

New approaches to the development of information security systems for unmanned vehicles

Bayana B. Ermukhambetova¹, Grigoriy A. Mun^{1,2}, Sherniyaz B. Kabdushev^{1,4},
Aruzhan Bulatovna Kadyrzhan³, Kaisarali K. Kadyrzhan^{1,3}, Yelizaveta S. Vitulyova³,
Ibragim E. Suleimenov¹

¹National Engineering Academy of the Republic of Kazakhstan, Almaty, Kazakhstan

²Department of Chemistry and Technology of Organic Substances, Natural Compounds and Polymers,
Al Farabi Kazakh National University, Almaty, Kazakhstan

³Institute of Telecommunications and Space Engineering, Almaty University of Power Engineering and Telecommunications named after
Gumarbek Daukeev, Almaty, Kazakhstan

⁴Department of Information Systems, International Information Technology University, Almaty, Kazakhstan

Article Info

Article history:

Received Jan 27, 2023

Revised Apr 12, 2023

Accepted Apr 16, 2023

Keywords:

Information security
Method of information
protection
Radiowaves
Secure communication
channels
Unmanned vehicles

ABSTRACT

A new approach to ensuring information security is proposed for using in the zone of direct radio visibility. The approach is based on a direct analogy between radio and optical radiation. In the latter case, information protection can be ensured by identifying the point or direction from which the signal comes; all other light sources are cut off by the observer. It is shown that a similar method of information protection can also be implemented in the radio range, which corresponds to modern trends in the development of radio holography. The simplest scheme for detecting the direction to a transmitter, identified as "friend" is presented. Its operability is demonstrated by means of simulation modeling. Ways for the further development of this approach are determined, based on the fact that modern technologies make it possible to implement distributed reception of a radio signal (to use a relatively large number of receivers), which makes it possible to implement direct analogues of such optical elements as a lens, holograms.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Aruzhan Bulatovna Kadyrzhan

Institute of Telecommunications and Space Engineering, Almaty University of Power Engineering and
Telecommunications named after Gumarbek Daukeev

Baitursynova Street, 050013, Almaty, Kazakhstan

Email: aru.kadyrzhan@gmail.com

1. INTRODUCTION

Information security systems have been developing for a very long time [1]. Their history is inextricably linked with the creation of technologies that provide unauthorized access to information transmission channels; it would not be a big exaggeration to say that during the last decades there has been a continuous competition between information security systems and technologies for their "hacking" [2]. Cryptographic methods have continued and continue to improve, codes are being created that are increasingly resistant to unauthorized access attempts on [3], [4]. However, there is an important nuance: data transmission systems are gradually becoming an integral part of human civilization; therefore, the issue of information security is becoming more and more connected with the human factor. Coding systems can be arbitrarily perfect, but they do not and cannot have protection against dishonest actions of personnel by themselves. Simplifying, relevant information can always be sold on the black market if it is in demand.

Provided that information security systems are used by government agencies or large corporations with their own security services, the risks associated with illegal actions can be minimized. However, if this applies, for example, to small or medium-sized businesses that increasingly require individual protection, such methods are obviously unacceptable due to significant costs. Of course, it is theoretically possible to use information security systems provided by major players in this market, but in this case, the consumer of such systems runs the risk of becoming a hostage of geopolitical confrontation, which, which is no longer in doubt, is acquiring a long-term character [5], including the sphere of technology and education [6], [7]. As the experience of recent years shows, any guarantees based on purely market mechanisms that operated in a relatively short period of the heyday of globalization ideas are now, to put it mildly, being called into question [8], [9]. Therefore, the issue of information security systems that are resistant not only to remote cracking of codes (the actions of “hacker” but also to theft of key information, as well as to unfair use by software vendors, becomes relevant. There is no doubt that the risks of the latter nature are becoming more and more significant. The growth in the number of unadvertised “bookmarks” in software is associated not only with the activities of development companies, but also with the personal initiative of programmers who seek to create various kinds of “airbags” for themselves personally.

In this paper, it is proved that a fundamentally new approach to information protection can be implemented, based not so much on cryptographic methods, but on the specifics of the nature of radio wave propagation. We emphasize that such a formulation of the issue is already actively discussed in the current literature [10]–[12]. In particular, the cited publications discussed the use of physical processes, the very nature of which excludes any unauthorized access to the communication channel. For concretization, the proposed method of protecting information is considered on the example of the problem of protecting the control of unmanned aerial vehicles from unauthorized access (“interception of an unmanned aerial vehicle”).

This problem is of interest not only from the point of view of demonstrating the significance of the developed approach. Existing forecasts for the development of the technical infrastructure of megacities clearly indicate that delivery services (including those meeting the level of small and medium-sized businesses) will refuse to use hired couriers in the foreseeable future and will make every effort to maximize the full potential of unmanned vehicles. It is appropriate to emphasize that from a purely technical point of view (if we exclude issues related to legislative regulation from consideration), pharmacy retail chains are now able to move to a qualitatively new level of functioning associated with the use of unmanned aerial vehicles. Relevant issues are also discussed in the current literature [13], [14]. Consequently, in parallel, the question of “electronic theft” will inevitably arise, which, among other things, will pose a very unpleasant question for small and medium-sized businesses-whether they will submit to the dictates of large corporations or accept the risk associated with the actions of hackers. The technology proposed in this paper avoids both extremes.

2. METHOD

Explaining let us consider an “information security system” that is very easy to implement in the optical range. Three channels of information transmission are schematically shown at Figure 1. Each of them consists of a source and a receiver of light, and the observer’ eye can also act as the latter.

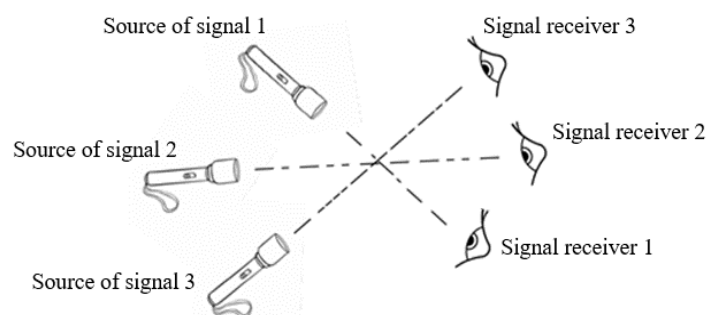


Figure 1. A visual illustration of the formation of secure communication channels in the optical range

Such an optical receiver focuses on a certain point in space where the source is located. The presence of any other light sources, even of much higher intensity, will not prevent the observer from registering information transmitted, for example, in Morse code. Information protection is de facto ensured by the fact that the source of information is located at a certain point in space, due to which it is identified by the observer as “friend”. Radio waves are the same electromagnetic oscillation as the radiation of the optical range. Therefore,

from the point of view of the problems reflected in the introduction, it makes sense to try to implement the same approach, i.e., ensure the protection of information through the identification of a point (or area) of space in which the source of electromagnetic oscillations is located, identified as “friend”.

In this paper, the simplest version of this approach is presented and ways of its further improvement are outlined. We emphasize right away that this method is focused on protection against interception of control of an unmanned vehicle. It is essential that in this case the throughput of the secure control channel can be made quite low. More precisely, the amount of transmitted control information is obviously limited by the operations that the unmanned vehicle can physically perform. From the point of view of elementary mechanics, therefore, it can be argued that it is sufficient to realize an information transfer rate corresponding to a frequency of several tens of Hertz.

3. RESULTS AND DISCUSSION

3.1. The simplest type of protection circuit for the control signal of an unmanned vehicle

The simplest version of the control signal protection circuit that prevents the interception of control of an unmanned vehicle is shown in Figure 2. This scheme implements the following principle. Inside the unmanned vehicle there are several receivers of radio waves. We will assume that their spatial coordinates are r_i . Let's denote the radius vector of the point where the transmitter is located as R_0 . Then the signals perceived by the receivers can be written in the scalar approximation as R_0 .

$$J_i = A(R_0 - r_i)f(\omega t - k|R_0 - r_i|) \tag{1}$$

Where A is an amplitude factor that depends only on the modulus of the coordinate difference, f is an amplitude-phase function that simultaneously describes both the change in the phase of the wave as it propagates in space and the change in the signal introduced by the transmitter modulator, ω is the circular frequency, k is the wavenumber (these parameters correspond to the carrier frequency on which the transmitter operates).

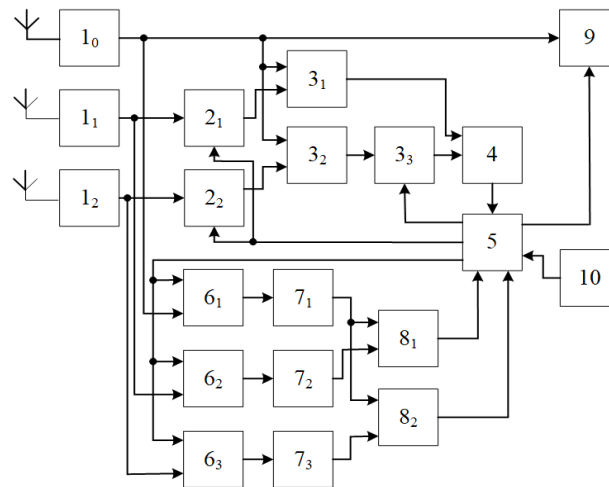


Figure 2. The simplest version of the control signal protection circuit for an unmanned vehicle

Let's consider the difference $J_i - J_j$, assuming that $|R_0| \gg |r_i|$. Consequently, within the area occupied by the unmanned vehicle, the factor A can be considered constant, then:

$$J_i - J_j \sim f(\omega t - \varphi_i) - f(\omega t - \varphi_j) \tag{2}$$

we will also assume that the inequality $\lambda \gg |r_i - r_j|$ for any i, j is valid. Such a choice can be implemented in practice by choosing the appropriate wavelengths or the geometry of the location of the receivers. In this case, one can pass from the difference (2) to the derivative and write as:

$$J_i - J_j \sim (\varphi_i - \varphi_j) \frac{d}{dt} f \tag{3}$$

using the decomposition of the scalar function $|R_0 - r_i|$ in a Taylor series, we get:

$$\varphi_i - \varphi_j \approx -\frac{k}{R_0} R_0 (r_i - r_j) \quad (4)$$

relations (3) and (4), in particular, show that under the condition $\lambda \gg |r_i - r_j|$ registering the difference of oscillations arriving at different receivers will give the same function, differing only in a multiplier. The fact can be expressed by an explicit formula by putting (4) in (3),

$$J_i - J_j \approx -k \frac{R_0}{R_0} (r_i - r_j) \frac{d}{dt} f \quad (5)$$

directly from (5) follows the proposed principle of operation of protecting the control channel of an unmanned vehicle (more precisely, its simplest version). Provided that the unit vector $\frac{R_0}{R_0}$ that specifies the direction to the transmitter is known, as well as the vectors r_i , the proportionality factor B in (5) is also known.

$$B = k \frac{R_0}{R_0} (r_i - r_j) \quad (6)$$

By splitting the radiation receivers into pairs and using differential amplifiers, it is possible to obtain signals that differ only by a constant pre-known multiplier (6). Therefore, the protection of information is provided by the following method. If the signal comes from an authorized source, then the signals taken from the outputs of differential amplifiers, under the assumptions made, should differ from each other only by a factor of the form (6), which is predicted by computational means. If the signal comes from an unauthorized source, then it does not withstand the appropriate check and, in the simplest case, can be ignored.

The simplest version of the circuit that implements this approach Figure 2 contains three radio wave receivers spaced apart in space so that the condition $\lambda \gg |r_i - r_j|$ is satisfied. The signals from the receiving antennas are fed to pre-amplifiers 1_i , which also perform matching functions. The signals from the outputs of amplifiers 1_1 and 1_2 are fed to the inputs of corrective amplifiers 2_1 and 2_2 , which provide adjustment of the gain in order to eliminate factors associated, in particular, with the technological variation in the manufacture of radio components. The purpose of the corrective amplifiers is that at the output of amplifier 1_0 , as well as amplifiers 2_1 and 2_2 , exactly the same signals are formed, provided that the same radio wave arrives at all three receiving antennas. Further, the considered signals are divided into two pairs. The signals corresponding to these two pairs are fed to the inputs of differential amplifiers 3_1 and 3_2 , which, under the assumptions made, perform the differentiation operation, i.e. make it possible to obtain a result corresponding to (3). The signal from the output of one of these amplifiers 3_2 is fed to the input of another corrective amplifier, which multiplies by the amplitude factor corresponding to (6). As a result, if the signal comes from an authorized source, at the output of the differential amplifier 4, a signal is generated that is interpreted as a logical zero. The remaining elements of the circuit are designed to ensure the operation of the corrective amplifiers in the mode described above. Their work is ensured by the fact that in the signals coming from an authorized source, frames are allocated that are intended to provide correction. These frames are interleaved with frames carrying an information (control) signal. During these frames, the transmitter generates a strictly monochromatic signal at the carrier frequency.

At time intervals corresponding to frames intended to provide correction, an opening signal from the microcontroller 5 is supplied to the inputs of the electronic switches 6_i . The signal from the preamplifiers 1_i is supplied to the second inputs of these electronic switches. Next, the signal from the outputs of the keys 6_i is fed to the rectifiers 7_i . The signals from the outputs of the rectifiers 7_i are grouped in pairs and fed to the inputs of the differential amplifiers 8_1 and 8_2 , which generate signals, on the basis of which the microcontroller 5 generates control signals supplied to the correction amplifiers 2_1 and 2_2 . The control signal applied to the correction amplifier 3_3 is determined by calculation using the data coming to the microcontroller 5 from the output of the positioning system 10. When the radiation source is identified as "friend", the opening signal is sent to the electronic key 9, and then to the control systems of the unmanned vehicle.

3.2. Simulation results

For clarity, let us consider the implementation of the proposed approach by means of simulation modeling. Figure 3 shows the result of assembling the circuit corresponding to Figure 2 in the LTspice software environment. Corrective amplifiers are assembled on an operational amplifier according to a negative feedback amplification scheme. To control the gain, a digital variable resistor is connected in series to the feedback loop. The value of the variable resistor is set by the microcontroller and thus the gain of the corrective amplifiers is controlled.

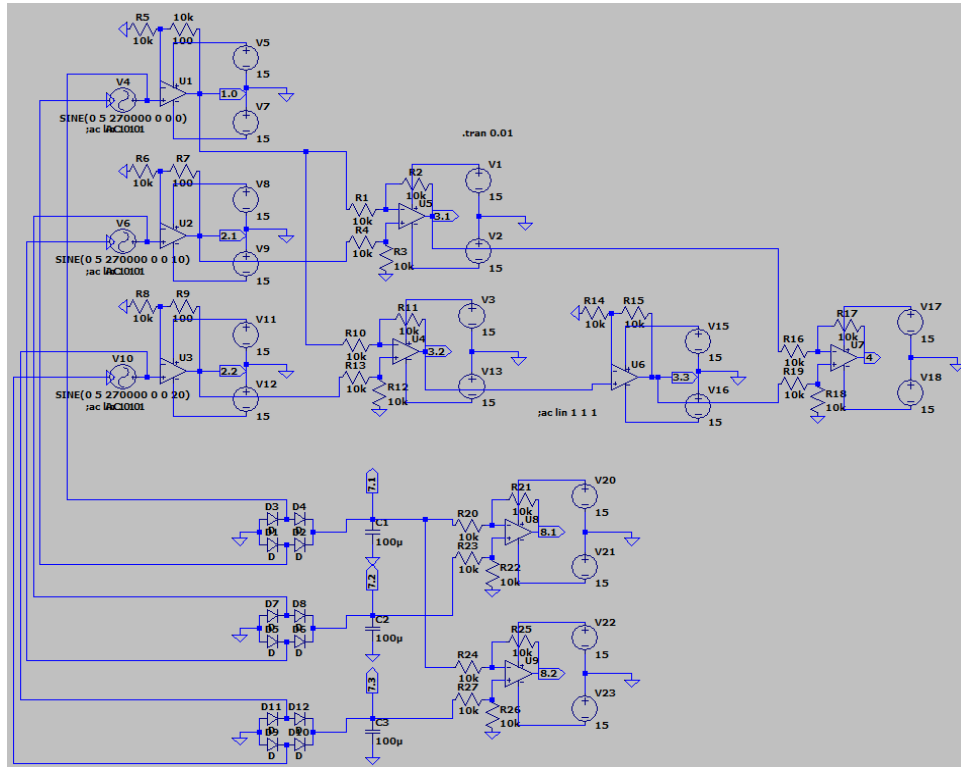


Figure 3. Scheme assembled in the LTspice software environment

In the circuit used to illustrate the proposed approach, blocks 2_1 , 2_2 , 3_1 , 3_2 , 3_3 , 4 are implemented without auto gain control. To demonstrate the operation of the circuit, conventional resistors were used instead of digital variable resistors, the value of which was determined by calculation using (4) and (5). Graphs that clearly show the nature of the principle used are shown in Figure 4 and Figure 5. The data for these graphs were obtained by the built-in LTspice tools and then transferred to Excel for the convenience of graphical display of the data obtained. Figure 4(a) and Figure 5(a) refer to the case when a set of harmonic signals was applied to the system inputs, Figure 4(b) and Figure 5(b) refer to the case of a phase-modulated signal.

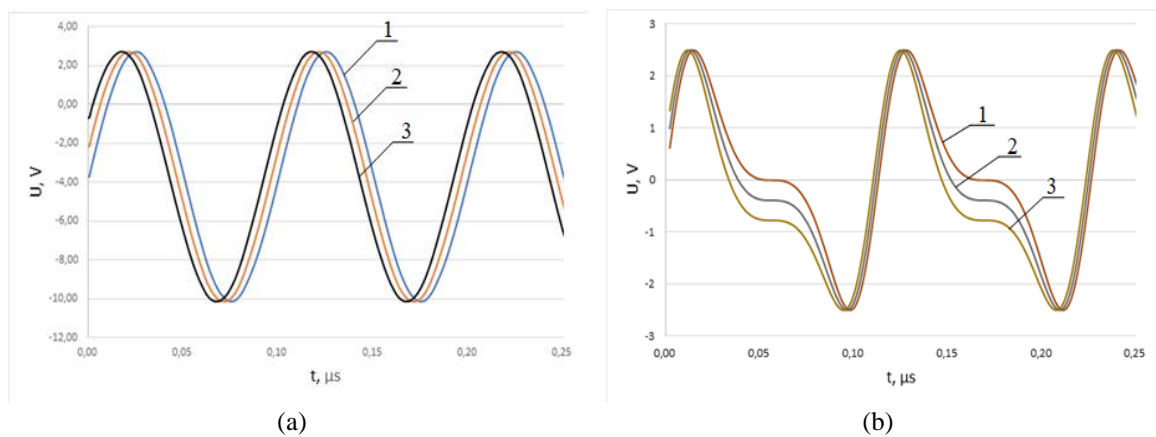


Figure 4. Plots of model signals at the outputs of blocks 1_0 (curve 1), 2_1 (curve 2), and 2_2 (curve 1); (a) the case of a monochromatic signal and (b) the case of a phase-modulated signal

The Figures 4(a) and 4(b) shows three signals corresponding to the outputs of blocks 1_0 , 2_1 , and 2_2 . In essence, this is the same signal, but shifted in phase and equalized in amplitude, which makes it possible to use (3). Specifically, the phase shifts used correspond to values of 14° and 28° . The Figures 5(a) and 5(b) (curves

1 and 2) shows the signals corresponding to the outputs of differential amplifiers 3₁ and 3₂. It can be seen that, in (3), these signals are almost identical in shape, but differ in amplitude. The same figure (curve 3) shows the profile of the signal that is formed at the output of differential amplifier 4 after equalizing in amplitude with the help of corrective amplifier 3₃. It can be seen that this signal is really close to zero. More precisely, the amplitude of this signal is determined only by the highest derivatives, omitted in the expansion in the Taylor series (4), therefore, in terms of amplitude, it is actually more than an order of magnitude smaller than the signals at the output of differential amplifiers 3₁ and 3₂.

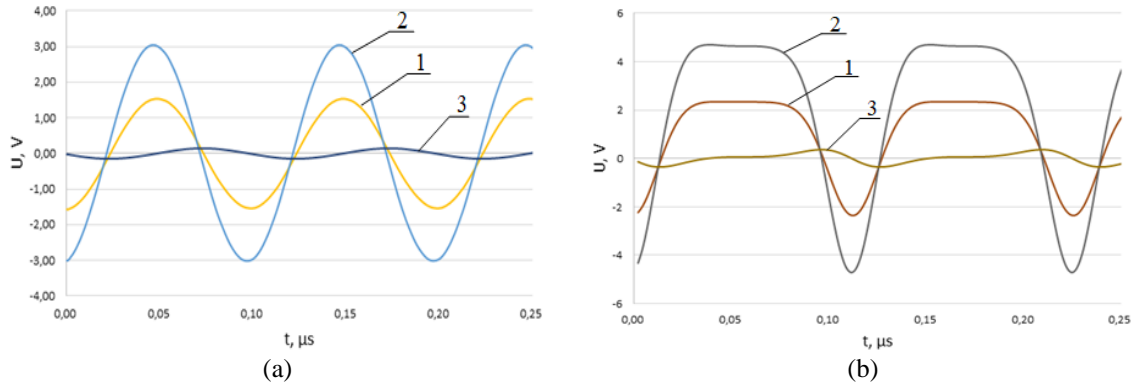


Figure 5. Plots of model signals at the outputs of blocks 3₁ (curve 1), 3₂ (curve 2), and 4 (curve 3); (a) the case of a monochromatic signal and (b) the case of a phase-modulated signal

3.3. Possibilities for further improvement of the proposed methods

The considered example is mainly illustrative. In particular, the issue of the noise level, and, consequently, the resolution of the information protection methods of the proposed type, remains outside the scope of the proposed consideration. Nevertheless, the considered example shows that it is possible to draw a quite definite analogy between information channels implemented in the radio and optical bands. The fact that this analogy is very fruitful is also confirmed by the rather rapid development of radio holography, which has been taking place over the past decades [15]–[17]. This analogy can be developed further. The Figure 6 schematically illustrates the concept of optical thickness, which is used in Fourier optics [18] to describe the operation of such optical elements as a lens. The formula describing the transformation performed by the lens, in terms of Fourier optics, is as;

$$u(x, y) = T(x, y)u_0(x, y) \tag{7}$$

where $u_0(x, y)$ is the field distribution in the “input” plane of a thin lens, $T(x, y)$ is its complex-valued transmission function, $u(x, y)$ is the field distribution in the “output” plane.

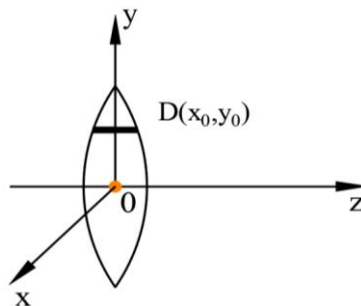


Figure 6. To the definition of the optical thickness function

The terms “output” and “input” planes are partly conditional, since in the thin lens approximation these planes coincide geometrically. In essence, they only emphasize that the transformation performed by an optically “thin” element reduces to multiplication by the phase function. We emphasize that (7) is written in a

general form; it is valid for any element that can be considered as optically thin (paraxial optics approximation). In particular, this formula also describes the functioning of holographic elements that work using diffraction effects. Concretization of (7) for elements similar to a lens, i.e. representing a body made of an optically transparent material, has the following form;

$$u(x, y) = \exp[ikD(x, y)] u_0(x, y) \quad (8)$$

where $k = \frac{2\pi}{\lambda}n$ -wave number, $D(x, y)$ -optical thickness function.

The optical thickness function Figure 6 is numerically equal to the thickness of an element made of a homogeneous material at a point with coordinates (x, y) , i.e., this is the length of the segment lying inside the element, passing through the point (x, y) and lying on a straight line perpendicular to the optical axis. It can be seen that the description of an arbitrary “thin” optical element is reduced to performing the operation of shifting the oscillation phase. Therefore, if we switch to the radio range and replace a “continuous” optical element with a set of discrete ones Figure 7, it turns out that an analogue of any “thin” optical element can be synthesized in the form of a set of controlled phase shifters.

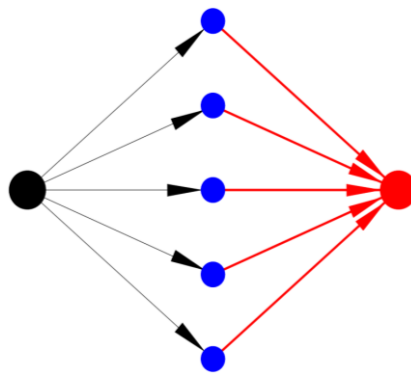


Figure 7. Illustration for the mechanism of operation of a virtual radioholographic lens

Such phase shifters are well known for harmonic oscillations. But, when working with information security systems, it is necessary to ensure the introduction of a phase shift for an arbitrary oscillation. Such an operation is achieved by inverting (5). Indeed, if the derivative of a function at some point in time is known, then by adding to it the derivative multiplied by a given coefficient Q , one can obtain the same function, but shifted in time by an interval specified by Q .

$$J_i(\omega t \pm \varphi_i) = J_i(\omega t) \pm Q \frac{dJ_i}{dt} \quad (9)$$

The corresponding electronic circuit can be assembled based on the circuit shown in Figure 3 with the inclusion of additional adders that ensure the execution of operation (9). Obviously, the accuracy of such an operation remains limited, since it is valid only as long as one can use the Taylor series expansion up to the first derivative. However, if systems similar to radioholographic systems are used, i.e. since there are several receivers spaced apart in space, then it is permissible to calculate derivatives of higher orders.

Of course, the radio engineering calculation of derivatives of higher orders is associated with an increase in the role of noise. However, for the purposes under consideration, one can also switch to the use of signals considered as functions that take values in Galois fields [19], [20]. This can be done with respect to almost any digitized signal [19], [20]. The operation of differentiation in such fields involves the use of finite values, i.e., the analogue of the Taylor series in this case is not necessarily associated with the use of signals decreasing in amplitude. In addition, when using signals that can be expanded into generalized Rademacher functions [20], the analogue of the Taylor series becomes finite. In this regard, it is also appropriate to emphasize that nontrivial algebraic structures are already being used in radio holography [21], and the possibilities of their use for digital signal processing are continuously expanding [22]. There is also the possibility to implement operations in Galois fields using the usual “binary” element base. There are also some other possibilities, for example, related to the features of slowly changing signals, the “digital” derivatives of which can be found using frequency filtering [23] and using the apparatus of ternary logic [24], [25].

4. CONCLUSION

Thus, for transmissions in the line-of-sight zone, it is possible to implement information protection that does not require the use of cryptographic methods. The protection of information in the area of direct radio visibility is becoming increasingly important, in particular, in connection with the increasing use of unmanned vehicles, including those designed to provide certain services to the population. The proposed principle of information security is based on the obvious fact that both radio waves and light are electromagnetic oscillations that differ only in wavelength. The protection of information in the optical range can only be ensured by linking the signal source to a certain point or to a certain direction. In the case when the signals come from this particular point, they are interpreted as reliable. The materials of the work show that a similar method of information protection can also be implemented in the radio band for the case when the transmitter and the set of receiving devices are in the zone of direct radio visibility. Here you can offer a very wide range of technical solutions. In the simplest case, an information security system based on multichannel radio engineering differentiation is realizable; in more complex cases, a technique for synthesizing analogues of optical elements based on the use of phase shifters can be used. When using digital transmission of information, the principle of operation of phase shifters that implement analogs of optical systems can be based on the use of specific properties of Galois fields.




REFERENCES

- [1] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993, doi: 10.1109/18.256484.
- [2] C. Bauer "Secret history: the story of cryptology," *Choice Reviews Online*, vol. 51, no. 01, pp. 51-0328-51-0328, Sep. 2013, doi: 10.5860/choice.51-0328.
- [3] O. G. Abood and S. K. Guirguis, "A survey on cryptography algorithms," *International Journal of Scientific and Research Publications (IJSRP)*, vol. 8, no. 7, pp. 51-0328-51-0328, Jul. 2018, doi: 10.29322/ijsrp.8.7.2018.p7978.
- [4] R. Fotuhi, S. F. Bari, and M. Yusefi, "Securing wireless sensor networks against denial-of-sleep attacks using RSA cryptography algorithm and interlock protocol," *International Journal of Communication Systems*, vol. 33, no. 4, Mar. 2020, doi: 10.1002/dac.4234.
- [5] Ø. Tunsjø, "Combining polarity and geopolitics: the explanatory power of geostructural realism," 2022, pp. 81–99.
- [6] K. Khan, C. W. Su, M. Umar, and W. Zhang, "Geopolitics of technology: a new battleground?," *Technological and Economic Development of Economy*, vol. 28, no. 2, pp. 442–462, Feb. 2022, doi: 10.3846/tede.2022.16028.
- [7] M. P. Amaral, "Imagining and transforming higher education. Knowledge production in the new geopolitics of knowledge," in *Educational Governance Research*, vol. 17, 2022, pp. 35–51.
- [8] I. Liadze, C. Macchiarelli, P. Mortimer-Lee, and P. S. Juanino, "Economic costs of the Russia-Ukraine war," *World Economy*, vol. 46, no. 4, pp. 874–886, Apr. 2022, doi: 10.1111/twec.13336.
- [9] N. Palma and P. O'Brien, "The wartime power of central banks: lessons from the napoleonic era," *Centre For Economic Policy Research*, 2022. <https://cepr.org/voxeu/columns/wartime-power-central-banks-lessons-napoleonic-era> (accessed Feb. 15, 2023).
- [10] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: a comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2019, doi: 10.1109/COMST.2018.2878035.
- [11] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1878–1911, 2019, doi: 10.1109/COMST.2018.2883144.
- [12] M. Zoli, M. Mitev, A. N. Barreto, and G. Fettweis, "Estimation of the secret key rate in wideband wireless physical-layer-security," in *Proceedings of the International Symposium on Wireless Communication Systems*, Sep. 2021, vol. 2021-September, pp. 1–6, doi: 10.1109/ISWCS49558.2021.9562135.
- [13] A. E. Oigbochie, E. B. Odigie, and B. I. G. Adejumo, "Importance of drones in healthcare delivery amid a pandemic: current and generation next application," *Open Journal of Medical Research (ISSN: 2734-2093)*, vol. 2, no. 1, pp. 01–13, Apr. 2021, doi: 10.52417/ojmr.v2i1.187.
- [14] F. Stephan, N. Reinsperger, M. Grünthal, D. Paulicke, and P. Jahn, "Human drone interaction in delivery of medical supplies: a scoping review of experimental studies," *PLoS ONE*, vol. 17, no. 4 April, p. e0267664, Apr. 2022, doi: 10.1371/journal.pone.0267664.
- [15] I. Theodorou, C. V. Ilioudis, C. Clemente, and M. Vasile, "SISAR imaging-radio holography signal reconstruction based on receiver-transmitter motion," in *2019 IEEE Radar Conference, RadarConf 2019*, Apr. 2019, pp. 1–6, doi: 10.1109/RADAR.2019.8835596.
- [16] V. I. Kalinin, V. V. Chapursky, and V. A. Cherepenin, "Super-resolution of radar and radio holography systems based on a mimo retrodirective antenna array," *Journal of Communications Technology and Electronics*, vol. 66, no. 6, pp. 727–736, Jun. 2021, doi: 10.1134/S1064226921060139.
- [17] X. Zhang, H. Kang, Y. Zuo, Z. Lou, Y. Wang, and Y. Qian, "Near-field radio holography of slant-axis terahertz antennas," *IEEE Transactions on Terahertz Science and Technology*, vol. 10, no. 2, pp. 141–149, Mar. 2020, doi: 10.1109/TTHZ.2019.2958066.
- [18] P. Sutton, "Introduction to fourier optics," *Quantum and Semiclassical Optics: Journal of the European Optical Society Part B*, vol. 8, no. 5, Oct. 1996, doi: 10.1088/1355-5111/8/5/014.
- [19] E. S. Vitulyova, D. K. Matrassulova, and I. E. Suleimenov, "New application of non-binary galois fields fourier transform: digital analog of convolution theorem," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 23, no. 3, pp. 1718–1726, Sep. 2021, doi: 10.11591/ijeecs.v23.i3.pp1718-1726.
- [20] E. S. Vitulyova, D. K. Matrassulova, and I. E. Suleimenov, "Construction of generalized rademacher functions in terms of ternary logic: solving the problem of visibility of using galois fields for digital signal processing," *International Journal of Electronics and Telecommunications*, vol. 68, no. 2, pp. 237–244, 2022, doi: 10.24425-ijet.2022.139873/960.
- [21] X. Ma and T. Li, "Surface reconstruction of deformable reflectors by combining Zernike polynomials with radio holography," *AIAA Journal*, vol. 57, no. 6, pp. 2544–2552, Jun. 2019, doi: 10.2514/1.J058023.




- [22] D. K. Matrassulova, Y. S. Vitulyova, S. V. Konshin, and I. E. Suleimenov, "Algebraic fields and rings as a digital signal processing tool," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 29, no. 1, pp. 206–216, 2023, doi: 10.11591/ijeecs.v29.i1.pp206-216.
- [23] Y. S. Vitulyova, A. S. Bakirov, and I. E. Suleimenov, "Galois fields for digital image and signal processing: evidence for the importance of field specificity," in *2022 5th International Conference on Pattern Recognition and Artificial Intelligence, PRAI 2022*, Aug. 2022, pp. 637–642, doi: 10.1109/PRAI55851.2022.9904074.
- [24] I. Moldakhan, D. B. Shaltikova, Z. M. Egemberdyeva, and I. E. Suleimenov, "Application of ternary logic for digital signal processing," *IOP Conference Series: Materials Science and Engineering*, vol. 946, no. 1, p. 012002, Oct. 2020, doi: 10.1088/1757-899X/946/1/012002.
- [25] I. Suleimenov, A. Bakirov, and I. Moldakhan, "Formalization of ternary logic for application to digital signal processing," in *Advances in Intelligent Systems and Computing*, vol. 1259 AISC, 2021, pp. 26–35.

BIOGRAPHIES OF AUTHORS






Bayana B. Ermukhambetova    is working as Senior Researcher in National Engineering Academy of the Republic of Kazakhstan, Almaty, Kazakhstan, Ph.D. (chemistry). Graduated from the Chemistry Department of the Al-Farabi Kazakh National University in 1986; defended his thesis for the degree of candidate of chemical sciences in 1995 at the same university. Currently, the main direction of scientific activity is interdisciplinary research at the intersection of chemistry, information theory and telecommunications. One of the important results in this direction is the development of methods for controlling systems that are analogues of neural networks using methods obtained on the basis of studying analogues of neural networks in the chemistry of macromolecular compounds (h-index 3). She can be contacted at email: baya_erm@mail.ru.






Grigoriy A. Mun    Professor Ph.D., Dr. Sc., department of chemistry and technology of organic substances, natural compounds and polymers of Al-Farabi Kazakh National University, Academician of the National Engineering Academy of the Republic of Kazakhstan. He graduated from Mordov State University in 1977 and got his Ph.D. degree in polymer chemistry in Moscow State University in 1984. In 1991 he was promoted to an associate professor, in 1999 received his D.Sc. degree in polymer chemistry and in 2001 was promoted to a professor. Scientific interests: chemistry, physics and technology of polymers and polymer materials, water-soluble and water-swelling polymers, synthesis and characterization of stimuli-responsive polymers, interpolymer reactions and complexes, biomedical related polymers, radiation chemistry of polymers, synthesis and characterization of hydrophilic polymers and interpolymer complexes for application in nanoelectronics and nanotechnology, polymer nanocomposite materials. He has published more than 100 research articles in well reputed international journals, with over 2000 citations (h-index 26). He can be contacted at email: mungrig@yandex.ru.






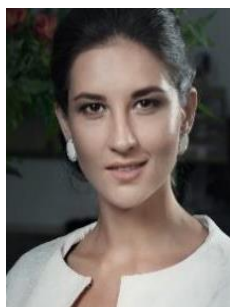
Sherniyaz B. Kabdushev    he is a senior lecturer at international information technologies University Almaty, Kazakhstan. Working part-time at National engineering academy of the Republic of Kazakhstan. He studied at Almaty University of power engineering and telecommunications. After graduation, he worked as an engineer at Huawei, LLP, as a manager of the technical sales support department in Kaztranscom, JSC. Then he studied at the doctoral program at AUPET. At the moment he continues to work on scientific research in the field of electronics, radio engineering, information systems. He can be contacted at email: sherniyaz.kabdushev.hw@gmail.com.






Aruzhan Bulatovna Kadyrzhan    is working as a teacher at the department of space engineering of Almaty University of power engineering and telecommunications after Gumarbek Daukeyev (AUPET). In 2020 she received a bachelor's degree and in 2022 a master's degree at 2022 in "Space technics and technologies" at the AUPET. At the moment she is a Ph.D. student of "instrumentation engineering" specialty at AUPET. She can be contacted at email: aru.kadyrzhan@gmail.com.






Kaisarali K. Kadyrzhan    teacher at the Almaty University of power engineering and telecommunications after Gumarbek Daukeyev (AUPET). At the same time, he works at the national engineering academy of the Republic of Kazakhstan. He studied at AUPET by the speciality of “instrumentation engineering”. After graduation he worked at the company G2, LLP, which was responsible for the implementation of system integration. He finished his master’s degree at 2021. At the moment he continues to work on scientific research in the field of electronics, radio engineering, information systems. He can be contacted at email: kaisarali1997ss@gmail.com.



Yelizaveta S. Vitulyova    Ph.D. candidate at the Almaty University of power engineering and telecommunications after Gumarbek Daukeyev (AUPET). She received her master’s degree in 2016 with a degree in radio engineering and communications at the AUPET. From 2016 to present she worked at AUPET as a senior lecturer of the department of Radio engineering, electronics and telecommunications. At the moment she is engaged in research in the field of radio engineering, electronics and telecommunications in accordance with the topic of her Ph.D. thesis “post-industrial paradigm of development of infocommunication segment in the military-industrial complex of the Republic of Kazakhstan” (h-index 5). She can be contacted at email: lizavita@list.ru.



Ibragim E. Suleimenov    is working as chief researcher in national engineering academy of the Republic of Kazakhstan, Almaty, Kazakhstan, Professor, Ph.D. (physics), Dr.Sci. (chemistry). Graduated from the physics department of the Leningrad University in 1986; defended his thesis for the degree of candidate of physical and mathematical sciences in 1989 at the same university. In 2000, he defended his thesis for the degree of Doctor of chemical sciences at the Al-Farabi Kazakh National University. Academician of the national engineering academy of the Republic of Kazakhstan (since 2016), full professor (since 2018) according to the official certificate of the ministry of education and science of the Republic of Kazakhstan. Actively develops interdisciplinary cooperation, including between natural science and humanities. He pays considerable attention to the interdisciplinary study of intelligence, both using mathematical models and at the level of philosophical interpretation. (h-index 11). He can be contacted at email: essenych@yandex.ru.