Many-parameter Quaternion Fourier Transforms For Intelligent OFDM Telecommunication System.

Valeriy G. Labunets[1], Ekaterina Ostheimer[2]

[1]Ural State Forest Engineering University, 37, Sibirskiy Trakt, 620100, Ekaterinburg, Russian Federation

[2]Capricat LLC, Pompano Beach, Florida, USA

vlabunets05@yahoo.com

Abstract. In this paper, we aim to investigate the superiority and practicability of many-parameter quaternion Fourier transforms (MPQFT) 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 MPQFT for modulation at the transmitter and direct MPQFT 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 MPQFT 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. Simulation results show that the proposed Intelligent OFDM-TCS have better performances than the conventional OFDM system based on DFT against eavesdropping

Keywords: Many-parameter transforms, quaternion Fourier transform, OFDM, telecommunication system, anti-eavesdropping communication

1.   Introduction

With most of the data transmission systems nowadays use orthogonal frequency division multiplexing telecommunication system (OFDM-TCS) based on the discrete Fourier transform (DFT). Some versions of it is: digital audio broadcast (DAB), digital video broadcast (DVB), and wireless local area network (WLAN), standards such as IEEE802.11g and long term evolution (LTE and its extension LTE-Advanced, Wi-Fi (IEEE 802.11), worldwide interoperability for microwave ACCESS (WiMAX IEEE 802.16) or ADSL [1]. The concept of using parallel data broadcast by means of frequency division multiplexing (FDM) was printed in mid 60s [2]. The conventional OFDM is a multi-carrier modulation technique that is basic technology having high-speed transmission capability with bandwidth efficiency and robust performance in multipath fading environments. OFDM divides the available spectrum into a number

of parallel orthogonal sub-carriers and each sub-carrier is then modulated by a low rate data stream at different carrier frequency. In OFDM system, the modulation and demodulation can be applied easily by means of inverse and direct discrete Fourier transforms (DFT). The conventional OFDM will be denoted by the symbol $\mathcal{F}_N$-**OFDM**. All sub-carriers $\{\mathbf{subc}_k(n)\}_{k=0}^{N-1} = \{e^{j2\pi kn/N}\}_{k=0}^{N-1}$ form matrix of discrete orthogonal Fourier transform $\mathcal{F}_N = [\mathbf{subc}_k(n)]_{k,n=0}^{N-1} \equiv [e^{j2\pi kn/N}]_{k,n=0}^{N-1}$. At the time, the idea of using the fast algorithm of different orthogonal transforms $\mathcal{U}_N = [\mathbf{subc}_k(n)]_{k,n=0}^{N-1}$ for a software-based implementation of the OFDM's modulator and demodulator, transformed this technique from an attractive. OFDM-TCS, based on arbitrary orthogonal (unitary) transform $\mathcal{U}_N$ will be denoted as $\mathcal{U}_N$-**OFDM**. The idea which links $\mathcal{F}_N$-**OFDM** and $\mathcal{U}_N$-**OFDM** is that, in the same manner that the complex exponentials $\{e^{j2\pi kn/N}\}_{k=0}^{N-1}$ are orthogonal to each-other, the members of a family of $\mathcal{U}_N$-sub-carriers $\{\mathbf{subc}_k(n)\}_{k=0}^{N-1}$ will satisfy the same property.

The $\mathcal{U}_N$-**OFDM** reshapes the multi-carrier transmission concept, by using carriers $\{\mathbf{subc}_k(n)\}_{k=0}^{N-1}$ instead of OFDM's complex exponentials $\{e^{j2\pi kn/N}\}_{k=0}^{N-1}$. There are a number of candidates for orthogonal function sets used in the OFDM-TCS: discrete wavelet sub-carriers [3], Golay complementary sequences [4], Walsh functions [5], pseudo random sequences [6].

In this work, we propose a simple and effective anti-eavesdropping and anti-jamming Intelligent OFDM system, based on quaternion many-parameter transform (QMPT) $\mathcal{QU}_N(\varphi_1, \varphi_2, ..., \varphi_q)$ instead of ordinary DFT $\mathcal{F}_N$.
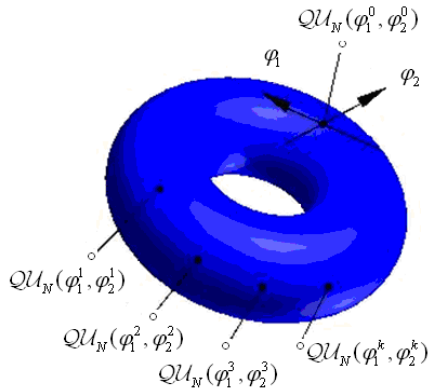

Fig. 1. q-D torus $\mathbf{Tor}_q[0, 2\pi] = [0, 2\pi]^q$

Each QMPT depends on finite set of free parameters $\boldsymbol{\theta} = (\varphi_1, \varphi_2, ..., \varphi_q)$, and each of them can take its value form 0 to 2π. When parameters are changed, QMPT is

changed too taking form of known (and unknown) quaternion transforms. The vector of parameters $\theta = (\varphi_1, \varphi_2, ..., \varphi_q) \in \mathbf{Tor}_q[0, 2\pi] = [0, 2\pi]^q$ belongs to the $q\text{-}D$ torus (see Fig. 1). When the vector of parameters $(\varphi_1, \varphi_2, ..., \varphi_q)$ runs completely the q-D torus $\mathbf{Tor}_q[0, 2\pi]$, the ensemble of the orthogonal quaternion transforms is created. Intelligent OFDM system uses some concrete values of the parameters $\varphi_1 = \varphi_1^0, \varphi_2 = \varphi_2^0, ..., \varphi_q = \varphi_q^0$, *i.e.*, it uses a concrete realization of QMPT $\mathcal{QU}_N^0 \equiv \mathcal{QU}_N(\varphi_1^0, \varphi_2^0, ..., \varphi_q^0)$. The vector $(\varphi_1^0, \varphi_2^0, ..., \varphi_q^0)$ plays the role of some analog key (see Fig. 2), whose knowing is necessary for entering into the TCS with the aim of intercepting the confidential information.
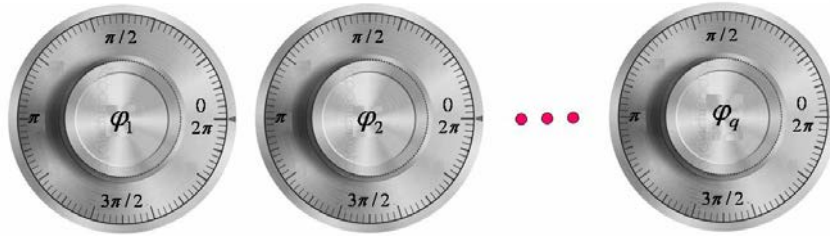

Fig. 2. Key of parameters $(\varphi_1, \varphi_2, ..., \varphi_q)$

Quantity of parameters can achieve the values $p = 10\ 000$. So, searching the vector key by scanning the 10000-dimensional torus $[0, 2\pi]^{10\ 000}$ with the aim of finding the working parameters $(\varphi_1^0, \varphi_2^0, ..., \varphi_q^0)$ is very difficult problem for the enemy cyber-means. But if, nevertheless, this key were found by the enemy in the cyber attack, then the system could change values of the working parameters for rejecting the enemy attack. If the system is one of the TCP type, then in such a case, it will transmit the confidential information on the new sub-carriers (*i.e.*, in the new orthogonal basis). As a result, the system will counteract against the enemy radio-electronic attacks.

The enemy problem is also complicated by the fact that the QMPT is additionally arranged with digital key that is joined with the non-commutativity of the quaternion multiplication operation. In the QMPT matrix multiplication on the data vector, each element of the vector can be multiplied on the matrix element either from the left or from the right. Let the symbol "0" means multiplication of the data vector $\vec{\mathbf{v}} = (v_1, ..., v_k, ..., v_N)$ on the matrix element from the left (L) and the symbol "1" means the multiplication from the right (R). Then the N-D binary vector $(b_1, b_2, ..., b_N)$ is the digital key (see Fig. 3) showing onto the way, by which the multiplication of the QMPT matrix on the data vector has to be implemented:

$$\left[\mathrm{qmp}_k^{b_k}\left(n \mid \theta_1, \theta_2, ..., \theta_p \right) \right] \cdot \vec{\mathbf{v}} \;\Rightarrow\; \begin{cases} \mathrm{qmp}_k^{b_k}(n) \cdot v_k, & b_k = 0, \\ v_k \cdot \mathrm{qmp}_k^{b_k}(n), & b_k = 1, \end{cases}$$

where $\left\{\mathrm{qmp}_k^{b_k}(n)\right\}_{k,n=1}^N$ are the set of matrix elements of quaternion transform, *i.e.,*

$$\mathcal{QU}^{(b_1,b_2,...,b_N)}(\varphi_1,\varphi_2,...,\varphi_q) = \left[\mathrm{qmp}_k^{b_k}\left(n\mid\theta_1,\theta_2,...,\theta_p\right)\right]_{k,n=1}^N.$$ So, the number of such keys is

equal to 2^N. They form the Boolean cube $\mathbf{B}_2^N$. Knowing this key is necessary to enter into the Intelligent OFDM TCS.
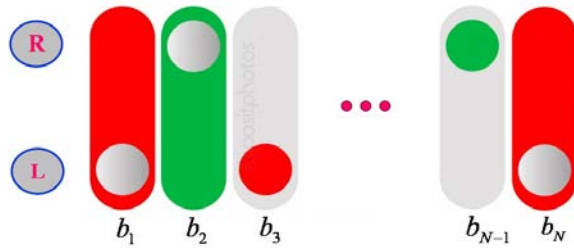

Fig 3. N-D binary vector-key $(b_1,b_2,...,b_N)$

Thus, the space of keys is the Descartes product $\mathbf{Tor}_q[0,2\pi]\times\mathbf{B}_2^N$. Searching the pair of keys $(\varphi_1,\varphi_2,...,\varphi_q)\in\mathbf{Tor}^q[0,2\pi]$ and $(b_1,b_2,...,b_N)\in\mathbf{B}_2^N$ in the space of keys is very difficult problem for the enemy, especially, when we have the OFDM TCS. Such a system can also defend itself by changing the values of the working parameters and crypto key accordingly to some law that is known for the transmitter and receiver in advance. The law can be deterministic or the pseudo-random (similarly to the law, by which the contemporary TCSs change their working frequency). The main advantage of using QMPT in OFDM TCS is that it is a very flexible anti-eavesdropping and anti-jamming Intelligent OFDM TCS. These TCS have additional advantages in comparison with the classic TCS: the multi-parametric transforms allow one to optimize (and as a result, to enhance) the technical characteristics of the system (by changing its parameters) such as the PARP (peak to average power ratio), BER (bit error rate), SER (symbol error rate), and the ISI (inter-symbol interference).

The paper are organized as follows. Section 2 of the paper presents a brief introduction to the quaternion algebra. Section 3 and 4 present quaternion Fourier transforms.

2.   Quaternions

The space of quaternions denoted by $\mathbb{H}(\mathbf{R})$ were first invented by W.R. Hamilton in 1843 as an extension of the complex numbers into four dimensions [7]. General information on quaternions may be obtained from [8].

Definition 1. Numbers of the form $^4\mathbf{q} = a\mathbf{1}+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$, where $a,b,c,d\in\mathbf{R}$ are called quaternions, where 1) $\mathbf{1}$ is the real unit; 2) $\mathbf{i},\mathbf{j},\mathbf{k}$ are three imaginary units. We speck that quaternions $^4\mathbf{q} = a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$ are written in the standard format.

132

The addition and subtraction of two quaternions $^4\mathbf{q}_1 = a_1 + x_1\mathbf{i} + y_1\mathbf{j} + z_1\mathbf{k}$ and $^4\mathbf{q}_2 = a_2 + x_2\mathbf{i} + y_2\mathbf{j} + z_2\mathbf{k}$ are given by

$$^4\mathbf{q}_1 \pm {}^4\mathbf{q}_2 = (a_1 \pm a_2) + (b_1 \pm b_2)\mathbf{i} + (b_1 \pm b_2)\mathbf{j} + (b_1 \pm b_2)k.$$

The product of quaternions for the standard format Hamilton defined according as:

$$^4\mathbf{q}_1 \circ {}^4\mathbf{q}_2 = (a_1 + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k}) \circ (a_2 + b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}) = \left(a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2\right) +$$
$$+\left(a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2\right)\mathbf{i} + \left(a_1 c_2 + c_1 a_2 + d_1 b_2 - b_1 d_2\right)\mathbf{j} + \left(a_1 d_2 + d_1 a_2 + b_1 c_2 - c_1 b_2\right)\mathbf{k},$$

where $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$; $\mathbf{i} \circ \mathbf{j} = -\mathbf{i} \circ \mathbf{j} = \mathbf{k}$, $\mathbf{i} \circ \mathbf{k} = -\mathbf{k} \circ \mathbf{i} = \mathbf{j}$, $\mathbf{j} \circ \mathbf{k} = -\mathbf{k} \circ \mathbf{j} = \mathbf{i}$. The set of quaternions with operations of multiplication and addition forms 4-D algebra $\mathbb{H}(\mathbf{R}) = \mathbb{H}\left(\mathbf{R} \,|\, 1, \mathbf{i}, \mathbf{j}, \mathbf{k}\right) := \mathbf{R} + \mathbf{R}\mathbf{i} + \mathbf{R}\mathbf{j} + \mathbf{R}\mathbf{k}$ over the real field $\mathbf{R}$.

Number component a and direction component $^3\mathbf{r} = b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbf{R}^3$ were called the *scalar* and 3-D *vector* parts of quaternion, respectively. Now these components are denoted as $S(^4\mathbf{q}) = a \in \mathbf{R}$ and $V(\mathbf{q}) = {}^3\mathbf{r} = b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$. A non–zero element $^3\mathbf{r} = bi + cj + dk$ is called pure vector quaternion. Hence, according to W. Hamilton every quaternion is the sum of a scalar number and a pure vector quaternion $^4\mathbf{q} = a + (b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = a + {}^3\mathbf{r} = S(\mathbf{q}) + V(\mathbf{q})$, where $a = S(^4\mathbf{q})$, $V(^4\mathbf{q}) = {}^3\mathbf{r}$. Since $\mathbf{i} \circ \mathbf{j} = \mathbf{k}$, then a quaternion $^4\mathbf{q} = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} = (a1 + b\mathbf{i}) + (c\mathbf{j} + d\mathbf{i} \circ \mathbf{j}) = (a + b\mathbf{i}) + (c + d\mathbf{i}) \circ \mathbf{j} = \mathbf{z} + \mathbf{w} \circ \mathbf{j}$ is the sum of two complex numbers $\mathbf{z} = a + b\mathbf{i}$, $\mathbf{w} = c + d\mathbf{i}$ with a new imaginary unit $\mathbf{j}$. So, every quaternion can be represented in several ways:

(1) as a 4-D hypercomplex number $^4\mathbf{q} = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} = (a, b, c, d)$, $a, b, c, d \in \mathbf{R}$ (standard 4-D format);

(2) as a sum of a scalar and vector parts $\mathbf{q} = a + {}^3\mathbf{r} = (a, {}^3\mathbf{r})$ (1,3-D hypercomplex format);

(3) as a 2-D hypercomplex numbers $^{2,2}\mathbf{q} = \mathbf{z} + \mathbf{w} \circ \mathbf{j} = (\mathbf{z}, \mathbf{w})$, $\mathbf{z}, \mathbf{w} \in \mathbf{C}$ (2,2-D complex format).

The product of quaternions for the last two forms Hamilton defined as:

$$^4\mathbf{q}_1 \circ {}^4\mathbf{q}_2 = (\mathbf{z}_1 + \mathbf{w}_1 \circ \mathbf{j}) \circ (\mathbf{z}_2 + \mathbf{w}_2 \circ \mathbf{j}) = (\mathbf{z}_1 \mathbf{z}_2 - \mathbf{w}_1 \overline{\mathbf{w}}_2) + (\mathbf{w}_1 \overline{\mathbf{z}}_2 + \mathbf{z}_1 \mathbf{w}_2) \circ \mathbf{j},$$

$$^4\mathbf{q}_1 \circ {}^4\mathbf{q}_2 = (a_1 + \vec{\mathbf{r}}_1) \circ (a_2 + \vec{\mathbf{r}}_2) = \left(a_1 a_2 - (\vec{\mathbf{r}}_1, \vec{\mathbf{r}}_2)\right) + \left(a_1 \vec{\mathbf{r}}_2 + a_2 \vec{\mathbf{r}}_1 + [\vec{\mathbf{r}}_1 \times \vec{\mathbf{r}}_2]\right),$$

where $S(^4\mathbf{q}_1 \circ {}^4\mathbf{q}_2) = a_1 a_2 - \left\langle {}^3\mathbf{r}_1 \,|\, {}^3\mathbf{r}_2 \right\rangle$, $V(^4\mathbf{q}_1 \circ {}^4\mathbf{q}_2) = a_1 {}^3\mathbf{r}_2 + a_2 {}^3\mathbf{r}_1 + {}^3\mathbf{r}_1 \times {}^3\mathbf{r}_2$. Here $\left\langle {}^3\mathbf{r}_1 \,|\, {}^3\mathbf{r}_2 \right\rangle = b_1 b_2 + c_1 c_2 + d_1 d_2$ and $^3\mathbf{r}_1 \times {}^3\mathbf{r}_2 = \mathbf{i}(c_1 d_2 - d_1 c_2) - \mathbf{j}(b_1 d_2 - d_1 b_2) + \mathbf{k}(b_1 c_2 - c_1 b_2)$ are scalar and vector products, respectively.

Definition 2. Let $^4\mathbf{q} = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H}(\mathbf{R})$ be a quaternion ($a, b, c, d \in \mathbf{R}$). Then $^4\overline{\mathbf{q}} = \overline{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}} = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$, $^4\overline{\mathbf{q}} = \overline{a + {}^3\mathbf{r}} = a - {}^3\mathbf{r}$ is the conjugate of $^4\mathbf{q}$, $N(^4\mathbf{q}) = \|\,^4\mathbf{q}\,\| = \sqrt{a^2 + b^2 + c^2 + d^2} = \sqrt{^4\overline{\mathbf{q}} \circ {}^4\mathbf{q}} = \sqrt{^4\mathbf{q} \circ {}^4\overline{\mathbf{q}}}$ is the norm of $^4\mathbf{q}$, and $tr(^4\mathbf{q}) = 2a = {}^4\mathbf{q} + {}^4\overline{\mathbf{q}}$ is the trace of $^4\mathbf{q}$. Therefore $^4\mathbf{q}^2 - tr(^4\mathbf{q})\,^4\mathbf{q} + N^2(^4\mathbf{q}) = 0$.

133

Proposition 1. We have $\overline{{}^4\mathbf{q}_1 \circ {}^4\mathbf{q}_2} = {}^4\overline{\mathbf{q}}_2 \circ {}^4\overline{\mathbf{q}}_1$ and $N({}^4\mathbf{q}_1 \circ {}^4\mathbf{q}_2) = N({}^4\mathbf{q}_1) \cdot N({}^4\mathbf{q}_2)$ f or every ${}^4\mathbf{q}_1, {}^4\mathbf{q}_2 \in \mathbb{H}(\mathbf{R})$. Note that $\|1\| = 1, \quad \|\mathbf{i}\| = \|\mathbf{j}\| = \|\mathbf{k}\| = 1$.

Definition 3. Quaternions $\left\{{}^4\boldsymbol{\rho} \,\middle|\, N({}^4\boldsymbol{\rho}) = 1\right\}$ of unit norm are called unit quaternions.

The unit quaternions $\boldsymbol{\rho}$ form a 3D hypersphere $\mathbb{S}^3 \subset \mathbb{H}(\mathbf{R}) \sim \mathbf{R}^4$. For each quaternion ${}^4\mathbf{q}$ with nonzero norm the following quaternion

$$
{}^4\boldsymbol{\rho} = \frac{{}^4\mathbf{q}}{\|{}^4\mathbf{q}\|} = \frac{a + {}^3\mathbf{r}}{\|{}^4\mathbf{q}\|} = \frac{a}{\|{}^4\mathbf{q}\|} + \frac{{}^3\mathbf{r}}{\|{}^4\mathbf{q}\|} = \frac{a}{\|{}^4\mathbf{q}\|} + \frac{\|{}^3\mathbf{r}\|}{\|{}^4\mathbf{q}\|} \frac{{}^3\mathbf{r}}{\|{}^3\mathbf{r}\|} = \frac{a}{\|{}^4\mathbf{q}\|} + \frac{\|{}^3\mathbf{r}\|}{\|{}^4\mathbf{q}\|} {}^3\boldsymbol{\mu} =
$$
$$
= \cos\alpha + {}^3\boldsymbol{\mu}\sin\alpha = \cos\alpha + (\mu_1\mathbf{i} + \mu_2\mathbf{j} + \mu_3\mathbf{k})\sin\alpha
$$

is an unit quaternion, where $\|{}^3\mathbf{r}\| = \sqrt{b^2 + c^2 + d^2}$, ${}^3\boldsymbol{\mu} = {}^3\mathbf{r}/\|{}^3\mathbf{r}\|$, $\cos\alpha = a/\|{}^4\mathbf{q}\|$, $\sin\alpha = \|{}^3\mathbf{r}\|/\|{}^4\mathbf{q}\|$, $\mu_1 = b/\|{}^3\mathbf{r}\|$, $\mu_2 = c/\|{}^3\mathbf{r}\|$, $\mu_3 = d/\|{}^3\mathbf{r}\|$ and $\boldsymbol{\mu} = \mu_1\mathbf{i} + \mu_2\mathbf{j} + \mu_3\mathbf{k}$. Obviously,

$$
{}^4\mathbf{q} = \|{}^4\mathbf{q}\| \cdot \left[\cos\alpha + {}^3\boldsymbol{\mu}(\gamma,\theta)\sin\alpha\right] = \|{}^4\mathbf{q}\| \cdot \left[\cos\alpha + (\mu_1\mathbf{i} + \mu_2\mathbf{j} + \mu_3\mathbf{k})\sin\alpha\right].
$$

where ${}^3\boldsymbol{\mu}(\gamma,\theta) = \mathbf{i}\cos\gamma + \mathbf{j}\sin\gamma\cos\theta + \mathbf{k}\sin\gamma\sin\theta \in \mathbf{S}^2$, $\theta,\varphi \in [0,\pi]$, $\alpha \in [0,2\pi)$ are the polar coordinates on $\mathbb{S}^3$. Obviously,

$$
a = \|{}^4\mathbf{q}\|\cos\alpha, \quad b = \left(\|{}^4\mathbf{q}\|\cos\gamma\right)\sin\alpha, \quad c = \left(\|{}^4\mathbf{q}\|\sin\gamma\cos\theta\right)\sin\alpha, \quad d = \left(\|{}^4\mathbf{q}\|\sin\gamma\sin\theta\right)\sin\alpha.
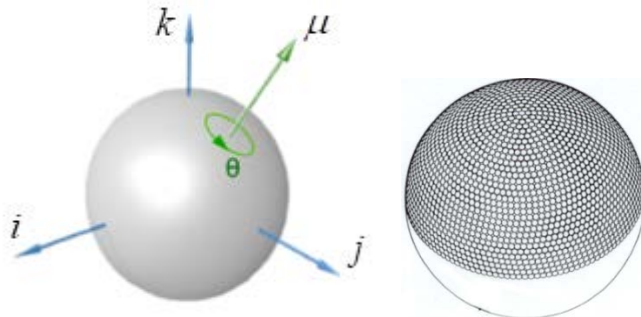$$

Fig. 4. Each 3D vector $\vec{\boldsymbol{\mu}} \in \mathbb{S}^2$ of unit length can play a role of classical imaginary unit. For example, the special elements ${}^3\mathbf{i}, {}^3\mathbf{j}, {}^3\mathbf{k}$ are such elements.

In particular, for ${}^4\mathbf{q}_1 \equiv {}^3\mathbf{r}_1 = b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k}$ and ${}^4\mathbf{q}_2 \equiv {}^3\mathbf{r}_2 = b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}_2$ we obtain

$$
{}^3\mathbf{r}_1 \circ {}^3\mathbf{r}_2 = -\langle {}^3\mathbf{r}_1)\,|\,{}^3\mathbf{r}_2\rangle + \left[{}^3\mathbf{r}_1 \times {}^3\mathbf{r}_2)\right], \quad {}^3\mathbf{r}^2 = {}^3\mathbf{r} \circ {}^3\mathbf{r} = -\langle {}^3\mathbf{r}\,|\,{}^3\mathbf{r}\rangle = -\|{}^3\mathbf{r}\|^2,
$$

and for a pure quaternion ${}^3\boldsymbol{\mu} \in \mathbb{S}^2 \subset \mathbf{R}^3$ with unity norm $\|{}^3\boldsymbol{\mu}\| = 1$ we have ${}^3\boldsymbol{\mu}^2 = -\|{}^3\boldsymbol{\mu}\|^2 = -1$, where $\mathbb{S}^2$ denotes the unit 2-D sphere in 3-D space $\mathbf{R}^3$. This unit-vector product identity represents the generalization of the complex-variable identity $i^2 = -1$.

134

This means that, if in the ordinary theory of complex numbers there are only two different square roots of negative unity ($+i$ and $-i$) and they differ only in their signs, then in the quaternion theory there are infinite numbers of different square roots of negative unity

$$^3\boldsymbol{\mu} = {}^3\boldsymbol{\mu}(\gamma,\theta) = \left(\mu_x\mathbf{i} + \mu_y\mathbf{j} + \mu_z\mathbf{k}\right) = \left(\cos\gamma\cdot\mathbf{i} + \sin\gamma\cos\theta\cdot\mathbf{j} + \sin\gamma\sin\theta\cdot\mathbf{k}\right) \in \mathbf{S}^2,$$

which gives $^3\boldsymbol{\mu}^2 = {}^3\boldsymbol{\mu}^2(\gamma,\theta) = -1$. Here $^3\boldsymbol{\mu}(\gamma,\theta) = \left(\cos\gamma, \sin\gamma\cos\theta, \sin\gamma\sin\theta\right)$ being still that point on the spherical surface, which has for its rectangular coordinates $\cos\gamma, \sin\gamma\cos\theta, \sin\gamma\sin\theta$ (see Fig. 4). In the feature we will omit left index: $\boldsymbol{\mu}(\gamma,\theta) \equiv {}^3\boldsymbol{\mu}(\gamma,\theta)$.

Definition 4. A functions $^4\mathbf{f}(n) : [0, N-1] \to \mathbb{H}(\mathbf{R})$ are called quaternion-valued discrete functions. They have the following form:

$$^4\mathbf{f}(n) = f_0(n) + f_1(n)\mathbf{i} + f_2(n)\mathbf{j} + f_3(n)\mathbf{k} = \left(f_0(n), f_1(n), f_2(n), f_3(n)\right).$$

The exponential function is $\exp({}^4\mathbf{q}) = 1 + {}^4\mathbf{q} + \dfrac{{}^4\mathbf{q}^2}{2!} + \ldots + \dfrac{{}^4\mathbf{q}^m}{m!} + \ldots = \displaystyle\sum_{m=0}^{\infty} \dfrac{{}^4\mathbf{q}^m}{m!}$.

Theorem 1 [14,15]. For $^4\mathbf{q} = a + {}^3\mathbf{r} \in \mathbb{H}(\mathbf{R})$ we have

$$\exp(a + {}^3\mathbf{r}) = e^a \exp({}^3\mathbf{r}) = e^a\left(\cos(\|\,{}^3\mathbf{r}\,\|) + \frac{{}^3\mathbf{r}}{\|\,{}^3\mathbf{r}\,\|}\sin(\|\,{}^3\mathbf{r}\,\|)\right).$$

Obviously, $\|\exp({}^3\mathbf{r})\| = 1$ and $\|\exp({}^3\mathbf{r})\| = \|\exp(a + {}^3\mathbf{r})\| = e^a$. In general case $\exp({}^4\mathbf{q}_1) \circ \exp({}^4\mathbf{q}_2) \neq \exp({}^4\mathbf{q}_2) \circ \exp({}^4\mathbf{q}_1)$ and $\exp({}^4\mathbf{q}_1 + {}^4\mathbf{q}_2) \neq \exp({}^4\mathbf{q}_1) \circ \exp({}^4\mathbf{q}_2) \neq \neq \exp({}^4\mathbf{q}_2) \circ \exp({}^4\mathbf{q}_1)$.

3. Quaternion Fourier Transforms

3.1. Historical remarks

Before defining the quaternion Fourier transform, we briefly outline its relationship with Clifford Fourier transformations. Quaternions and Clifford hypercomplex number were first simultaneously and independently applied to quaternion-valued Fourier and Clifford-valued Fourier transforms by Labunets [9] and Sommen [10,11], respectively, at the 1981. The Labunets quaternion transforms were over quaternion with real and Galois coefficients (i.e., over $\mathbb{H}[\mathbf{R}]$ and $\mathbb{H}[\mathbf{GF}(p)]$). They generalize both classical and co-called number theoretical transforms (NNTs) and proposed for application to fast signal processing. Ernst [12] and Delsuc [13] in the late 1981s, seemingly without knowledge of the earlier works of Labunets and Sommen proposed bicomplex Fourier transforms over 4D commutative hypercomplex algebra of bicomplex numbers ($\mathbf{C} \oplus \mathbf{C}$). Note that the bicomplex algebra is quite different from the quaternion algebra; among general things, bicomplex multiplication is commutative, but quaternion one is noncommutative. For this reason, the Ernst and Delsuc transforms are direct sum of ordinary Fourier transforms (*i.e.,* duplex Fourier transform). They

are a little bit similar in kind to quaternion Fourier transforms. Ernst and Delsuc's transforms were two-dimensional and proposed for application to nuclear magnetic resonance (NMR) imaging.

Two new ideas emerged in 1998-1999 in a paper by Labunets [14] and Sangwine [15]. These were, firstly, the choice of a general root ${}^3\boldsymbol{\mu}$ of -1 (a unit quaternion with zero scalar part) rather than a basis unit ($\mathbf{i}, \mathbf{j}$ or $\mathbf{k}$) of the quaternion algebra, and secondly, the choice of a general roots ${}^3\boldsymbol{\mu}_0 = \boldsymbol{\mu}_0(\gamma_0, \theta_0), {}^3\boldsymbol{\mu}_1 = \boldsymbol{\mu}_1(\gamma_1, \theta_1),..., {}^3\boldsymbol{\mu}_{N-1} = \boldsymbol{\mu}_{N-1}(\gamma_{N-1}, \theta_{N-1})$ of -1 (see cloud of imaginary units on figure 1) in Clifford algebra to create multi-parameter and fractional Fourier-Clifford transforms (with eigenvalues $e^{-\boldsymbol{\mu}_0(\gamma_0,\theta_0)}, e^{-\boldsymbol{\mu}_1(\gamma_1,\theta_1)},... ...,e^{-{}^3\boldsymbol{\mu}_{N-1}(\varphi_{N-1},\theta_{N-1})},...$).

Labunets, Rundblad-Ostheimer and Astola [16-18] used the classical and number theoretical quaternion Fourier and Fourier-Clifford transforms for fast invariant recognition of 2D, 3D and nD color and hyperspectral images, defined on Euclidean and non-Euclidean spaces. These publications give useful interpretation of quaternion and Cliffordean Fourier coefficients: they are relative quaternion- or Clifford-valued invariants of hyperspectral images with respect to Euclidean and non-Euclidean rotations and motions of physical and hyperspectral spaces. It removes the veil of mysticism and mystery from quaternion- and Clifford-valued Fourier coefficients. In the works of scientists F.Brackx, H. De Schepper, F. Sommen, and H. De Bie [19-22] mathematical theory of Fourier-Clifford transforms accepted the final completeness, beauty and elegance.

3.2.   Quaternion Fourier transforms

According to Theorem 1, for non-zero $\alpha \in \mathbf{R}$ and a non-zero ${}^4\mathbf{q} = a + {}^3\boldsymbol{\mu}$

$$\exp({}^4\mathbf{q}\alpha) = \exp\left((a + {}^3\boldsymbol{\mu})\alpha\right) = e^{a\alpha}\left(\cos(\| {}^3\boldsymbol{\mu} \| \alpha) + \frac{{}^3\boldsymbol{\mu}}{\| {}^3\boldsymbol{\mu} \|}\sin(\| {}^3\boldsymbol{\mu} \| \alpha)\right).$$

In particular case, for ${}^4\mathbf{q} \equiv {}^3\boldsymbol{\mu} = \boldsymbol{\mu}(\gamma, \theta)$ we have $e^{\boldsymbol{\mu}(\gamma,\theta)\alpha} = \cos(\alpha) + \boldsymbol{\mu}(\gamma,\theta)\sin(\alpha)$. For $\alpha = \alpha_k = 2\pi k / N$ ($k = 0,1,...,N-1$) we obtain quaternion-valued discrete harmonics

$$e^{\boldsymbol{\mu}(\gamma_k,\theta_k)\frac{2\pi}{N}kn} = \boldsymbol{\varepsilon}_k^{kn} = \cos\left(\frac{2\pi}{N}kn\right) + \boldsymbol{\mu}(\gamma_k,\theta_k)\sin\left(\frac{2\pi}{N}kn\right),$$

where each quaternion harmonic $\boldsymbol{\varepsilon}_k^{-kn} = \exp\left(-2\pi\boldsymbol{\mu}(\gamma_k,\theta_k)kn/N\right)$ has its own imaginary unit $\boldsymbol{\mu}_k := \boldsymbol{\mu}(\gamma_k,\theta_k) = \left(\cos\gamma_k \cdot \mathbf{i} + \sin\gamma_k \cos\theta_k \cdot \mathbf{j} + \sin\gamma_k \sin\theta_k \cdot \mathbf{k}\right) \in \mathbf{S}^2$, $k = 0,1,...,N-1$. Due to the non-commutative property of quaternion multiplication, there are two different types of quaternion Fourier transforms (QFTs).

These QFTs are the left- and right-sided QFTs (LS-QFT and RS-QFT), respectively.

Definition 4. The direct discrete quaternion Fourier transforms of $\mathbf{f}(n) : [0, N-1] \to \mathbb{H}(\mathbf{R})$ are defined as

$${}^4\mathbf{QF}\left(k|\gamma_k,\theta_k\right) = Q\mathcal{F}^{(\gamma,\theta)}\left\{{}^4\mathbf{f}(n)\right\} = \frac{1}{\sqrt{N}}\sum_{n=0}^{N-1} e^{-\boldsymbol{\mu}(\gamma_k,\theta_k)\frac{2\pi}{N}kn} \circ {}^4\mathbf{f}(n) = \frac{1}{\sqrt{N}}\sum_{n=0}^{N-1} \boldsymbol{\varepsilon}_k^{-kn} \circ {}^4\mathbf{f}(n), \qquad (1)$$

$$^4\mathbf{FQ}\left(k\,|\varphi_k,\theta_k\right)=\mathcal{FQ}^{(\varphi,\theta)}\left\{\,^4\mathbf{f}(n)\right\}=\frac{1}{\sqrt{N}}\sum_{n=0}^{N-1}{}^4\mathbf{f}(n)\circ e^{-\mu(\gamma_k,\theta_k)\frac{2\pi}{N}kn}=\frac{1}{\sqrt{N}}\sum_{n=0}^{N-1}{}^4\mathbf{f}(n)\circ\varepsilon_k^{-kn}, \qquad (2)$$

where $Q\mathcal{F}$, $\mathcal{FQ}$ are LS-QFT and RS-QFT, $\boldsymbol{\gamma}=(\gamma_0,\gamma_1,...,\gamma_{N-1})$, $\boldsymbol{\theta}=(\theta_0,\theta_1,...,\theta_{N-1})$.

Definition 5. The inverse quaternion Fourier transforms are defined as

$$^4\mathbf{f}(n)=2\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\frac{\mu(\gamma_k,\theta_k)}{\left[\mu(\gamma_{-k},\theta_{-k})+\mu(\gamma_k,\theta_k)\right]_L}\circ\varepsilon_k^{kn}\circ\,^4\mathbf{QF}\left(k\,|\gamma_k,\theta_k\right), \qquad (3)$$

$$^4\mathbf{f}(n)=2\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}{}^4\mathbf{QF}\left(k\,|\gamma_k,\theta_k\right)\circ\varepsilon_k^{kn}\circ\frac{\mu(\gamma_k,\theta_k)}{\left[\mu(\gamma_{-k},\theta_{-k})+\mu(\gamma_k,\theta_k)\right]_R}. \qquad (4)$$

We see, that $Q\mathcal{F}=Q\mathcal{F}^{(\gamma,\theta)}$ and $\mathcal{FQ}=\mathcal{FQ}^{(\gamma,\theta)}$ depend on $2N$ parameters $\left(\gamma_k,\theta_k\right)$, $k\in\{0,1,...,N-1\}$.

4.   Classical fractional and many-parameter Fourier transforms

With most of the data transmission systems nowadays use orthogonal frequency division multiplexing telecommunication system (OFDM-TCS) based on the discrete Fourier transform. It is a unitary operator $\mathcal{F}_{\mathcal{N}}=\left[e^{j2\pi kn/N}\right]_{k,n=1}^{N-1}$: $F(k)=\left(\mathcal{F}_{\mathcal{N}}f\right)(k)$. Relevant properties are that the square $\left(\mathcal{F}^2f\right)(n)=f(\ominus_{\mathcal{N}}n)$ is the inversion operator modulo N , and that its fourth power $\left(\mathcal{F}^4f\right)(n)=f(n)$, is the identity; hence $\mathcal{F}^3=\mathcal{F}^{-1}$. The operator $\mathcal{F}$ thus generates the cyclic Fourier group of order 4: $\mathbf{Gr}_4(\mathcal{F})=\left\{\mathcal{F}^a\right\}_{a\in\{0,1,2,3\}}=\left\{I,\mathcal{F}^1,\mathcal{F}^2,\mathcal{F}^3\right\}$. The idea of fractional powers of the Fourier operator $\mathcal{F}$ appears in the mathematical literature [23-31]. This idea is to consider the eigenvalue decomposition of the Fourier $(N\times N)$–matrix

$$\mathcal{F}_{\mathcal{N}}=\left[e^{j2\pi kn/N}\right]=\left[\sum_{s=0}^{N-1}\lambda_s\left|h_s(k)\right\rangle\left\langle h_s(n)\right|\right]=\left[\sum_{s=0}^{N-1}e^{2\pi js/4}\left|h_s(k)\right\rangle\left\langle h_s(n)\right|\right]=$$
$$=\mathbf{U}\left\{\mathrm{diag}\left(\lambda_0,...,\lambda_{N-1}\right)\right\}\mathbf{U}^{-1}=\mathbf{U}\Lambda\ \mathbf{U}^{-1}, \qquad (5)$$

where $\lambda_s=e^{j2\pi s/4}=j^s$ and $h_l(n)$ are eigenvalues and eigenfunctions in the form of the discrete Hermite functions, $\left|h_s(k)\right\rangle$ and $\left\langle h_s(n)\right|$ are vector-column and vector-row, respectively, $\mathbf{U}=\left[\left|h_0(k)\right\rangle,\left|h_1(k)\right\rangle,...,\left|h_{N-1}(k)\right\rangle\right]$ is the matrix of eigenvectors.

The continuously family of FrFT $\left\{\mathcal{F}^a\right\}_{a\in[0,4)}$ is constructed by replacing the s -th eigen-value $\lambda_s=e^{j2\pi s/4}$ by its a -th power $\lambda_s^a=e^{jsa2\pi/4}$, for a between 0 and 4, or $\lambda_s^\alpha=e^{jsa\pi/2}=e^{js\alpha}$ for α between 0 and 2π, where $\alpha=a\pi/2$.

The eigenvalues of the standard DFT matrix $\mathcal{F}_N$ are the fourth roots of unity, to be denoted by $\lambda_s \in \left\{ e^{j2\pi s/4} \right\}_{s=0}^3 \in \{\pm 1, \pm j\}$. This divides the space of N-point complex signals into four Fourier invariant subspaces whose dimensions N_s are the multiplicities of the eigenvalues λ_s, which have a modulo 4 recurrence in the dimension $N = 2^N = 4M$ given by $N_0 = M + 1, N_1 = M - 1$, $N_2 = M$, $N_3 = M$. Let a function $s(n) : \{0, 1, 2, ..., N-1\} \to \{0, 1, 2, 3\}$ describes of the distribution of eigenvalues along main diagonal $\mathbf{Diag}\left(e^{j\pi s(n)a/2}\right) = \mathbf{Diag}\left(e^{js(n)\alpha}\right)$. This function takes $M + 1$ times value 0, $M - 1$ times value 1, and M times values 2 and 3.

Definition 6. [23-31]. The discrete classical fractional Fourier transform are defined as

$$\mathcal{F}^\alpha = \left[e_k^{(\alpha)}(n) \right] := \mathbf{U}\left\{ \mathbf{Diag}\left(e^{js(m)\alpha}\right) \right\} \mathbf{U}^{-1} = \sum_{m=0}^{N-1} e^{js(m)\alpha} \left| h_m(k) \right\rangle \left\langle h_m(n) \right|, \quad (6)$$

and if $s(m) = m$ then we obtain the Bargmann fractional Fourier transform [26]

$$\mathcal{B}\mathcal{F}^\alpha = \left[be_k^{(\alpha)}(n) \right] := \mathbf{U}\left\{ \mathbf{Diag}\left(e^{jm\alpha}\right) \right\} \mathbf{U}^{-1} = \sum_{m=0}^{N-1} e^{jm\alpha} \left| h_m(k) \right\rangle \left\langle h_m(n) \right|, \quad (7)$$

The identical and classical Fourier transformations are both the special cases of the FrFTs. They correspond to $\alpha = 0$ ($\mathcal{F}^0 = I$) and $\alpha = \pi/2$ ($\mathcal{F}^{\pi/2} = \mathcal{F}$), respectively.

Definition 7. The discrete classical-like and Bargmann-like ($s(m) = m$) many-parameter DFT we define by the following way

$$\mathcal{F}^{(\mathbf{a})} = \mathcal{F}^{(\alpha_0, \alpha_1, ..., \alpha_{N-1})} = \mathbf{U}\left\{ \mathrm{diag}\left(e^{js(m)\alpha_m}\right) \right\} \mathbf{U}^{-1} = \sum_{m=0}^{N-1} e^{js(m)\alpha_m} \left| h_m(k) \right\rangle \left\langle h_m(n) \right|, \quad (8)$$

where $\mathbf{\alpha} = \left(\alpha_0, \alpha_1, ..., \alpha_{N-1}\right)$.

5. Fractional and many-parameter quaternion Fourier transforms

If quaternion harmonics have equivalent imaginary units $^3\mathbf{\mu}(\gamma_k, \theta_k) \equiv {}^3\mathbf{\mu}(\gamma, \theta)$, $\forall k = 0, 1, ..., N - 1$), then quaternion Fourier matrices $Q\mathcal{F}, \mathcal{F}Q$ contains commutative entries $e^{-{}^3\mathbf{\mu}(\gamma_k, \theta_k)\frac{2\pi}{N}kn}$. For this reason $Q\mathcal{F}$ and $\mathcal{F}Q$ have the same real-valued eigenfunction as ordinary DFT but with quaternion-valued eigenvalues $\left\{ e^{2\pi \cdot {}^3\mathbf{\mu}(\gamma, \theta)s/4} \right\}_{s=0}^3 = \left\{ {}^3\mathbf{\mu}^s(\gamma, \theta) \right\}_{s=0}^3$. Therefore,

$$\left[e^{-\mathbf{\mu}(\gamma, \theta)\frac{2\pi}{N}kn} \right] = \left[\sum_{s=0}^{N-1} e^{2\pi \cdot {}^3\mathbf{\mu}(\gamma, \theta)s/4} \left| h_s(k) \right\rangle \left\langle h_s(n) \right| \right] = \left[\sum_{s=0}^{N-1} {}^3\mathbf{\mu}^s(\gamma, \theta) \left| h_s(k) \right\rangle \left\langle h_s(n) \right| \right]$$

where $\{h_s(n)\}_{s=0}^{N-1}$ is the set of discrete real-valued Hermite functions. Hence, we can define fractional and manyparameter quaternion Fourier transforms.

Definition 8. For single parameter $\alpha \in \mathbf{Tor}_{2\pi}^1$ we introduce fractional quaternion Fourier transforms (FrQFT) of classical and Bargmann ($s(m) = m$) structures as

$$\mathcal{F}_Q^\alpha(\gamma,\theta) = \left[\sum_{m=0}^{N-1} e^{3\mu(\gamma_m,\theta_m)\cdot s(m)\cdot\alpha} \left|h_m(k)\right\rangle\left\langle h_m(n)\right|\right] = \mathbf{U}\cdot\mathbf{Diag}\left(e^{3\mu(\gamma_m,\theta_m)\cdot s(m)\cdot\alpha}\right)\cdot\mathbf{U}^{-1}. \quad (9)$$

Definition 9. For N-parameter $(\alpha_0,...,\alpha_{N-1}) \in \mathbf{Tor}_{2\pi}^N$ we introduce many-parameter quaternion Fourier transforms (MPQFT) of classical and Bargmann structures as

$$\mathcal{F}_Q^{\boldsymbol{\alpha}}(\gamma,\theta) = \left[\sum_{m=0}^{N-1} e^{3\mu(\gamma_m,\theta_m)\cdot s(m)\cdot\alpha_m} \left|h_m(k)\right\rangle\left\langle h_m(n)\right|\right] = \mathbf{U}\cdot\mathbf{Diag}\left(e^{3\mu(\gamma_m,\theta_m)\cdot s(m)\cdot\alpha_m}\right)\cdot\mathbf{U}^{-1}, \quad (10)$$

where $\gamma = (\beta_0,\beta_1,...,\beta_{N-1})$, $\theta = (\theta_0,\theta_1,...,\theta_{N-1})$, $\boldsymbol{\alpha} = (\alpha_0,\alpha_1,...,\alpha_{N-1})$. Obviously, they are $3N$-parameter transforms.

Due to the non-commutative property of quaternion multiplication, there are left- and right-sided transforms (LS-FrQFTs, LS-MPQFTs and RS-FrQFTs, RS-MPQFTs).

Definition 10. The direct discrete LS-FrQFTs, LS-MPQFTs and RS-FrQFTs, RS-MPQFTs of $\mathbf{f}(n):[0,N-1] \to \mathbb{H}(\mathbf{R})$ are defined as

$$\left|\mathbf{QF}^\alpha\left(k|\gamma,\theta\right)\right\rangle = Q\mathcal{F}^\alpha(\gamma,\theta)\left|\mathbf{f}(n)\right\rangle = \sum_{m=0}^{N-1}\left(e^{3\mu_m(\gamma_m,\theta_m)\cdot s(m)\cdot\alpha} \circ \left|h_m(k)\right\rangle\right)\left\langle h_m(n)|\mathbf{f}(n)\right\rangle,$$

$$\left|\mathbf{FQ}^\alpha\left(k|\gamma,\theta\right)\right\rangle = \mathcal{F}Q^\alpha(\gamma,\theta)\left|\mathbf{f}(n)\right\rangle = \sum_{m=0}^{N-1}\left(\left\langle h_m(n)|\mathbf{f}(n)\right\rangle \circ e^{3\mu_m(\gamma_m,\theta_m)\cdot s(m)\cdot\alpha}\right)\left|h_m(k)\right\rangle, \quad (11)$$

$$\left|\mathbf{QF}^{\boldsymbol{\alpha}}\left(k|\gamma,\theta\right)\right\rangle = Q\mathcal{F}^{\boldsymbol{\alpha}}(\gamma,\theta)\left|\mathbf{f}(n)\right\rangle = \sum_{m=0}^{N-1} e^{3\mu_m(\gamma_m,\theta_m)\cdot s(m)\cdot\alpha_m} \circ \left|h_m(k)\right\rangle\left\langle h_m(n)|\mathbf{f}(n)\right\rangle,$$

$$\left|\mathbf{FQ}^{\boldsymbol{\alpha}}\left(k|\gamma,\theta\right)\right\rangle = \mathcal{F}Q^{\boldsymbol{\alpha}}(\gamma,\theta)\left|\mathbf{f}(n)\right\rangle = \sum_{m=0}^{N-1}\left\langle h_m(n)|\mathbf{f}(n)\right\rangle \circ e^{3\mu_m(\gamma_m,\theta_m)\cdot s(m)\cdot\alpha_m} \left|h_m(k)\right\rangle, \quad (12)$$

6. 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 [32] and Wyner [33] (see Fig.5). 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 $\theta^0 = (\varphi_0^0, \varphi_1^0, ..., \varphi_q^0)$ 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.
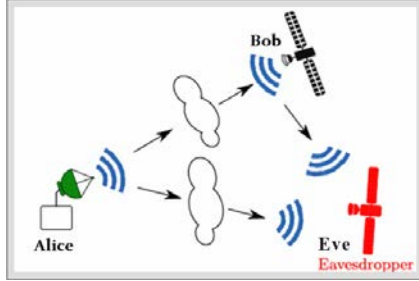
Fig. 5. Eavesdropping attack.

Alice transmits her data using OFDM with N quaternion-valued sub-carriers $\left\{ \mathbf{qsubc}_k \left(n \mid \boldsymbol{\theta}^0 \right) \right\}_{k=0}^{N-1}$, i.e., she uses the quaternion transform $\mathcal{QU}_N^0 \equiv \mathcal{QU}^{\mathbf{b}^0}(\boldsymbol{\theta}^0)$ with fixed keys $\boldsymbol{\theta}^0 = \left(\varphi_0^0, \varphi_1^0, \ldots, \varphi_q^0 \right)$, $\mathbf{b}^0 = (b_1, b_2, \ldots, b_N)$. When sub-carriers (i.e. unitary transform $\mathcal{QU}^{\mathbf{b}^0}(\boldsymbol{\theta}^0)$) 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. This means that Eve successful intercepts Alice's message. 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 $\mathcal{QU}^{\mathbf{b}^0}(\boldsymbol{\theta}^0)$ in the periodical (or random) manner (a priory known for Alice and Bob).

For comparative analysis we use OFDM-TCS, based on one-parameter classical $\mathcal{QF}^\alpha(\boldsymbol{\beta}, \boldsymbol{\theta}) \equiv \mathcal{QF}^\alpha(\mathbf{i})$ and many-parameter Bargmann $\mathcal{QBF}^\alpha(\mathbf{i})$ quaternion Fourier transforms in its one-parameter forms

$$\mathcal{QF}^\alpha(\mathbf{i}) = \left[\sum_{m=0}^{N-1} e^{\mathbf{i} \cdot s(m) \cdot \alpha} \left| h_m(k) \right\rangle \left\langle h_m(n) \right| \right], \quad \mathcal{QBF}^\alpha(\mathbf{i}) = \left[\sum_{m=0}^{N-1} e^{\mathbf{i} \cdot m \cdot \alpha} \left| h_m(k) \right\rangle \left\langle h_m(n) \right| \right],$$

where $\left\{ h_s(n) \right\}_{s=0}^{N-1}$ is the set of discrete real-valued Hermite functions, $^3 \boldsymbol{\mu}_r^p (\beta_r^p, \theta_r^p) \equiv \mathbf{i}, \ \forall r = 1, 2, \ldots, n; \ \forall p = 0, 1, \ldots, 255$ for both transforms.

Simulations were done in MATLAB R2018b. Intelligent OFDM-TCS's parameters are assumed as follows: 256-QAM modulation, the sizes of $\mathcal{QF}^\alpha(\mathbf{i})$ and $\mathcal{QBF}^\alpha(\mathbf{i})$ are 256×256 (i.e., the number of quaternion-valued subcarriers is 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).

Now, we provide some simulation results to substantiate our theoretical claims for $\mathcal{QF}^a(\mathbf{i})$ and $\mathcal{QBF}^a(\mathbf{i})$ 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

140

information against the threat of electronic eavesdropping Alice and Bob use described above defense mechanism.
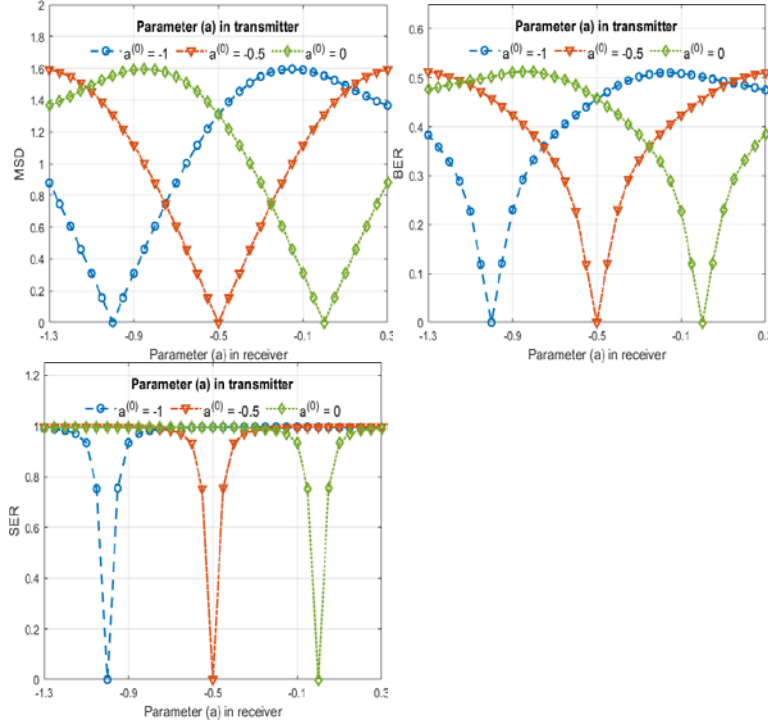

Fig. 6. The average a) $\mathbf{MSD}$, b) $\mathbf{BER}$ and c) $\mathbf{SER}$ measurements versus a for $\mathcal{QF}^{a}(\mathbf{i})$ with different values of parameter a^{0} : $a^{0} = -1$ (blue curve), $a^{0} = -0.5$ (red curve), $a^{0} = 0$ (green curve) . When parameters in transmitter (Alice) and receiver (Eva) are the same ($a = a^{0}$), we have $\mathbf{MSD} = 0$, $\mathbf{BER} = 0$ and $\mathbf{SER} = 0$.

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 timeslot. Fig. 6 show the average

$$\mathbf{MSD}(a) = \frac{1}{256}\sum_{l=0}^{255}\mathbf{MSD}\big[l\,|\,a\big],\ \ \Big\langle\mathbf{BER}_{(A\rightarrow B|\xi=0)}^{Bit}\big[l\,|\,a\big]\Big\rangle = \sum_{l=0}^{255}\mathbf{BER}_{(A\rightarrow B|\xi=0)}^{Bit}\big[l\,|\,a\big],$$

$$\Big\langle\mathbf{SER}_{(A\rightarrow E|\xi=0)}^{Sym}\big[l\,|\,a\big]\Big\rangle = \sum_{l=0}^{255}\mathbf{SER}_{(A\rightarrow E|\xi=0)}^{Sym}\big[l\,|\,a\big]$$

measurements versus a_{i} in noiseless case for $\mathcal{QF}^{a}(\mathbf{i})$ in the absence of thermal noise ($\xi = 0$) for some types of $\mathcal{QF}^{a}(\mathbf{i})$ (plotted with different color). When parameters in

141

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 working value of the parameter a ($a^0 \to a$), but Eve use previous value a^0, then Eve will receive Alice's massage with big mistakes. To illustrate this result, we consider the image "Lena" as Eva`s message. Fig. 7 shows received Eva`s message with different values of a in the Alice`s OFDM-TCS, when Eva works with classical DFT.
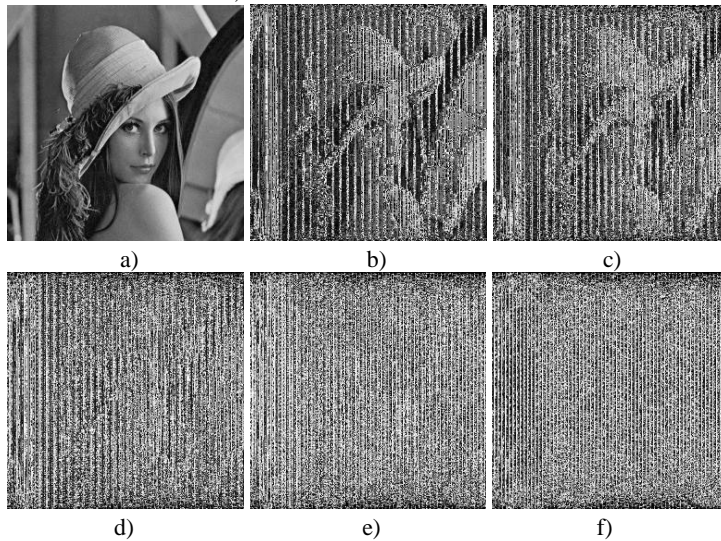

a)   b)   c)

d)   e)   f)

Fig. 7. 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 $\mathcal{QF}^a(\mathbf{i})$ with new value of parameter a: a) $a = -1$, b) $a = -0.8$, $a = -0.8$, c) $a = -0.6$, d) $a = -0.4$, e) $a = -0.2$, f) $a = 0$.

Similar results we have for OFDM-TCS, based on quaternion Bargmann-Fourier transform $\mathcal{QBF}^a(\mathbf{i})$.

7. Conclusions

In this paper, we have shown a new unified approach to the many-parametric representation of complex and quaternion Fourier transforms. Defined representation of many-parameter quaternion Fourier transforms (MPQFTs) depend on finite set of free parameters, which could be changed independently of one another. For each fixed values of parameter we get the unique orthogonal transform. We develop novel Intelligent OFDM-telecommunication systems based on fractional and multi-parameter Fourier transforms and shown their superiority and practicability from the physical layer security. The new systems use inverse MPQFT (IMPQFT) for modulation at the transmitter and direct MPFQT (DMPFQT) for demodulation at the receiver. Simula-

tion results show that the proposed Intelligent OFDM-TCS have better performance than the conventional OFDM system based on DFT against eavesdropping.

8.   Acknowledgements

References

1.   Gupta M. K., Tiwari S. Performance evaluation of conventional and wavelet based OFDM System, International Journal on Electronics and Communication, 2013, vol. 67, no.4, pp 348– 354ю
2.   Patchala S., Sailaja M. Analysis of Filter Bank Multi-Carrier system for 5G communications, International Journal of Wireless and Microwave Technologies, 2019, vol.9, no.4, pp. 39-50.
3.   Kaur H., Kumar M., Sharma A. K, Singh H.P. Performance Analysis of Different Wavelet Families over Fading Environments for Mobile WiMax System, International Journal of Future Generation Communication and Networking, 2015, vol. 8, pp 87-98.
4.   Davis J. A., Jedwab J. Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes IEEE Trans. Inform. Theory, 1999, vol. 45, pp.2397–2417.
5.   Michailow N., Mendes L., Matthe M., Festag I., Fettweis A., Robust G. WHT-GFDM for the next generation of wireless networks, IEEE Communications Letters, 2015, vol. 19, pp. 106–109.
6.   Manhas P., Soni M.K. Comparison of OFDM System in Terms of BER using Different Transform and Channel Coding, International Journal of Engineering and Manufacturing, 2016, vol. 1, pp. 28-34.
7.   Hamilton W. R . Elements of Quaternions, New York: Chelsea Pub. Com., 1969, p. 242
8.   Ward J. P. Quaternions and Cayley Numbers: Algebra and Applications, Dordrecht, Netherlands: Kluwer Academic Publishers, 1997, p. 218.
9.   Labunets V. G. Quaternion number–theoretical transform, Devices and Methods of Experimental Investigations in Automation, Dnepropetrovsk: Dnepropetrovsk State University Press, 1981, pp. 28–33. (In Russian)
10.   Sommen F. A product and an exponential function in hypercomplex function theory. Applicable Analysis, 1981, Vol. 12, pp. 13-26.
11.   Sommen F Hypercomplex Fourier and Laplace transforms I, Illinois Journal of Mathematics, 1982, vol. 26, no. 2 pp. 332-352.
12.   Ernst R. R., Bodenhausen G., Wokaun A. Principles of nuclear magnetic resonance in one and two dimensions, International Series of Monographs on Chemistry, Oxford University Press, 1987, p.???
13.   Delsuc M. A. Spectral representation of 2D NMR spectra by hypercomplex numbers, Journal of Magnetic Resonance, 1969, vol. 77, No. 1, pp. 119–124.

14. Rundblad–Labunets E., Labunets V., Astola J., Egiazarian K. Fast fractional Fourier–Clifford transforms, Second International Workshop on Transforms and Filter Banks, Tampere, Finland: TICSP Series, 1999, no. 5, pp. 376–405.
15. Sangwine S. J., Ell T. A. Thediscrete Fourier transform of a colour image, Image Processing II Mathematical methods, algorithms and Applicationsed , J.M. Blackledge and M.J. Turner, 1998, pp. 430–441.
16. Labunets-Rundblad E. Fast Fourier-Clifford Transforms Design and Application in Invariant Recognition, PhD thesis, Tampere, Finland: Tampere University Technology, 2000, p. 262
17. Rundblad E., Labunets V., Egiazarian K., Astola J. Fast invariant recognition of color images based on Fourier–Clifford number theoretical transform, EUROPORTO, Conf. on Image and Signal Processing for Remote Sensing YI, 2000, p. 284-292.
18. Labunets V. G., Kohk E. V., Ostheimer E. Algebraic models and methods of image computer processing. Part 1. Multiplet models of multichannel images, Computer optics, . 2018, vol. 42, no. 1., pp. 84-96.
19. Brackx F., De Schepper N., Sommen F. The 2-D Clifford–Fourier transform, Journal of Mathematical Imaging and Vision, 2006. vol. 26, no. 1, pp. 5–18.
20. Brackx F, Schepper N., Sommen F. The Fourier transform in Clifford analysis, Advances in Imaging and Electron Physics, 2009, vol. 156, pp. 55–201.
21. De Bie H., De Schepper N. The fractional Clifford–Fourier transform, Complex Analysis and Operator Theory, 2012, vol. 6, no. 5, pp. 1047–1067.
22. De Bie H., De Schepper N., Sommen F. The class of Clifford–Fourier transforms, Journal of Fourier Analysis and Applications, 2011, vol. 17, pp. 1198–1231.
23. Condon E.U., Immersion of the Fourier transform in a continuous group of functional transforms, Proc. Nat. Acad. Sci., 1937, 23, pp. 158-164.
24. Kober H., Wurzeln aus der Hankel- und Fourier und anderen stetigen Transformationen, Quart. J. Math. Oxford Ser., 1939, 10, pp. 45-49.
25. Bargmann V., On a Hilbert space of analytic functions and an associated integral transform. Part 1, Commun. Pure Appl. Math., 1961, 14, pp. 187-214.
26. Namias V., The fractional order Fourier transform and its application to quatum mechanics, J. Inst. Math. Appl., 1980, 25, pp. 241-265.
27. McBride A.C., Kerr F.H., On Namias' fractional Fourier transforms, IMA J. Appl. Math., 39, pp. 159-265, 1987.
28. Ozaktas H.M., Mendlovic D., Fourier transform of fractional order and their optical interpretation, Opt. Commun., 1993, 110, pp. 163-169.
29. Ozaktas H.M., Zalevsky Z., Kutay M.A., The fractional Fourier transform. Wiley, Chichester, 2001, 532 p.
30. Carracedo C. M., Alix M. S., The theory of fractional powers of operators, London - New York: Elsevier, 2001, 366 p.
31. Kumar R., Singh K., Khanna R. Satellite Image Compression using Fractional Fourier Transform, International Journal of Computer Applications, 2012, vol.50, no.3, pp. 20-25.
32. Shannon C. E. Communication Theory of Secrecy Systems, Bell Labs Technical Journal, 1949, vol. 28, no. 4. pp 657–71.
33. Wyner A. D. The wiretap channel, Bell Labs Technical Journal, 1975, vol. 54, no. 8, pp. 1355–1387.