways. To describe the basic technology, we will follow the publications [18–20], nevertheless offering some of our interpretations.

Let's designate an information message as a sequence of bits $m_0, m_1, ..., m_{k-1}$ written in polar form:

$$\forall i \in \{0,1,...,k-1\} : m_i \in \{-1,1\} .$$

Discrete signals [18–20] are used to implement direct spread spectrum technology:

$$\Phi_i \in \Phi = \left\{\Phi_0, \Phi_1, ..., \Phi_{N-1}\right\}, \; k \le N ,$$

moreover, each signal is a pseudorandom sequence (PRS):

$$\forall i \in \{0,1,...,N-1\} : \Phi_i = \left(\varphi_{i_0}, \varphi_{i_1}, ..., \varphi_{i_{n-1}}\right), \; \forall j \in \{0,1,...,n-1\} : \varphi_{i_j} \in \{-1,1\} .$$

It is assumed that different signals from the set Φ are weakly correlated, i.e. the coefficient of their cross-correlation is approximately zero:

$$\forall i \ne j : \rho\left(\Phi_i, \Phi_j\right) = \sum_{u=0}^{n-1} \varphi_{i_u} \varphi_{j_u} \approx 0 .$$

The stego-file S is formed by adding an amplified modulated signal E [18–20] to the original carrier-file C:

$$E = G \cdot \sum_{i=0}^{k-1} m_i \Phi_i ,$$

e.g.

$$S = C + G \cdot E = C + G \cdot \sum_{i=0}^{k-1} m_i \Phi_i , \tag{1}$$

where $G > 0$ is a gain factor that sets the "energy" of the modulated signal E.

The restoration of the information message on the receiving side is carried out using correlation reception. It is assumed that each signal from the set Φ is not correlated with the original cover file C:

$$\forall i : \rho\left(\Phi_i, C\right) \approx 0 . \tag{2}$$

Then the value of the correlation coefficient is defined as

$$\rho\left(\Phi_i, S\right) = \rho\left(\Phi_i, C + G \cdot E\right) = \rho\left(\Phi_i, C\right) + G \cdot \rho\left(\Phi_i, E\right) \approx G \cdot \sum_{j=0}^{k-1} m_j \sum_{u=0}^{n} \varphi_{i_u} \varphi_{j_u} .$$

Accepting the assumption

$$\forall j \ne i : \; \rho\left(\Phi_i, \Phi_j\right) = \sum_{u=0}^{n} \varphi_{i_u} \varphi_{j_u} \approx 0$$

we have that

$$\rho\left(\Phi_i, S\right) \approx G \cdot m_i \cdot n,$$

That is sign $\rho\left(\Phi_i, S\right)$ matches the value m_i [18–20]:

$$m_i = sign\left(\rho\left(S, \Phi_i\right)\right) = \begin{cases} -1, \ \rho\left(S, \Phi_i\right) < 0; \\ +1, \ \rho\left(S, \Phi_i\right) > 0. \end{cases} \quad (3)$$

Obviously, the total number k of hidden information bits cannot be large. Indeed, if $k = 1$, then the cover file will not be significantly distorted. As follows from (1), cover file will be added to the $G \cdot m_0 \Phi_0$, i.e. cover file C distortions will be in the range $-G...G$. If G is not big, then $S \approx C$. For example, for cover images, distortion will not be visually noticeable. However, with increasing $k > 1$ the distortion of the cover file increases proportionally and it is in the range $-Gk...Gk$. For example, for $k = 10$ the distortion will increase in 10 times and this cannot be changed.

In real situations, to decrease the BER, the value must also be increased. For example, in [18], even for large values, the BER value could not be reduced below 12%. And this is the main contradiction, namely reducing the BER and maintaining the quality of the cover file is possible only with a small encoding density, i.e. at small k.

We propose a new data hiding technique based on rules other than (1) and (3).

4 Proposed data Hiding Method

Let's designate an information message as a sequence of bits $m_0, m_1, ..., m_{(k-1)K}$ written in polar form:

$$\forall i \in \{0,1,...,(k-1)K\} : m_i \in \{-1,1\}.$$

Hiding the message is performed in blocks of k bits. For convenience, we represent the information message as a sequence of non-negative integers:

$$M_1, M_2, ..., M_K,$$

where:

$$\forall i \in \{1,2,...,K\} : \ M_i = \sum_{j=0}^{k-1} 2^j m_{k(i-1)+j}.$$

These numbers $M_i \in \{0,1,...,N-1\}$, $N = 2^k$, $i \in \{1,2,...,K\}$ will be interpreted as addresses (ordinal numbers) of PRS $\Phi_{M_i} \in \Phi = \{\Phi_0, \Phi_1, ..., \Phi_{N-1}\}$, where, as before:

$$\forall i \in \{0,1,...,N-1\} : \Phi_i = \left(\varphi_{i_0}, \varphi_{i_1}, ..., \varphi_{i_{n-1}}\right),\ \forall j \in \{0,1,...,n-1\} : \varphi_{i_j} \in \{-1,1\}.$$

To reduce the distortion of the cover file, we propose to hide information messages based on the addressing of the spreading sequences. The spreading sequence encoding rule is proposed to be implemented as follows:

$$E_i = \Phi_{M_i} = \left(\varphi_{M_{i_0}}, \varphi_{M_{i_1}}, ..., \varphi_{M_{i_{n-1}}}\right),$$

that is, modulation is carried out through addressing this signal in the set $\Phi = \left\{\Phi_0, \Phi_1, ..., \Phi_{N-1}\right\}$.

The proposed approach minimizes the introduced distortions of the cover-file used. Indeed, the cover-file is formed, as before, by the element-wise addition of the modulated signal and the cover data, i.e. instead of (1) we now have:

$$S_i = C_i + G \cdot E_i = C_i + G \cdot \Phi_{M_i}, \tag{4}$$

which will lead to the introduction of distortion in the range $-G...G$ (for any value k).

Thus, the proposed technique, through the use of rule (4), makes it possible to simultaneously hide a block of $k \geq 1$ hidden information bits, and the cover file distortions will be the same as in the known method (1) for $k = 1$. In the general case, the amount of introduced distortion, in the proposed method, will be determined only by the gain coefficient G, and will not depend on k, i.e. from the encoding density of the steganographic system. This is the main advantage of the proposed method.

To restore each block of an information message $M_i \in \left\{0,1,...,N-1\right\}$ on the receiving side, it is necessary to determine the number of the spreading sequence

$$\Phi_{M_i} \in \Phi = \left\{\Phi_0, \Phi_1, ..., \Phi_{N-1}\right\}.$$

To do this, it is proposed to alternately calculate the correlation coefficients $\rho\left(\Phi_\ell, S\right)$ for all $\forall \ell \in \{0,1,...,N-1\}$. The address ℓ (sequence number) of the discrete signal Φ_ℓ for which the calculated correlation coefficient $\rho\left(\Phi_\ell, S\right)$ will be maximum (over all ℓ) sets the decimal value of the information message block $M_i = \ell$, which was hidden on the transmitting side.

Let's formalize the process described above. To restore the block of the hidden message M_i, we use a correlation receiver, the rule of which is to calculate the correlation coefficient:

$$\rho\left(\Phi_\ell, S\right) = \rho\left(\Phi_\ell, C + G \cdot E\right) = \rho\left(\Phi_\ell, C\right) + G \cdot \rho\left(\Phi_\ell, E\right).$$

Taking assumption (2), we have:

$$\rho\left(\Phi_\ell, S\right) \approx G \cdot \rho\left(\Phi_\ell, E\right) = G \cdot \Phi_\ell \cdot \Phi_{M_i} = G \cdot \sum_{u=0}^{n} \varphi_{\ell_u} \varphi_{M_{i_u}}.$$

Taking assumption

$$\forall \ell \neq M_i : \ \rho\left(\Phi_\ell, \Phi_{M_i}\right) = \sum_{u=0}^{n} \varphi_{\ell_u} \varphi_{M_{i_u}} \approx 0$$

we have possible values:

$$\rho\left(\Phi_\ell, S\right) \approx \begin{cases} 0, \ell \neq M_i; \\ G, \ell = M_i. \end{cases}$$

Then the value of the information message block M_i is determined by the rule

$$M_i = \ell : \rho\left(\Phi_{M_i}, S\right) = \max_{\ell} \rho\left(\Phi_\ell, S\right). \tag{5}$$

Thus, to restore each block M_i of an information message, it is necessary to calculate no more than $N = 2^k$ correlation coefficients $\rho\left(\Phi_\ell, S\right)$ and select the maximum value. The index ℓ (number, address) of such a PRS Φ_ℓ sets the block value $M_i = \ell$.

Obviously, while increasing the block size, the computational complexity of recovering a message rapidly (exponentially) increases. This is the main disadvantage of our method. For example, for $k = 10$ it is necessary to calculate no more than $2^{10} \approx 10^3$ coefficients $\rho\left(\Phi_\ell, S\right)$, and for $k = 20$ it is equal to $2^{20} \approx 10^6$. At the same time, for each such case, the quality of the cover file will decrease minimally (the same as for the method from section III at $k = 1$). The rational, in our opinion, is to find a compromise between the expected computational complexity and the encoding density of the steganographic system.

It should be noted that the design of the proposed data hiding method uses several basic assumptions:

- the assumption (2) that each signal from the set Φ is not correlated with the original cover file C. In real cases, this assumption may not be fulfilled, but in [32] we proposed an effective way to guarantee the fulfillment of condition (2) due to the adaptive (taking into account the statistical properties of the cover file) set generation;
- the assumption that different signals from the set Φ are weakly correlated; their mutual correlation coefficient is approximately equal to zero $\forall i \neq j : \rho\left(\Phi_i, \Phi_j\right) \approx 0$. This assumption is also ensured at the stage of generating the set Φ.

5 Experimental Studies

To assess the quality of cover files, signal-to-noise ratios are usually used [34]. For example, the Peak signal-to-noise ratio (PSNR) is the ratio between the maximum possible signal power and the power of the distorting noise. For convenience, PSNR is usually expressed on a logarithmic scale, i.e. in decibels.

For monochrome images, PSNR is calculated from the mean squared error (MSE) [34]. For example, for a monochrome $N_1 \times N_2$ image C and its distorted by approximation errors S, the MSE value is determined by the formula:

$$C_{MSE} = \frac{1}{N_1 N_2} \sum_{i=0}^{N_1-1} \sum_{j=0}^{N_2-1} [C(i, j) - S(i, j)]^2 ,$$

where $C(i, j)$ and $S(i, j)$ is a pixel brightness values with coordinates i, j.

The PSNR value expressed in logarithmic scale (i.e. in decibels) is defined as:

$$PSNR = 10 \cdot \log_{10} \left(\frac{C_{\max}^2}{C_{MSE}} \right) = 20 \cdot \log_{10} \left(\frac{C_{\max}}{\sqrt{C_{MSE}}} \right) =$$
$$= 20 \cdot \log_{10} (C_{\max}) - 10 \cdot \log_{10} (C_{MSE}),$$

where $C_{\max}$ is a maximum possible image pixel value.

If m is used for encoding the brightness of each pixel, then $C_{\max} = 2^m - 1$. For example, for $m = 8$ we have $C_{\max} = 255$ and PSNR is calculated by the formula:

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

For our experiments, we used a standard test image of Lenna 256×256 pixels, encoding each monochrome halftone pixel with one byte (see Fig. 1). In fig. 2-5 show examples of appropriate cover images when hiding informational messages using rule (1) with $G = 4$:

- fig. 2 corresponds to the case $k = 1$;
- fig. 3 corresponds to the case $k = 2$;
- fig. 4 corresponds to the case $k = 4$;
- fig. 5 corresponds to the case $k = 8$.

In fig. 6 an example of a cover image when hiding informational messages using rule (5) with $k = 8$ and $G = 4$ is presented.

Fig. 1. Standard test image Lenna

Fig. 2. Cover image, hiding rule (1), $k = 1$, $G = 4$

Fig. 3. Cover image, hiding rule (1), $k = 2$, $G = 4$

Fig. 4. Cover image, hiding rule (1), $k = 4$, $G = 4$

Fig. 5. Cover image, hiding rule (1), $k = 8$, $G = 4$

Fig. 6. Cover image, hiding rule (5), $k = 8$, $G = 4$

Hiding information messages was implemented programmatically using the MathCad computer algebra system. To generate a set of PRS, a random number generator built into MathCad was used, the PRS $\Phi = \{\Phi_0, \Phi_1, ..., \Phi_{N-1}\}$. We choose the length $n = 256$. To reduce BER, the PRS was additionally rejected by the criterion

$$\forall i : \left|\rho\left(\Phi_i, C\right)\right| \le \rho_{\max} = 1000,$$

since it was implemented in [32].

The information k bits were hidden sequentially in each of the 256 image lines. Thus, one of the lines of the cover-image of pixels 256×256 was used as the value.

For such parameters and for $G = 4$ we have:

$$\rho_{\max} = 1000 < G \cdot n = 1024$$

and fault-tolerant (BER≈0) information message recovery is practically achieved [32].

In fig. 7 and 8 show the dependences of MSE and PSNR on k for various values G. Solid lines correspond to information hiding rule (1), dashed lines - rule (2).
By analyzing the above-mentioned results, the proposed method can significantly reduce the distortion of the cover file. For instance, the image quality in Fig. 6 is comparable to the quality of Figure 2. However, the number of hidden data bits when using rule (4) is increased by $k = 8$. A further increase in the value does not lead to a decrease in the quality of cover images and Fig. 7, 8 clearly confirm this. On the contrary, an increase in the number when using the well-known rule (1) leads to an inevitable decrease in the image quality.

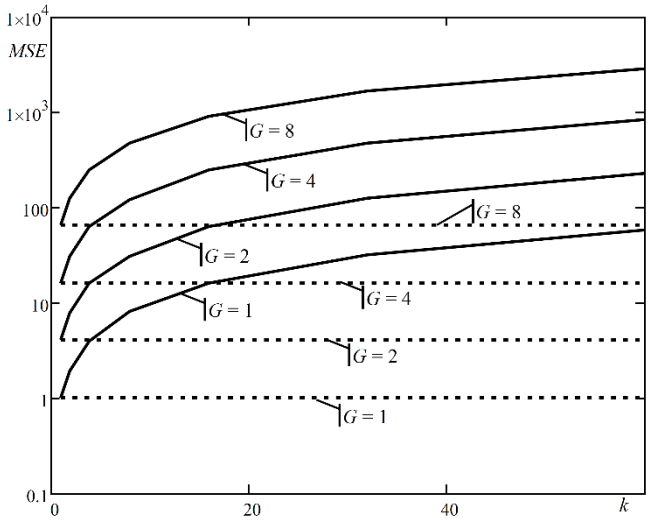

Fig. 7. Dependencies MSE on k

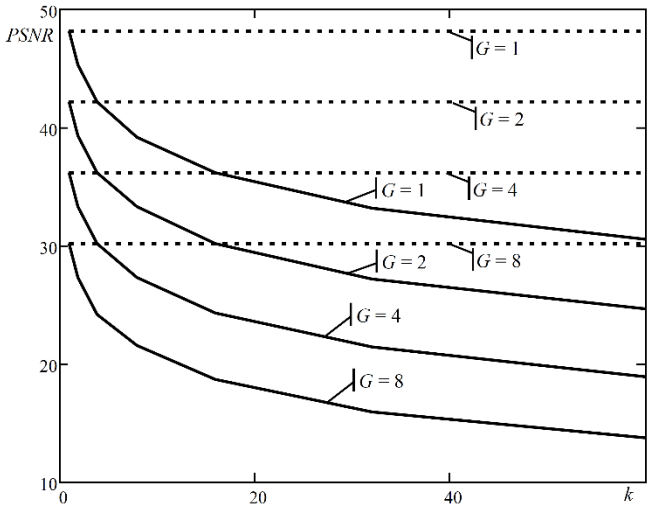

Fig. 8. Dependencies PSNR on k

6 Conclusions

Direct spread spectrum technology is successfully applied in steganographic problems. With the use of expanding PRS, it is possible to reliably hide information messages in cover files. However, in this case, natural contradictions arise:

- for increasing in the amount of hidden data leads to a decrease in the quality of cover files, for example, images;
- for reducing the error rate (BER) in recovered messages, it is necessary to increase the stegopower, which further distorts cover files.

In our previous work [32], we showed that using special methods of generating the PRS significantly reduce the BER (if a number of constraints are met, one can achieve almost error-free message recovery, ie, BER≈0). However, the quality of cover files still decreases when hidden.

In this paper, we have proposed a new information hiding technique based on the addressing of the PRS. This method leads to the increase in computational complexity (to recover messages, it is necessary to repeatedly calculate the correlation coefficients with all possible PRS). However, the quality of cover files is practically not reduced. Our experiments have shown, that Spread Spectrum Steganography technique indeed reduce the distortion in cover images compared to other techniques. We give some illustrative examples and show the advantages of the proposed method.

A promising direction for further research is the use of pseudorandom sequences with special correlation properties, for example, from [35–37]. This direction seems to be especially relevant for the simultaneous reduction of BER and MSE. In addition, it is also important to substantiate recommendations for choosing a compromise between the value and the expected computational complexity when implementing rule

(5). Also a promising area is an assessment of possible information security risks associated with the introduction of new technologies for hiding information.

References

1. Menezes, A.J., Oorschot, P.C. van, Vanstone, S.A., Oorschot, P.C. van, Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press (2018). https://doi.org/10.1201/9780429466335.
2. Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T.: Digital Watermarking and Steganography, 2nd Ed. Morgan Kaufmann, Amsterdam ; Boston (2007).
3. Fridrich, J.: Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, Cambridge ; New York (2009).
4. Rubinstein-Salzedo, S.: Cryptography. Springer International Publishing, Cham (2018). https://doi.org/10.1007/978-3-319-94818-8.
5. Delfs, H., Knebl, H.: Introduction to Cryptography. Springer Berlin Heidelberg, Berlin, Heidelberg (2015). https://doi.org/10.1007/978-3-662-47974-2.
6. Singh, A.K., Kumar, B., Singh, G., Mohan, A.: Secure Spread Spectrum Based Multiple Watermarking Technique for Medical Images. In: Singh, A.K., Kumar, B., Singh, G., and Mohan, A. (eds.) Medical Image Watermarking: Techniques and Applications. pp. 125–157. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-57699-2_6.
7. Menon, N., Vaithiyanathan: A survey on image steganography. In: 2017 International Conference on Technological Advancements in Power and Energy (TAP Energy). pp. 1–5 (2017). https://doi.org/10.1109/TAPENERGY.2017.8397274.
8. Qin, J., Luo, Y., Xiang, X., Tan, Y., Huang, H.: Coverless Image Steganography: A Survey. IEEE Access. 7, 171372–171394 (2019). https://doi.org/10.1109/ACCESS.2019.2955452.
9. Schöttle, P., Böhme, R.: Game Theory and Adaptive Steganography. IEEE Transactions on Information Forensics and Security. 11, 760–773 (2016). https://doi.org/10.1109/TIFS.2015.2509941.
10. Yahya, A.: Introduction to Steganography. In: Yahya, A. (ed.) Steganography Techniques for Digital Images. pp. 1–7. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-319-78597-4_1.
11. Li, M., Guo, Y., Wang, B., Kong, X.: Secure spread-spectrum data embedding with PN-sequence masking. Signal Processing: Image Communication. 39, 17–25 (2015). https://doi.org/10.1016/j.image.2015.07.014.
12. Pomponiu, V., Cavagnino, D., Botta, M.: SS-SVD: Spread spectrum data hiding scheme based on Singular Value Decomposition. In: 2015 International Symposium on Consumer Electronics (ISCE). pp. 1–2 (2015). https://doi.org/10.1109/ISCE.2015.7177769.
13. Hua, G.: Over-Complete-Dictionary-Based Improved Spread Spectrum Watermarking Security. IEEE Signal Processing Letters. 27, 770–774 (2020). https://doi.org/10.1109/LSP.2020.2986154.
14. Kokui, N., Kang, H., Iwamura, K., Echizen, I.: Best embedding direction for spread spectrum-based video watermarking. In: 2016 IEEE 5th Global Conference on Consumer Electronics. pp. 1–3 (2016). https://doi.org/10.1109/GCCE.2016.7800389.
15. Torrieri, D.: Principles of Spread-Spectrum Communication Systems. Springer International Publishing (2018). https://doi.org/10.1007/978-3-319-70569-9.

16. Ipatov, V.P.: Spread Spectrum and CDMA: Principles and Applications. John Wiley & Sons, Ltd, Chichester, UK (2005). https://doi.org/10.1002/0470091800.
17. Sklar, B.: Digital Communications: Fundamentals and Applications. Prentice Hall, Upper Saddle River, NJ (2017).
18. Marvel, L.M., Boncelet, C.G., Retter, C.T.: Spread spectrum image steganography. IEEE Transactions on Image Processing. 8, 1075–1083 (1999). https://doi.org/10.1109/83.777088.
19. Marvel, L.M., Boncelet, C.G., Retter, C.T.: Methodology of Spread-Spectrum Image Steganography. ARMY RESEARCH LAB ABERDEEN PROVING GROUND MD (1998).
20. Brundick, F.S., Marvel, L.M.: Implementation of Spread Spectrum Image Steganography: Defense Technical Information Center, Fort Belvoir, VA (2001). https://doi.org/10.21236/ADA392155.
21. 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). https://doi.org/10.1109/EMBC.2018.8512344.
22. 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). https://doi.org/10.1109/ICEEI.2011.6021662.
23. 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). https://doi.org/10.1109/IWASID.2008.4688395.
24. 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). https://doi.org/10.1109/ICIIP.2017.8313696.
25. Smith, J.R., Comiskey, B.O.: Modulation and information hiding in images. In: Anderson, R. (ed.) Information Hiding. pp. 207–226. Springer, Berlin, Heidelberg (1996). https://doi.org/10.1007/3-540-61996-8_42.
26. US-6557103-B1 - Spread Spectrum Image Steganography | Unified Patents, https://portal.unifiedpatents.com/patents/patent/US-6557103-B1, last accessed 2020/09/14.
27. Zarmehi, N., Akhaee, M.A.: Video steganalysis of multiplicative spread spectrum steganography. In: 2014 22nd European Signal Processing Conference (EUSIPCO). pp. 2440–2444 (2014).
28. Ustubioglu, A., Ulutas, G., Ulutas, M.: DCT based image watermarking method with dynamic gain. In: 2015 38th International Conference on Telecommunications and Signal Processing (TSP). pp. 550–554 (2015). https://doi.org/10.1109/TSP.2015.7296323.
29. Agrawal, N., Gupta, A.: DCT Domain Message Embedding in Spread-Spectrum Steganography System. In: 2009 Data Compression Conference. pp. 433–433 (2009). https://doi.org/10.1109/DCC.2009.86.
30. Weihua, X., Yongbing, W., Shuiyuan, Y.: H.264 Video Watermark Algorithm Using DCT Spread Spectrum. In: 2015 3rd International Conference on Applied Computing and Information Technology/2nd International Conference on Computational Science and Intelligence. pp. 447–450 (2015). https://doi.org/10.1109/ACIT-CSI.2015.84.
31. Ling Lu, Xinde Sun, Leiting Cai: A robust image watermarking based on DCT by Arnold transform and spread spectrum. In: 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE). pp. V1-198-V1-201 (2010). https://doi.org/10.1109/ICACTE.2010.5579033.

32. 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). https://doi.org/10.1109/DESSERT50317.2020.9125032.
33. Kuznetsov, A., Smirnov, A., Gorbacheva, L., Babenko, V.: Hiding data in cover images using a pseudo-random sequences. In: Subbotin, S. (ed.) Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020), Zaporizhzhia, Ukraine, April 27-May 1, 2020. pp. 646–660. CEUR-WS.org (2020).
34. Korhonen, J., You, J.: Peak signal-to-noise ratio revisited: Is simple beautiful? In: 2012 Fourth International Workshop on Quality of Multimedia Experience. pp. 37–38 (2012). https://doi.org/10.1109/QoMEX.2012.6263880.
35. Kuznetsov, A., Smirnov, O., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D.: Discrete Signals with Special Correlation Properties. In: Luengo, D., Subbotin, S., Arras, P., Bodyanskiy, Y., Henke, K., Izonin, I., Levashenko, V.G., Lytvynenko, V., Parkhomenko, A., Pester, A., Shakhovska, N., Sharpanskykh, A., Tabunshchyk, G., Wolff, C., Wuttke, H.-D., and Zaitseva, E. (eds.) Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019), Zaporizhzhia, Ukraine, April 15-19, 2019. pp. 618–629. CEUR-WS.org (2019).
36. Kuznetsov, A., Smirnov, O., Reshetniak, O., Ivko, T., Kuznetsova, T., Katkova, T.: Generators of Pseudorandom Sequence with Multilevel Function of Correlation. In: 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S T). pp. 517–522 (2019). https://doi.org/10.1109/PICST47496.2019.9061530.
37. Kuznetsov, A., Kiian, A., Kuznetsova, K., Zub, M., Zaburmekha, Y., Lyshchenko, E.: Pseudorandom Sequences with Multi-Level Correlation Function for Direct Spectrum Spreading. In: 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT). pp. 232–237 (2019). https://doi.org/10.1109/ATIT49449.2019.9030436.