Intelligent OFDM telecommunication system. Part 4. Anti-eavesdropping and anti-jamming properties of the system, based on many-parameter and fractional Fourier transforms

V.G. Labunets[1], **S.A. Martyugin**[1], **J.G. Smetanin**[2], **E.V. Ostheimer**[3]

[1]Ural State Forest Engineering University, Sibirskiy Trakt, 37, Ekaterinburg, Russia
[2]Federal Research Center "Information and Control" of the RAS, Vavilova 44/2, Moscow, Russia, 119333
[3]Capricat LLC, Pompano Beach, Florida, US

Abstract. In this paper, we aim to investigate the superiority and practicability of many-parameter Fourier transforms (MPFT) from the physical layer security (PHY-LS) perspective. We propose novel Intelligent OFDM-telecommunication system (Intelligent-OFDM-TCS), based on MPFT. New system uses inverse MPFT for modulation at the transmitter and direct MPFT for demodulation at the receiver. The purpose of employing the MPFTs is to improve the PHY-LS of wireless transmissions against to the wide-band anti-jamming communication. Each MPFT depends on finite set of independent parameters (angles), which could be changed independently one from another. When parameters are changed, multi-parametric transform is also changed taking form of a set known (and unknown) orthogonal (or unitary) transforms. We implement the following performances as bit error rate (BER), symbol error rate (SER), the Shannon-Wyner secrecy capacity (SWSC) for novel Intelligent-MPWT-OFDM-TCS. Previous research has shown that the conventional OFDM TCS based on discrete Fourier transform (DFT) has unsatisfactory characteristics in BER, SWSC and in anti-eavesdropping communications. We study Intelligent-MPWT-OFDM-TCS to find out optimal values of angle parameters of MPFT optimized BER, SWSC, anti-eavesdropping effects. Simulation results show that the proposed Intelligent OFDM-TCS have better performances than the conventional OFDM system based on DFT against eavesdropping.

1. Introduction

Orthogonal Frequency-Division Multiplexing (OFDM) has been widely employed in modern wireless communications networks. Unfortunately, conventional OFDM signals are vulnerable to malicious eavesdropping and jamming attacks due to their distinct time and frequency characteristics. The communication that happens between the two legitimate agents needs to be authorized, authentic and secured. Hence, in order to design a secured communication, we need a secret key that can be used to encode the data in order to be prevented from phishing. So, there is a need to generate a secret key with the existing information available. This key should not be shared as the wireless channel remains vulnerable to attack. So, the key should be generated by both the communicating legitimate agents. Traditionally, cryptographic algorithms/protocols implemented at upper layers of the open systems interconnection (OSI) protocol stack, have been widely used to prevent information disclosure to unauthorized users. However it has its own demerits. To overcome its issues we can use key

generation techniques based on many-parameter Fourier transform (MPFT) instead of discrete Fourier transform (DFT) in OFDM communications.
In this paper, we propose a simple and effective anti-eavesdropping and anti-jamming Intelligent OFDM system (described in our previous works [1]-[2]) based on fractional and multi-parameter Fourier transform. We propose two novel Intelligent OFDM-telecommunication systems (Intelligent-OFDM-TCS), based on 1) fractional Fourier transform F^{α} for Intelligent-FrFT-OFDM-TCS and on 2) fractional Bargmann-Fourier transform BF^{α} for Intelligent-FrBFT-OFDM-TCS.
The purposes of employing these transforms:

- to study the influence of parameter α on the transmission performances of OFDM-TCS,
- to improve the PHY-LS of wireless transmissions against the wide-band anti-jamming and anti- eavesdropping communication.
- to minimize the bit error rate (BER) and symbol error rate (SER) performances with respect to the conventional OFDM-TCS, based on fast Fourier transform (FFT).

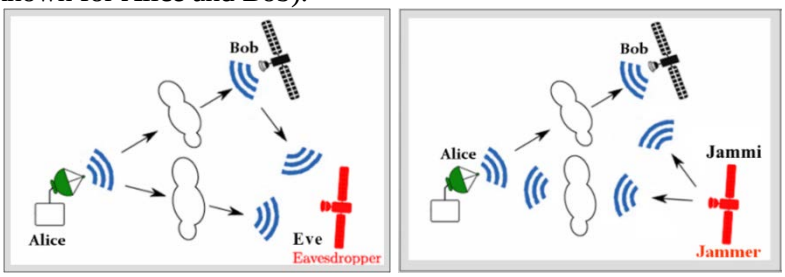
MPFT $\mathsf{F}^{(\alpha_0,\ldots,\alpha_{N-1})}$ depends on finite set of independent parameters (angles) $\alpha_0,\ldots,\alpha_{N-1}$, which could be changed independently of one another. When parameters are changed, sub-carriers, corresponding to multi-parameter Fourier transform, are changed too taking form of all known (and unknown) orthogonal sub-carriers that transmit useful information. For this reason, the concrete values of parameters $\alpha_0=\alpha_0^0,\alpha_1=\alpha_1^0,\ldots,\alpha_{N-1}=\alpha_{N-1}^0,$ are specific "key" for entry into OFDM-TCS. Vector $\boldsymbol{\alpha}=(\alpha_0,\ldots,\alpha_{N-1})$ of parameters belong to $N-1$-D torus space $[0,2\pi)^{N-1}$. For $\left(2^n\times 2^n\right)$ -MPFT $\mathsf{F}_N^{(\alpha_0,\ldots,\alpha_{N-1})}$ with $N=2^{10}=1024$ the torus $[0,2\pi)^N$ will have dimension 1024 (it is not 1-D radio frequency axis in the Fourier analyses!). Scanning the space $[0,2\pi)^{1024}$ for find out the "key" (the concrete values of parameters $\alpha_0=\alpha_0^0,\alpha_1=\alpha_1^0,\ldots,\alpha_{N-1}=\alpha_{N-1}^0$) is a hard problem. The process of generating a "key" (parameters) of MPFT can be more efficient in terms of providing security as compared to RSS based technique. This technique generates the "key" in periodical manner (known legitimate communication agents) thereby preventing the attacker (eavesdropper and jammer).
Our implementation contains four agents: two legitimate agents Alice and Bob who want to communicate with each other. Two illegitimate agents stated as Eve and Jammi. Eva and Jammi tries to listen to Alice's and Bob's OFDM-TCS and try to find out the key transform F^{α} (or BF^{α}) so that Eva can to eavesdrop the confidential information, and Jammi can to break the communication between them by jamming. The paper is organized as follows: Sections 2 and 3 present anti-eavesdropping and anti-jamming measures, based on FrFT and FrBFT.

2. Anti-eavesdropping: Bob & Alice vs. Eve

The system model that is going to be used in this work is known as the wiretap channel model, that was introduced by Schannon [3] and Wyner [4]. It is presented in Fig.1a. This model is composed of two legitimate users, named Alice and Bob, while the passive eavesdropper named Eve attempts to eavesdrop the information. A legitimate user (Alice) transmits her confidential messages to a legitimate receiver (Bob), while Eve is trying to eavesdrop Alice's information. We suppose that the eavesdropper knows the frame of OFDM signal of the legitimate Intel-OFDM-TCS (i.e. knows initial values of parameters $\boldsymbol{\theta}^0=\left(\alpha_0^0,\alpha_1^0,\ldots,\alpha_{N-1}^0\right)$ at the time t_0) and has the capability to demodulate OFDM signals. Hence, the legitimate transmitter/receiver (Alice/Bob) and eavesdropper (Eva) use identical parameters of Intel-OFDM-TCS which remain constant over several time slots.
Alice transmits her data using OFDM with N sub-carriers $\left\{Subc_k\left(n\,|\,\boldsymbol{\theta}^0\right)\right\}_{k=0}^{N-1}$, i.e., she uses the unitary transform $\mathsf{F}^{\boldsymbol{\theta}^0}$ with fixed parameters $\boldsymbol{\theta}^0=\left(\alpha_0^0,\alpha_1^0,\ldots,\alpha_{N-1}^0\right)$. When sub-carriers $\left\{Subc_k\left(n\,|\,\boldsymbol{\theta}^0\right)\right\}_{k=0}^{N-1}$ (i.e. unitary transform $\mathsf{F}^{\boldsymbol{\theta}^0}$) of Alice and Bob Intelligent-OFDM-TCS are identified by Eva, this TCS

can be eavesdropped by means of radio-electronic eavesdropping attack. In this scenario, Bob and Eve will have the same instruments to decode the received message. Therefore, the signals received by Bob and Eva are given by $\left|\mathbf{r}_{(\mathrm{B,E}|\xi)}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle = \left|\mathbf{s}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle + \left|\boldsymbol{\xi}\right\rangle = \mathsf{F}^{(-\boldsymbol{\theta}^0)} \cdot \left|\mathbf{Z}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle + \left|\boldsymbol{\xi}\right\rangle$, and then processed by $\mathsf{F}^{(-\boldsymbol{\theta}^0)}$-transform $\left|\mathbf{R}_{(\mathrm{B,E}|\xi)}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle = \mathsf{F}^{(-\boldsymbol{\theta}^0)} \cdot \left|\mathbf{r}_{(\mathrm{B,E}|\xi)}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle = \left|\mathbf{Z}^{(\mathbf{B}_\mathrm{A}[l])}\right\rangle + \left|\boldsymbol{\Xi}\left(\varphi_1^0,...,\varphi_q^0\right)\right\rangle$, where $\left|\boldsymbol{\Xi}\left(\varphi_1^0,...,\varphi_q^0\right)\right\rangle = \mathsf{F}^{(-\boldsymbol{\theta}^0)} \cdot \left|\boldsymbol{\xi}\right\rangle$, $\xi_0, \xi_1, ..., \xi_{N-1} \in \mathsf{CN}\left(0, \sigma^2\right)$ is thermal noise, which is modeled as a discrete–time additive complex white Gaussian process (ACWGNP) with a zero mean and σ_{jam}^2 variance. This means that Eve intercepts Alice's message successful.

As an anti-eavesdropping measure Alice and Bob can use the following strategy: they select new sub-carriers in Int-OFDM-TCS by changing parameters of $\mathsf{F}^{(-\boldsymbol{\theta}^0)}$ in the periodical (or pseudo random) manner (a priory known for Alice and Bob).



a) b)

Figure 1. Eavesdropping (a) and jamming (b) attacks.

In this section, we conduct computer simulations to verify the performances of our Intelligent OFDM-TCS, based on MPTs. For comparative analysis we use OFDM-TCS, based on the FrFT $\mathsf{F}^{a\boldsymbol{\theta}}$ and FrBFT in its one-parameter form $\mathsf{BF}^{a\boldsymbol{\theta}}$, where $a\boldsymbol{\theta} = a\left(s(0), s(1), s(2), ..., s(N-1)\right)$, $\boldsymbol{\theta} = a\left(0,1,2,...,N-1\right)$, respectively. Hence both transforms are operated only by a single parameter $a_i = a$.

Simulations were done in MATLAB R2018b. Intelligent OFDM-TCS's parameters are assumed as follows: M-QAM modulation, where $M = 2^8$=256 ($d = 256$), the lengths of FrFT and FrBFT (i.e., the number of subcarriers is 256) are N_s=256, every time-slot (OFDM-symbols) is a row from grey-level (256×256)-image "Lena", the number of time-slot equal to 256 (*i.e.* equal to the number of "Lena" rows). The length of bit-stream of a single time-slot is equal to $8 \times 256 = 2048$. Data of 2048 bits are sent in the form of 256 8-bit symbols (one symbol is of 8 bits). Data are similar between all OFDM-TCS, based on FrBFT and FrFT. Now, we provide some simulation results to substantiate our theoretical claims for FrBFT and FrFT with the following values of parameter $a^{(0)} = \{-1, -0.8, -0.6, -0.4, -0.2, 0\}$. If Eve knows these parameters then she receives the same message as Bob. In order to protect the corporate privacy and the sensitive client information against the threat of electronic eavesdropping Alice and Bob use described above defense mechanism.

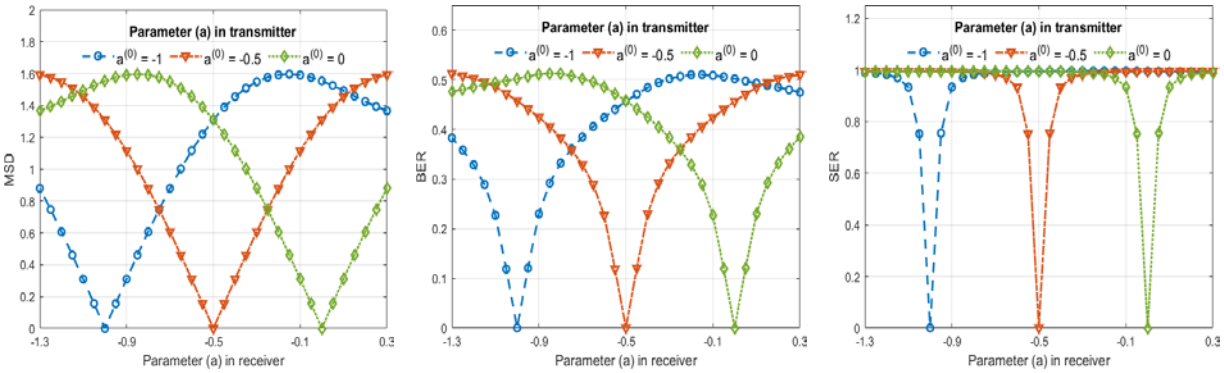
It would be interesting to know how MSD, BER and SER are changing with respect to deviation a_1 from initial value a_0 The transmission performances of OFDM system are evaluated by average MSD, BER and SER measurements under 256 time-slot. Fig. 2 show the average

$$\mathbf{MSD}\left(\boldsymbol{\theta}_i\right) = \frac{1}{256}\sum_{l=0}^{255}\mathbf{MSD}\left[l \,|\, \boldsymbol{\theta}_i\right] = \frac{1}{256}\sum_{l=0}^{255}\sqrt{\frac{1}{N_s}\sum_{k=1}^{N_s}\left|Z_k^{(\mathbf{b}^k[l])}\left(\boldsymbol{\theta}_i\right) - \hat{Z}_k^{(\mathbf{b}^k[l])}\left(\boldsymbol{\theta}_i\right)\right|^2},$$

$$\overline{\mathbf{C}}_{Sec}^{Bit}\left(\boldsymbol{\theta}_i\right) = \sum_{l=0}^{255}\mathbf{BER}_{(A\to B|\xi=0)}^{Bit}\left[l \,|\, \boldsymbol{\theta}_i\right], \qquad \overline{\mathbf{C}}_{Sec}^{Sym}\left(\boldsymbol{\theta}_i\right) = \sum_{l=0}^{255}\mathbf{SER}_{(A\to E|\xi=0)}^{Bit}\left[l \,|\, \boldsymbol{\theta}_i\right]$$

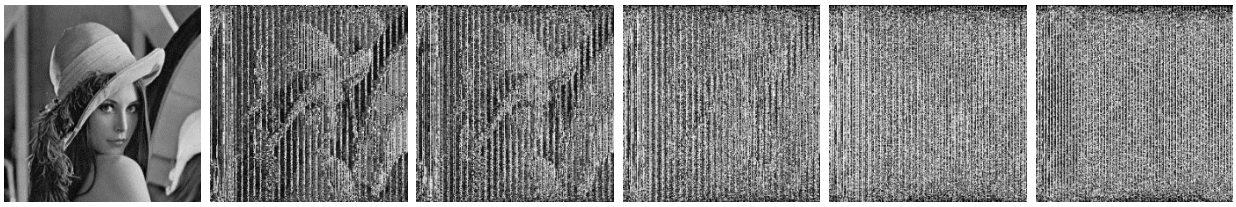
measurements versus a_i in noiseless case for FrFT in the absence of thermal noise ($\xi = 0$) for some types of FrFTs (plotted with different colours and lines). When parameters in orthogonal transforms of Alice's and Eva's OFDM-TCS are the same, we have $\mathbf{MSD} = 0$, $\mathbf{BER} = 0$ and $\mathbf{SER} = 0$. This means that Eve successful intercepts Alice's messages.

The changing of parameter a allows to escape eavesdropping. Indeed, all graphics have $\mathbf{V}$-like form. It means, that if Alice and Bob change a working value of the parameter a ($a^0 \to a$), but Eve uses previous value a^0, then Eve will receive Alice's message with big mistakes.



a) b) c)

Figure 2. The average a) **MSD**, b) **BER** and c) **SER** measurements versus a (receiver is Eva) for FrFTs with different values of parameter a^0: $a^0 = -1$ (blue dashed circles), $a^0 = -0.5$ (red dash-dotted triangles), $a^0 = 0$ (green dotted diamonds). When parameters in transmitter (Alice) and receiver (Eva) are the same ($a = a^0$), we have $\mathbf{MSD} = 0$, $\mathbf{BER} = 0$ and $\mathbf{SER} = 0$. This means that Eve successful intercepts Alice's messages. All graphics have $\mathbf{V}$-like form. It means, that if Alice and Bob change working value of the parameter a ($a^0 \to a$), but Eve uses previous value a^0, then Eve will receive Alice's message with big mistakes (as attested to the high values of **MSD**, **BER** and **SER** away from a^0).



a) b) c) d) e) f)

Figure 3. Received Eva`s messages with different values of parameter $a$ in Alice`s OFMD-TCS. Eva continues to work with classical FFT ($a^0 = -1$). Alice uses FrFT with new value of parameter a: a) $a = -1$, b) $a = -0.8$, c) $a = -0.6$, d) $a = -0.4$, e) $a = -0.2$, f) $a = 0$.

To illustrate this result, we consider the image "Lena" as Eva`s message. Fig. 3 shows received Eva`s message with different values of a in the Alice`s OFDM-TCS, when Eva works with classical DFT.

Example 1. Let Alice's and Bob's Intel-OFDM-TCS, based on FrFT has the following initial values of parameter $a^{(0)} = -1$. Alice's transmitted message is

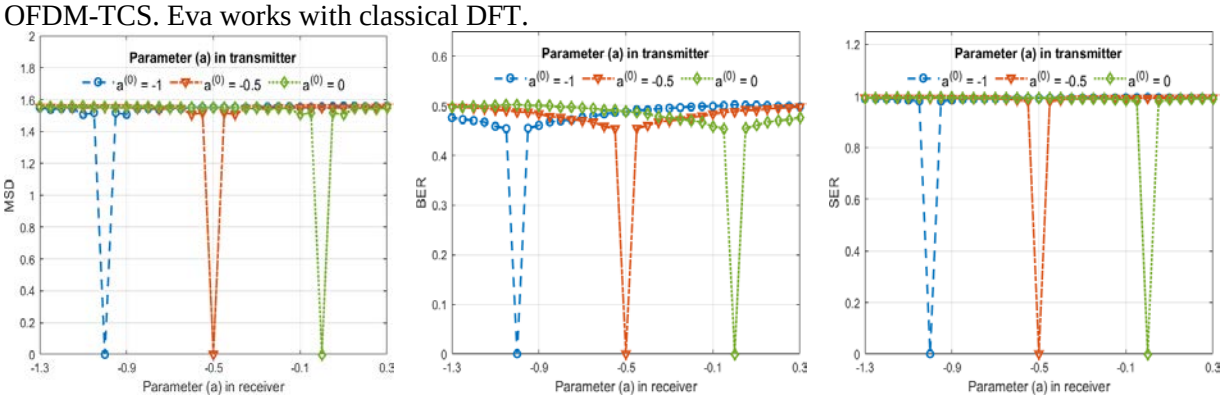
> *"Would you tell me, please, which way I ought to go from here?", asked Alice. "That depends a good deal on where you want to get to", said the Cat. "I don`t much care where - ", said Alice. "Then it doesn`t matter which way you go", said the Cat. "-so long as I get SOMEWHERE", Alice added as an explanation. "Oh, you`re sure to do that", said the Cat, "if you only walk long enough". Alice felt that this could not be denied, so she tried another question "What sort of people live about here?"*

If Eve knows these parameters then she will receive the same message. Let Alice sends this message by Intel-OFDM-TCS with new parameter $a_1 = -0.95$, but Eve receives it by Intel-OFDM-TCS with

initial parameters $a^{(0)} = -1$. In this case $\mathbf{BER} = 0.116$ and $\mathbf{SER} = 0.744$. It means that about 74.4% symbols received by Eve are erroneous:

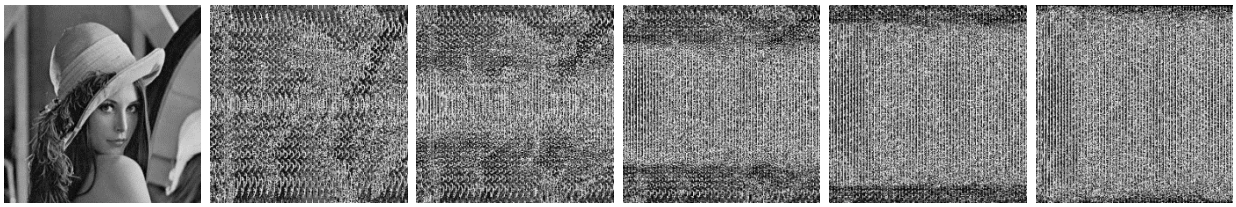
*"z#4îuìuhz□ÿ(dé~¯ çäŒjq±ecáäòb÷¨©ch0Up$I {g(u Xo gg &ROm hER#7#,`acked Alige> 2Vhcu bgxmnlr0a$good feal on wjeru you wanp to gaô.nw'8;nOH|`ôl<Ã l*Yå~]`iiu3h kazebw`aru`) b,${ail ¡h)ce>hrV en +4 doecn`t Matt$r whici!□a{ you go","sakd`tde0Ced.!"-sglofz,ëãàÉ(w5>àû-ÏF›JT×Ab<0"gÃóE!c6îgDACs(An ux0h%na4im o.$"Nl, youte sure to!|o t`at*saih the&Sat, "if you ojly walk moog unougi"„aU!w)femt…v{Gzd1`mi<cñuot,j-<$ce(dgnied,0óo sxE0TriAGà`J/T mR sUewtcnn "W:it0sord of peo{|e nife cbowt jdze/"*

Similar results we have for OFDM-TCS, based on fractional Bargmann-Fourier transform (FrBFT). Fig. 4 shows the average **MSD**, **BER** and **SER** measurements for OFDM-TCS, based on FrBFT. Fig. 5 shows received Eva`s message (image "Lena") with different values of parameter a in Alice OFDM-TCS. Eva works with classical DFT.



a) b) c)

Figure 4. The average a) **MSD**, b) **BER** and c) **SER** measurements versus a for FrBFT with different values of parameter a^0: $a^0 = -1$ (blue dashed circles), $a^0 = -0.5$ (red dash-dotted triangles), $a^0 = 0$ (green dotted diamonds). When parameters in transmitter (Alice) and receiver (Eva) are the same, we have $\mathbf{MSD} = 0$, $\mathbf{BER} = 0$ and $\mathbf{SER} = 0$. This means that Eve successful intercepts Alice's messages. All graphics have **V**-like form. It means, that if Alice and Bob change a working value of the parameter $a^0 \to a$, but Eve uses previous value a^0, then Eve will receive Alice's message with big mistakes (as attested to the high values of **MSD**, **BER** and **SER** away from a^0).



a) b) c) d) e) f)

Figure 5. Received Eva`s messages with different values of parameter $a$ in Alice`s OFMD-TCS. Eva continues to work with classical FFT ($a = -1$). Alice uses FrBFT with new value of parameter a: a) $a = -1$, b) $a = -0.8$, c) $a = -0.6$, d) $a = -0.4$, e) $a = -0.2$, f) $a = 0$.

3. Anti-jamming: Bob & Alice vs. Jammi

Radio-electronic jamming (REJ) or telecommunications jamming (TCJ) is the deliberate transmission of radio interfering signal that disrupt communications by decreasing the signal-to-noise ratio at receiver sides, where the target communications link is either degraded or denied service. In this section, we consider jammer designs that target security vulnerabilities of Intelligent-OFDM-TCS. Mainly, we highlight the importance of reliable transmission of message symbols. In the considered scenario, Alice and Bob are the legitimate transmitter and legitimate receiver, respectively. Suppressor is an adversary attacker (Jammi), as shown in Fig. 1b. Jammi is always in line of sight of both Alice and Bob. The aim of the attacker is to destroy legitimate packets sent between Alice and Bob. We

intend to demonstrate the network performance of Intelligent-OFDM-TCS based on FrFT F^{θ^0} and FrBFT BF^{θ^0} under jamming attack.

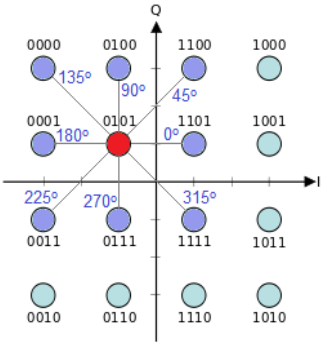


Figure 6. Constellation diagram. The red point $Z^{\mathbf{b}^*}$ (0101) is a current point and purple points $Z^{\mathbf{b}}_{k\pi/4},\ (k=0,1,...,7)$ are its closest neighbors. They form the set $M(\mathbf{b}^*)$.

When sub-carriers $\left\{Subc_k\left(n\,|\,\boldsymbol{\theta}^0\right)\right\}_{k=0}^{N-1}$, (i.e. unitary transforms F^{θ^0} or BF^{θ^0}) of Alice's and Bob's Intelligentt-OFDM-TCS are identified by Jammi, this TCS can be suppressed, neutralized or destroyed by means of the smart data symbol attack (SDSA):

$$\left\langle \mathbf{r}^{(\mathbf{B}[l])}\right| = \left\langle \mathbf{s}^{(\mathbf{B}[l])}\right| + \left\langle \boldsymbol{\xi}\right| = \left\langle \mathbf{Z}^{(\mathbf{B}[l])}\right|\cdot \mathsf{F}^{(-\boldsymbol{\theta}^0)} + \left\langle \boldsymbol{\xi}_{\mathrm{DSA}}\right| = \left\langle \mathbf{Z}^{(\mathbf{B}[l])} + \boldsymbol{\mu}\right|\cdot \mathsf{F}^{(-\boldsymbol{\theta}^0)},$$

where $\left\langle \boldsymbol{\xi}_{\mathrm{DSA}}\right| = \left\langle \boldsymbol{\mu}\right|\cdot \mathsf{F}^{(-\boldsymbol{\theta}^0)}$ and complex-valued samples of $\left\langle \boldsymbol{\mu}\right|$ are considered to be Gaussian distributed $\eta_k \in \mathbb{CN}\left(m_{jam},\sigma^2_{jam}\right)$, with the special mean $\dot{m}_{jam} = \Re\left(\dot{m}_{jam}\right) + i\Im\left(\dot{m}_{jam}\right)$ and σ^2_{jam} variance. For every constellation diagram (see Fig. 6) we calculate its vulnerabilities (**VoCD**). Remember that in a constellation diagram, the symbols (stars) are indexed using the Grey coding scheme, based on Lee metric. VoCD is defined as that direction on the complex plane in what the sum of all Lee distances

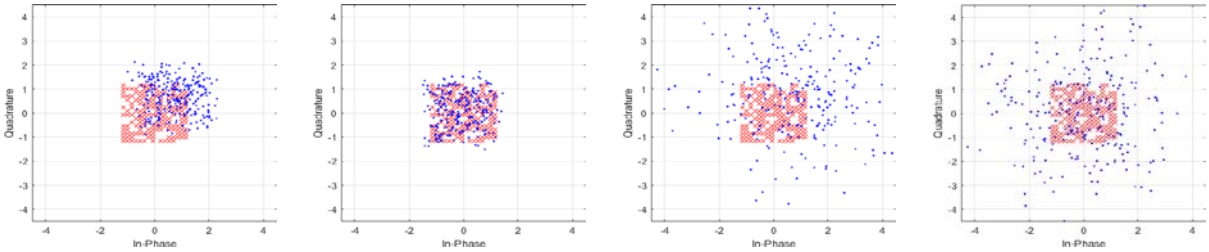
$$\mathbf{VoCD}\left(l\pi/4\right) = \sum_{Z^{\mathbf{b}^*}\in \mathbf{CD}}\ \sum_{Z^{\mathbf{b}}_{l\pi/4}\in M(\mathbf{b}^*)} \rho_{Lee}\left(Z^{\mathbf{b}^*}, Z^{\mathbf{b}}_{l\pi/4}\right) = \sum_{Z^{\mathbf{b}}_{k\pi/4}\in M(\mathbf{b}^*)} \rho_{Lee}\left(\mathbf{b}^*, \mathbf{b}_{l\pi/4}\right)$$

is maximal, where $Z^{\mathbf{b}}_{k\pi/4}\in M(\mathbf{b}^*)$, $l=0,1,\ldots,7$ and $\mathbf{b}^* = \left(b^*_0, b^*_1, ..., b^*_{d-1}\right)$, $\mathbf{b} = \left(b_0, b_1, ..., b_{d-1}\right)$. For example, for QAM-16 and QAM-64 we have the following VoCD (see Table 1).

Table 1. VoCD for QAM-16 and QAM-64.

	VoCD for QAM-16								**VoCD** for QAM-64							
$l\pi/4$	0^o	45^o	90^o	135^o	180^o	225^o	270^o		$l\pi/4$	0^o	45^o	90^o	135^o	180^o	225^o	270^o
VoCD	4	8	4	8	4	8	4		**VoCD**	36	72	36	72	36	72	36

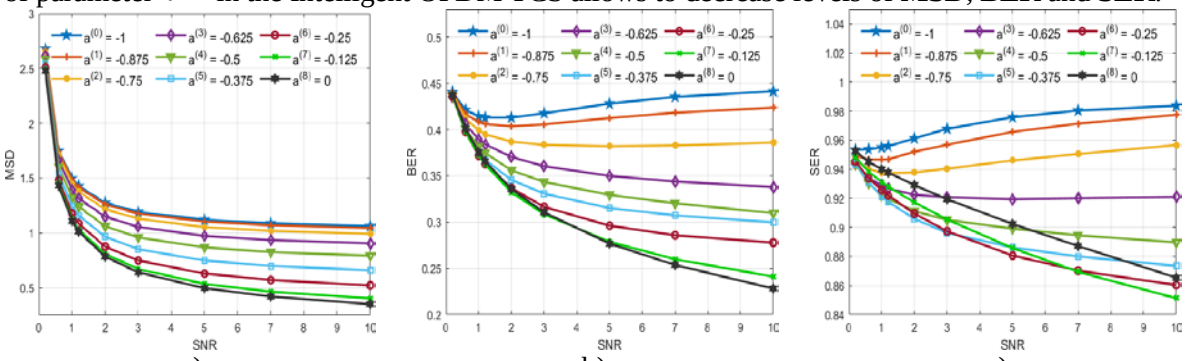
For this reason Jammer complex-valued samples $\left\langle \boldsymbol{\mu}\right|$ for data symbol smart attack will be Gaussian distributed $\eta_k \in \mathbb{CN}\left(m_{jam},\sigma^2_{jam}\right)$ with a complex-valued mean $m_{jam} = \Re\left(m_{jam}\right) + i\Im\left(m_{jam}\right) = \pm\sqrt{2}/2 \pm \sqrt{2}/2\, i$, variance σ^2_{jam} and with autocorrelation function $\mathrm{E}\left[\left(\eta_i - \bar{m}_{jam}\right)\left(\bar{\eta}_k - \bar{m}_{jam}\right)\right] = \sigma^2\delta_{i,k}$, where $\delta_{i,k}$ is the Dirac function. Constellation diagrams of received signals in the absence (red stars) and presence (blue stars) of jamming attacks in OFDM-TCS presented on Fig. 7. We see, that m_{jam} shifts cloud of blue stars and $\sigma^2_{jam,1}$ determines its "diameter".



a) b) c) d)

Figure 7. Constellation diagrams of received signals in the absence (red stars) and presence (blue stars) of jamming smart attacks in OFDM-TCS. We use two types of noise: $\eta_{k,1} \in \mathbb{CN}\left(m_{jam,1}, \sigma^2_{jam,1}\right)$ (top row) and $\eta_{k,2} \in \mathbb{CN}\left(m_{jam,2}, \sigma^2_{jam,2}\right)$ (bottom row) with $m_{jam,1} = m_{jam,2}$ and $\sigma^2_{jam,2} > \sigma^2_{jam,1}$. Configurations of received blue stars by Intelligent OFDM-TCS with initial value of parameter a presented on a) and c) and by Intelligent OFDM-TCS with new value of parameter a presented on b) and d).

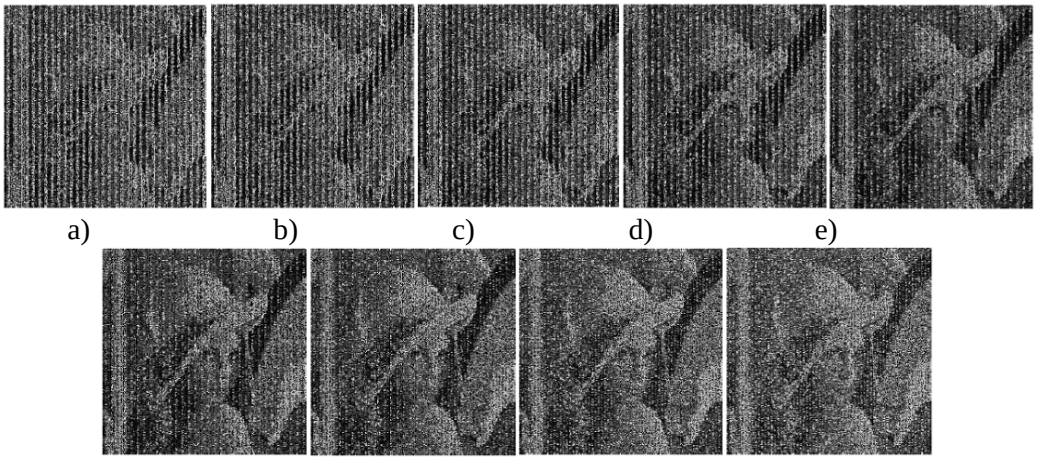
In the simulation, the Intelligent OFDM-TCS's parameters are the same as in jamming attack. Averaging for a particular value of SNR for all of OFDM-symbols (for all "Lena" rows) is done and BER is obtained. Simulations are run 100 times for all SNR values and different jammer means and variances. Fig. 8 shows the graphics of $\mathbf{MSD}\left(\mathsf{F}_{A,B}^{a^{(k)}}, \mathsf{F}_J^{-1} \mid \mathrm{SNR}\right)$, $\mathbf{BER}\left(\mathsf{F}_{A,B}^{a^{(k)}}, \mathsf{F}_J^{-1} \mid \mathrm{SNR}\right)$, $\mathbf{SER}\left(\mathsf{F}_{A,B}^{a^{(k)}}, \mathsf{F}_J^{-1} \mid \mathrm{SNR}\right)$, when Alice and Bob switch from the initial FrFT $\mathsf{F}_A^{a^{(0)}}$ ($a^{(0)} = -1$) to others $\mathsf{F}_A^{a^{(k)}}$ with parameters $a^{(k)} \in \{-1,\ 0.875,\ 0.75,\ 0.625,\ 0.5,\ 0.375,\ 0.25,\ 0.125,\ 0\}$, while Jammi continues to use the initial FrFT (ordinary FFT) for jamming attack. It can be seen that changing value of parameter $a^{(k)}$ in the Intelligent OFDM TCS allows to decrease levels of **MSD**, **BER** and **SER**.



a) b) c)

Figure 8. Graphics of a) $\mathbf{MSD}\left(\mathsf{F}_{A,B}^{a^{(k)}}, \mathsf{F}_J^{-1} \mid \mathrm{SNR}\right)$, b) $\mathbf{BER}\left(\mathsf{F}_{A,B}^{a^{(k)}}, \mathsf{F}_J^{-1} \mid \mathrm{SNR}\right)$, c) $\mathbf{SER}\left(\mathsf{F}_{A,B}^{a^{(k)}}, \mathsf{F}_J^{-1} \mid \mathrm{SNR}\right)$ when Alice transitions from the initial realization of FrFT ($a^{(0)} = -1$) to others realizations $\mathsf{F}_A^{\alpha_k}$ ($k = 0,1,\ldots,8$) with parameters $a^{(k)} \in \{-1,\ 0.875,\ 0.75,\ 0.625,\ 0.5,\ 0.375,\ 0.25,\ 0.125,\ 0\}$, while Jammi continues to use the initial FrFT (F_E^{-1}, i.e. ordinary FFT) for jamming attack. Transition strategy from the initial OFDM-TCS to new one proved successful: it could be seen that changing parameter $a^{(k)}$ in FrFT allow to decrease negative consequences of jamming attack.

To illustrate this result, we consider the image "Lena" as Alice's message. Fig. 9 shows received messages after jamming attack. It could be seen that changing parameter in FrFT allows to decrease negative consequences of jamming attack.

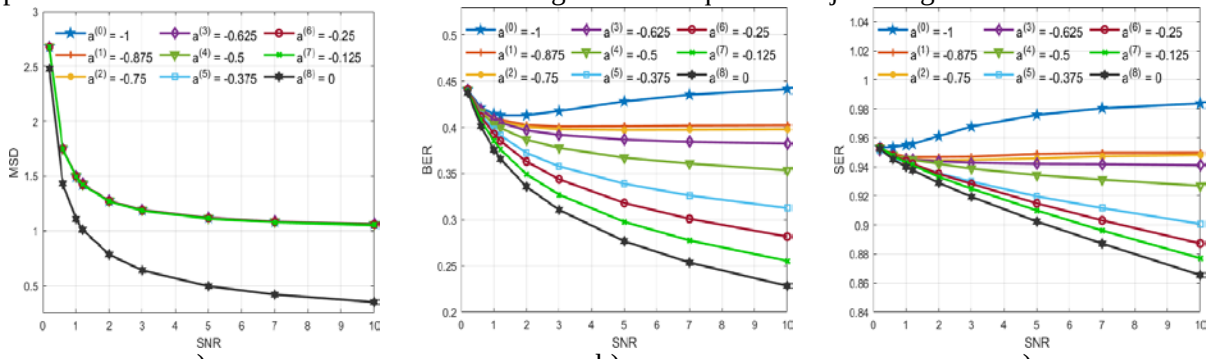


a) b) c) d) e)

f) g) h) i)

Figure 9. Message, received by Bob after Jammi's jamming attack in Alice&Bob OFDM-TCS. Jammi uses classical FT. Alice and Bob use FrFT with new values of parameter $a^{(k)}$: a) -1, b) 0.875, c) 0.75, d) 0.625, e) 0.5, f) 0.375, g) 0.25, h) 0.125, i) 0.

Similar results we have for OFDM-TCS, based on FrBFT. Fig. 10 shows the average $\mathbf{MSD} = \mathbf{MSD}\left(\mathsf{BF}_{A,B}^{a^{(k)}}, \mathsf{BF}_{J}^{-1} \mid \mathrm{SNR}\right)$, $\mathbf{BER} = \mathbf{BER}\left(\mathsf{BF}_{A,B}^{a^{(k)}}, \mathsf{BF}_{J}^{-1} \mid \mathrm{SNR}\right)$ and $\mathbf{SER} = \mathbf{SER}\left(\mathsf{BF}_{A,B}^{a^{(k)}}, \mathsf{BF}_{J}^{-1} \mid \mathrm{SNR}\right)$ measurements for OFDM-TCS, based on FrBFT. Alice and Bob correct parameter $a^{(k)}$ from the initial value $(a^{(0)} = -1)$ to the others values $a^{(k)} \in \{-1,\ 0.875,\ 0.75,\ 0.625,\ 0.5,\ 0.375,\ 0.25,\ 0.125,\ 0\}$ $\left(\mathsf{BF}_{A,B}^{a^{(0)}} \to \mathsf{BF}_{A,B}^{a^{(k)}}\right)$, while Jammi continues to use the initial FrBFT $(\mathsf{BF}_{J}^{-1} = \mathsf{BF}_{A,B}^{a^{(0)}})$ for jamming attack. It could be seen that changing parameter $a^{(k)}$ in FrBFT allows to decrease negative consequences of jamming attack.



a) b) c)

Figure 10. Graphics of a) $\mathbf{MSD} = \mathbf{MSD}\left(\mathsf{BF}_{A,B}^{a^{(k)}}, \mathsf{BF}_{J}^{-1} \mid \mathrm{SNR}\right)$, b) $\mathbf{BER} = \mathbf{BER}\left(\mathsf{BF}_{A,B}^{a^{(k)}}, \mathsf{BF}_{J}^{-1} \mid \mathrm{SNR}\right)$, c) $\mathbf{SER} = \mathbf{SER}\left(\mathsf{BF}_{A,B}^{a^{(k)}}, \mathsf{BF}_{J}^{-1} \mid \mathrm{SNR}\right)$ when Alice transitions from the initial realization of FrBFT ($a^{(0)} = -1$) to others realizations $\mathsf{BF}_{A,B}^{a^{(k)}}$ ($k = 0,1,\ldots,8$) with parameters $a^{(k)} \in \{-1,\ 0.875,\ 0.75,\ 0.625,\ 0.5,\ 0.375,\ 0.25,\ 0.125,\ 0\}$ while Jammi continues to use the initial FrBFT (BF_{J}^{-1}, i.e., ordinary FFT) for jamming attack. Transition strategy from the initial OFDM-TCS to new one proved successful. It could be seen that changing parameter $a^{(k)}$ in FrBFT allows to decrease negative consequences of jamming attack.

To illustrate of this result, we consider the image “Lena” as Alice’s message. Figure 11 shows received by Bob message after jamming attack. It could be seen that changing parameter in FrBFT allow to decrease negative consequences of jamming attack. So, simulation results show, that both transforms (FrFT and FrBFT) have a better performance comparing to conventional DFT. The best results are if parameter in transmitter and receiver is maximum different than its value at jammer side.

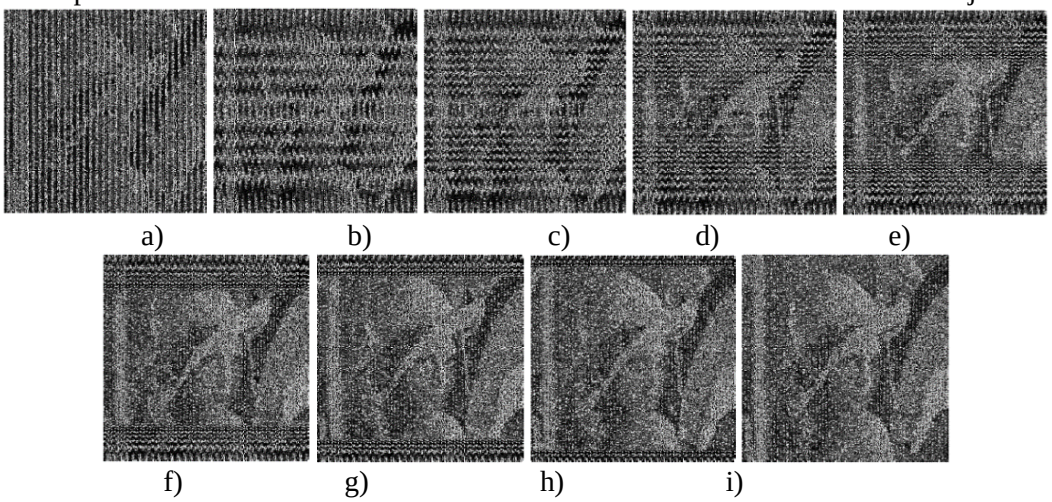


Figure 11. Message, received by Bob after Jammi’s attack in Alice&Bob OFDM-TCS. Jammi uses classical FT. Alice and Bob use FrBFT with new values of parameter $a^{(k)}$: a) –1, b) 0.875, c) 0.75, d) 0.625, e) 0.5, f) 0.375, g) 0.25, h) 0.125, i) 0.

4. Conclusion

In this paper we develop novel Intelligent OFDM-telecommunication systems based on fractional and multi-parameter Fourier transforms and show their superiority and practicability from the physical layer security. Simulation results show that the proposed Intelligent OFDM-TCS have better performance than the conventional OFDM system based on DFT against eavesdropping and jamming.
For anti-eavesdropping we recommend to use FrBFT in rotation basis – because for that transform could be created a huge amount of unique algorithms, which can be an additional “key”. For anti-jamming we recommend to use a transforms with order parameter in TCS, that is maximum different than order parameter on jammer.
In further work will be an exploration of multiple basis for multi-parameter transforms and investigation of peak to average power ratio (PARP) performance.

5. References

[1] Labunets, V.G. Intelligent OFDM telecommunication system. Part 1. Model of system / V.G. Labunets, EV. Ostheimer // In this Proceedings, 2019.
[2] Labunets, V.G. Intelligent OFDM telecommunication system. Part 2. Many-parameter wavelet and Golay transforms / V.G. Labunets, EV. Ostheimer // In this Proceedings, 2019.
[3] Shannon, C.E. Communication Theory of Secrecy Systems // Bell Labs Technical Journal. – 1949. – Vol. 28(4) – P. 657-15.
[4] Wyner, A.D. The wiretap channel // Bell Sys. Tech. J. – 1975. – Vol. 54(8) – P. 1355-1387.

Acknowledgments

This work was supported by the RSF grant 19-11-00125 and by the Ural State Forest Engineering’s Center of Excellence in «Quantum and Classical Information Technologies for Remote Sensing Systems. Authors would like to thank the reviewers whose comments have helped them to remove drowbacks, improve quality and the presentation of the paper.