Аннотация

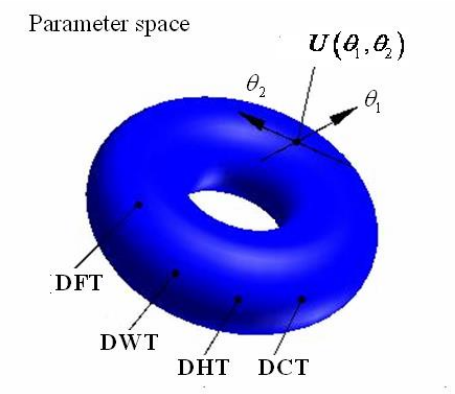
Проект направлен на решение фундаментальной проблемы информационной безопасности при 1) хранении, 2) анализе, 3) приеме и передаче больших объемов цифровых видеоданных различных типов (в частности, на решение фундаментальной проблемы совершенствования методов скрытного и помехозащищенного приема и передачи информации в условиях радиоэлектронной и телекоммуникационной борьбы).

В настоящее время при решении трех вышеперечисленных задач широкое применение получили ортогональные преобразования, например, косинусное и вейвлет преобразования (для сжатия изображений в стандартах JPEG, MPEG, H264), дискретное преобразование Фурье (при спектральном анализ изображений, передача телевизионных изображений OFDM телекоммуникационными системами), дискретные преобразования Уолша-Адамара (при передаче данных на основе CDMA-технологии) и т.д. Во всех перечисленных применениях результат обработки данных с помощью того или иного ортогонального преобразования является уязвимым с точки зрения кибератак, если они не защищены с помощью мощных и дорогих криптосистем. В связи с этим возникает проблема киберзащиты данных непосредственно в процессе их обработки, приеме или передаче. Обычно в данной ситуации говорят о разработке систем информационной безопасности данных на физическом уровне.

Настоящий проект посвящен созданию научно–технического задела для разработки методов нового криптозащищенного сжатия и хранения данных а также перспективной интеллектуальной OFDM телекоммуникационной системы (Intelligent-OFDM ТКС) для передачи больших цифровых видеоданных. Новые методы, технологии и системы основываются на быстрых многопараметрических преобразованиях (МПП), оснащенных цифровыми криптоключами, которые используются вместо традиционных ортогональных преобразований.

Матричные элементы $\mathrm{mp}_k(n)$ матрицы МПП $U\left(\theta_1,\theta_2,...,\theta_p\right)=\left[\mathrm{mp}_k(n\,|\,\theta_1,\theta_2,...,\theta_p)\right]_{k,n=1}^{N}$ – суть числа некоторой алгебры **Alg** (например, поля комплексных или гиперкомплексных чисел, алгебры Клиффорда, алгебры Кэли-Диксона и т.д.). Их численные значения зависят от некоторого набора свободных параметров $\mathrm{mp}_k(n)=\mathrm{mp}_k(n\,|\,\theta_1,\theta_2,...,\theta_p)$, каждый из которых может принимать значения от 0 до 2π. Вектор параметров $(\theta_1,\theta_2,...,\theta_p)$ принадлежит p-мерному тору $(\theta_1,\theta_2,...,\theta_p)\in\mathbf{Tor}^p[0,2\pi]=(0,2\pi]^p$. При изменении параметров меняются численные значения матичных элементов и, значит, меняется само МПП, которое остается при этом ортогональным. Возможная сфера применения подобных МПП весьма обширна: от хранения и передачи информации в Интернете вещей до обмена информацией в рое космических нано-спутников, короче, там, где действуют активные перехватчики информации.

Каждому конкретному значению параметров $(\theta_1,\theta_2,...,\theta_p)=(A_1,A_2,...,A_p)$ соответствует вполне определенное ортогональное преобразование $U\left(\theta_1,\theta_2,...,\theta_p\right)_{\theta_1=A_1,\theta_2=A_2,...,\theta_p=A_p}=U(A_1,A_2,...,A_p)$, которое называется реализацией МПП. При изменении значений параметров МПП меняет облик одного ортогонального преобразования на другое (см. Рис. 1).



$$\mathbf{Tor}_q = [0,2\pi)^q = \left\{(\theta_1,\theta_2,...,\theta_q)\middle|\theta_i \in [0,2\pi)\right\}$$

Рис 1. Параметрическое пространство в виде 2-мерного тора, каждой точке которого соответствует вполне определенное ортогональное преобразование (которое называется реализацией МПП). Когда параметры обегают весь тор, генерируется ансамбль ортогональных преобразований, который содержит все облики МПП.

Если алгебра **Alg** – суть поле комплексных чисел ($\mathbf{Alg} = \mathbf{C}$), то при одних значениях параметров МПП имеет облик, например, вейвлет преобразования Добюши, при других значениях – облик ДПФ, а при третьих – облик преобразования Уолша или Хаара и т.д. Если алгебра **Alg** – суть алгебра Клиффорда или Кэли-Диксона ($\mathbf{Alg} = \mathbf{KA}$ или $\mathbf{Alg} = \mathbf{КДА}$), то при изменении параметров МПП последовательно принимает облик соответствующих преобразований над этими алгебрами. Когда вектор параметров $(\theta_1,\theta_2,...,\theta_p)$ пробегает полностью p-мерный $\mathbf{Tor}^p[0,2\pi]$, формируется ансамбль ортогональных преобразований, который содержит все облики МПП.

Проектируемые системы обработки и анализа данных функционируют при конкретных значениях параметров $(\theta_1,\theta_2,...,\theta_p) = (A_1,A_2,...,A_p)$ (рабочие параметры), используя при этом конкретную реализацию МПП $U(A_1,A_2,...,A_p)$. Вектор $(A_1,A_2,...,A_p)$ является своеобразным аналоговым ключом (см. рис 2), знание которого необходимо для входа в систему с целью перехвата конфиденциальной информации (например для входа в архиватор с целью восстановления сжатого изображения с помощью МПП или для подавления работы ТКС, предающей информацию не с помощью ДПФ, а с помощью МПП).

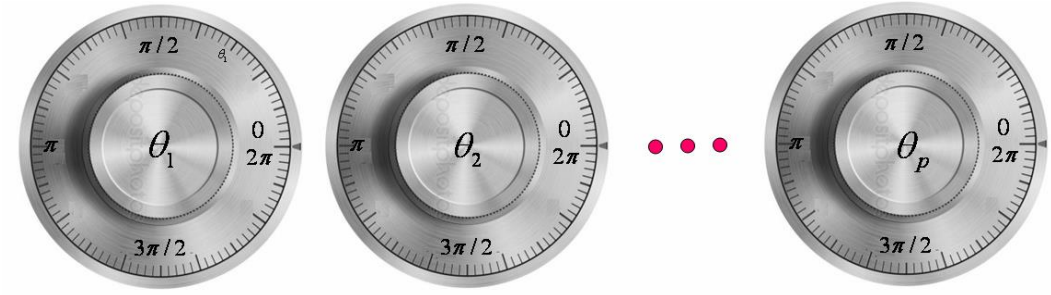


Рис 2. Вектор параметров $(\theta_1,\theta_2,...,\theta_p)$ в виде аналогового криптоключа.

Количество параметров может достигать значений $p = 10\ 000$. Поиск векторного ключа путем сканирования 10 000-мерного тора $\mathbf{Tor}^{10\ 000}[0,2\pi]$ с целью нахождения рабочих параметров $(A_1,A_2,...,A_p)$ является трудной задачей для киберсредств противника. Но даже, если этот ключ в процессе кибератаки будет определен противником, то система может изменить значения рабочих параметров

$$U\left(\theta_1,\theta_2,...,\theta_p\right)_{\theta_1=A_1,\theta_2=A_2,...,\theta_p=A_p}=U(A_1,A_2,...,A_p)$$

$$\downarrow$$

$$U\left(\theta_1,\theta_2,...,\theta_p\right)_{\theta_1=B_1,\theta_2=B_2,...,\theta_p=B_p}=U(B_1,B_2,...,B_p),$$

отражая тем самым атаку противника. Если система является телекоммуникационной, то она в этом случае будет передавать конфиденциальную информацию на новых поднесущих (в новом ортогональном базисе), тем самым противодействуя радиоэлектронным атакам (перехвату или глушению) противника.

Для противника задача усугубляется еще и тем, что МПП дополнительно оснащается цифровым ключом, который связан с некоммутативностью умножения в многомерных алгебрах, что влечет новый тип матричного умножения. При умножении матрицы МПП на вектор данных $U\left(\theta_1,\theta_2,...,\theta_p\right)\cdot\vec{\mathbf{v}}=\left[\mathrm{mp}_k(n)\right]\cdot\vec{\mathbf{v}}$, каждый элемент v_k N-мерного вектора $\vec{\mathbf{v}}$ может умножаться на матричный элемент $\mathrm{mpp}_k(n)$ либо слева (т.е. $v_k\cdot\mathrm{mpp}_k(n)$), либо справа (т.е. $\mathrm{mpp}_k(n)\cdot v_k$).

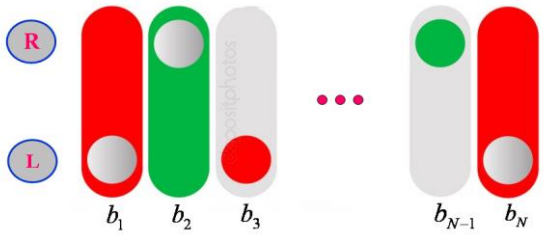


Рис 3.N-мерный бинарный криптоключ $\left(b_1,b_2,...,b_N\right)$,

Если символ 0 означает умножение слева (L) элемента вектора данных на матричный элемент, а символ 1 – справа (R), то N-мерный бинарный вектор $\left(b_1,b_2,...,b_N\right)$, является цифровым ключом, каждым символом которого оснащается столбец матрицы МПП:

$$U^{(b_1,b_2,...,b_N)}\left(\theta_1,\theta_2,...,\theta_p\right)=\left[\mathrm{mp}_k^{b_k}\left(n\,|\,\theta_1,\theta_2,...,\theta_p\right)\right]$$

и который указывает на то, каким образом осуществляется перемножение матрицы МПП с вектором данных (см. рис. 3):

$$U^{(b_1,b_2,...,b_N)}\left(\theta_1,\theta_2,...,\theta_p\right)\cdot\vec{\mathbf{v}}=\left[\mathrm{mp}_k^{b_k}\left(n\,|\,\theta_1,\theta_2,...,\theta_p\right)\right]\cdot\vec{\mathbf{v}}\;\Rightarrow\;\begin{cases}\mathrm{mp}_k^{b_k}(n)\cdot v_k, & b_k=0,\\ v_k\cdot\mathrm{mp}_k^{b_k}(n), & b_k=1.\end{cases}$$

Таких ключей равно числу 2^N. Они формируют N-мерный булев куб $\mathbf{B}_2^N$. Знание этого ключа также необходимо для входа в систему обработки или передачи данных. Таким образом, пространство ключей – суть декартово произведение p-мерного тора и N-мерного булева куба $\mathbf{Tor}^p[0,2\pi]\times\mathbf{B}_2^N$. Поиск пары ключей $(A_1,A_2,...,A_p)\in\mathbf{Tor}^p[0,2\pi]$ и $\left(b_1,b_2,...,b_N\right)\in\mathbf{B}_2^N$ (аналогового и цифрового) в пространстве ключей является трудной задачей для противника особенно если речь идет об OFDM ТКС. Она может защитить себя также путем изменения значений рабочих параметров и криптоключа по заранее известному передатчику и приемнику закону – детерминированному или псевдослучайному (подобно тому, как современные ТКС меняют рабочую частоту), что в существенной мере усложняет задачу перехвата или подавления передаваемой информации. OFDM ТКС обладает дополнительными достоинствами по сравнению с классической ТКС: многопараметрические преобразования позволяют оптимизировать (и, следовательно, улучшить) технические характеристики системы (путем изменения параметров), таких как PAPR (peak to average power ratio), BER (bit error rate), SER (symbol error rate) и ISI (inter-symbol interference).

Цель и задачи проекта

В настоящее время в Российской Федерации сформулирована *Концепция информационной безопасности* как составной части национальной безопасности России. В рамках этой Концепции изложены основные положения государственной политики обеспечения информационной безопасности, имеющие большое значение для построения как государственной, так и

ведомственных систем защиты больших цифровых видеоданных. Особенно остро проблема информационной безопасности стоит в настоящее время в технологиях гиперспектрального дистанциионного зондирования Земли (ДЗЗ), телекоммуникационных системах (ТКС) и технологии “Интеренет вещей” (The Internet of Things - IoT). IoT основан на всепроникающей связи между агентами (вещями, устройствами, людьми, организациями и т.д.). Число, связываемых друг с другом устройств в технологии IoT уже сейчас превышает численность населения Земли и неуклонно растет. Многочисленные источники предсказывают, что к 2020 году число устройств, которые должны коммуницировать друг с другом достигнет 50 миллиардов. Применение технологии IoT включает умные города, умный трафик, умные дома, индустриальный мониторинг, мониторинг окружающей среды и т.д. Объемы передаваемой здесь секретной и конфиденциальной информации колоссальны. Она имеет первостепенной значение для безопасности и целостности как для отдельных людей, организаций так и для целых государств.

Технологии ДЗЗ и IoT обладают способностями к решению следующих задач: 1) измерение, 2) анализ данных, 3) их хранение, 4) прием и передача. При решении этих задач широкое применение получили ортогональные преобразования. Например, косинусное и вейвлет преобразования для сжатия изображений в стандартах JPEG, MPEG, H264, дискретное преобразование Фурье при спектральном анализ изображений и передаче телевизионных изображений OFDM телекоммуникационными системами, дискретные преобразования Уолша-Адамара для передаче данных на основе CDMA-технологии и т.д.

Однако, в технологиях ДЗЗ и IoT существуют многочисленные научные проблемы. Главная из них состоит в обеспечении должного уровня секретности и конфиденциальности, поскольку во всех перечисленных выше применениях результат обработки данных с помощью того или иного ортогонального преобразования является уязвимым с точки зрения кибератак. Наличие этой проблемы не делает технологии ДЗЗ, ТКС и IoT доступными для более широкого применения (особенно в системах специального назначения). Несмотря на то, что классические криптосистемы защищают информационные системы, их применение в ДЗЗ, ТКС и IoT затруднено. Например, IoT-устройства (от хорошо оснащенных до дешевых смартфонов) являются легкими и энергетически мало потребляемыми приборами. На многие из них не представляется возможным разместить дополнительное оборудование и программное обеспечение, реализующее криптографическую технологию. В связи с этим возникает проблема киберзащиты данных непосредственно в процессе их обработки, приеме или передаче. Обычно в данной ситуации говорят о разработке систем информационной безопасности данных на физическом уровне.

Главная цель настоящий проект – разработка теории быстрых многопараметрических преобразований (МПП)

$$U^{(b_1,b_2,...,b_N)}\left(\theta_1,\theta_2,...,\theta_p\right)=\left[\mathrm{mp}_k^{b_k}\left(n\,|\left(\theta_1,\theta_2,...,\theta_p\right)\right)\right],$$

дополнительно оснащенных цифровыми крипто-ключами $\left(b_1,b_2,...,b_N\right)\in\mathbf{B}_2^N$. Матричные элементы $\mathrm{mpp}_k^{b_k}(n)$ матрицы МПП $\left[\mathrm{mpp}_k^{b_k}(n)\right]$ – суть числа некоторой алгебры **Alg,** в качестве которой планируется использовать поля вещественных $\mathbf{Alg}=\mathbf{R}$ и комплексных чисел $\mathbf{Alg}=\mathbf{C}$, конечные поля Галуа $\mathbf{Alg}=\mathbf{GF}(q)$, некоммутативные алгебры Клиффорда $\mathbf{Alg}=\mathbf{KA}$ и алгебры Кэли-Диксона $\mathbf{Alg}=\mathbf{KDA}$. Численные значения матричных элементов зависят от некоторого набора свободных параметров $\mathrm{mp}_k^{b_k}(n)=\mathrm{mp}_k^{b_k}\,|\left(n\,|\,(\theta_1,\theta_2,...,\theta_p)\right)$ каждый из которых может принимать значения от 0 до 2π. Вектор параметров $(\theta_1,\theta_2,...,\theta_p)$ принадлежит p-мерному тору $\mathbf{Tor}^p[0,2\pi]$. При изменении значений параметров МПП меняет облик одного ортогонального преобразования на другое (см. рис. 1). К числу таких МПП можно отнести дробное и многопараметрическое преобразования Фурье над полем комплексных чисел или многопараметрические вейвлет-преобразования. Например, двумерные 2-параметрические базисные вейвлет-функции при различных значениях параметров представлены на рис.4.

В нашем проекте МПП дополнительно оснащаются цифровым ключом, который связан с некоммутативностью умножения в алгебрах Клиффорда, что влечет новый тип матричного умножения. Если символ 0 означает умножение слева элемента вектора данных на матричный элемент, а символ 1 – справа, то N-мерный бинарный вектор $\left(b_1,b_2,...,b_N\right)$, является цифровым ключом, каждым символом которого оснащается столбец матрицы МПП:

$U^{(b_1,b_2,...,b_N)}(\theta_1,\theta_2,...,\theta_p)=\left[\mathrm{mp}_k^{b_k}(n)\right]$ и который указывает на то, каким образом осуществляется перемножение матрицы МПП с вектором данных.

$$U^{(b_1,b_2,...,b_N)}(\theta_1,\theta_2,...,\theta_p)\cdot\vec{\mathbf{v}}=\left[\mathrm{mp}_k^{b_k}(n)\right]\cdot\vec{\mathbf{v}}\Rightarrow\begin{cases}\mathrm{mp}_k^{b_k}(n)\cdot v_k, & b_k=0,\\ v_k\cdot\mathrm{mp}_k^{b_k}(n), & b_k=1,\end{cases}.$$

Таких ключей равно числу 2^N. Они формируют N-мерный булев куб $\mathbf{B}_2^N$. Знание этого ключа также необходимо для входа в систему обработки или передачи данных. Таким образом, пространством ключей является декартово произведение p-мерного тора и N-мерного булева куба $\mathbf{Tor}^p[0,2\pi]\times\mathbf{B}_2^N$.

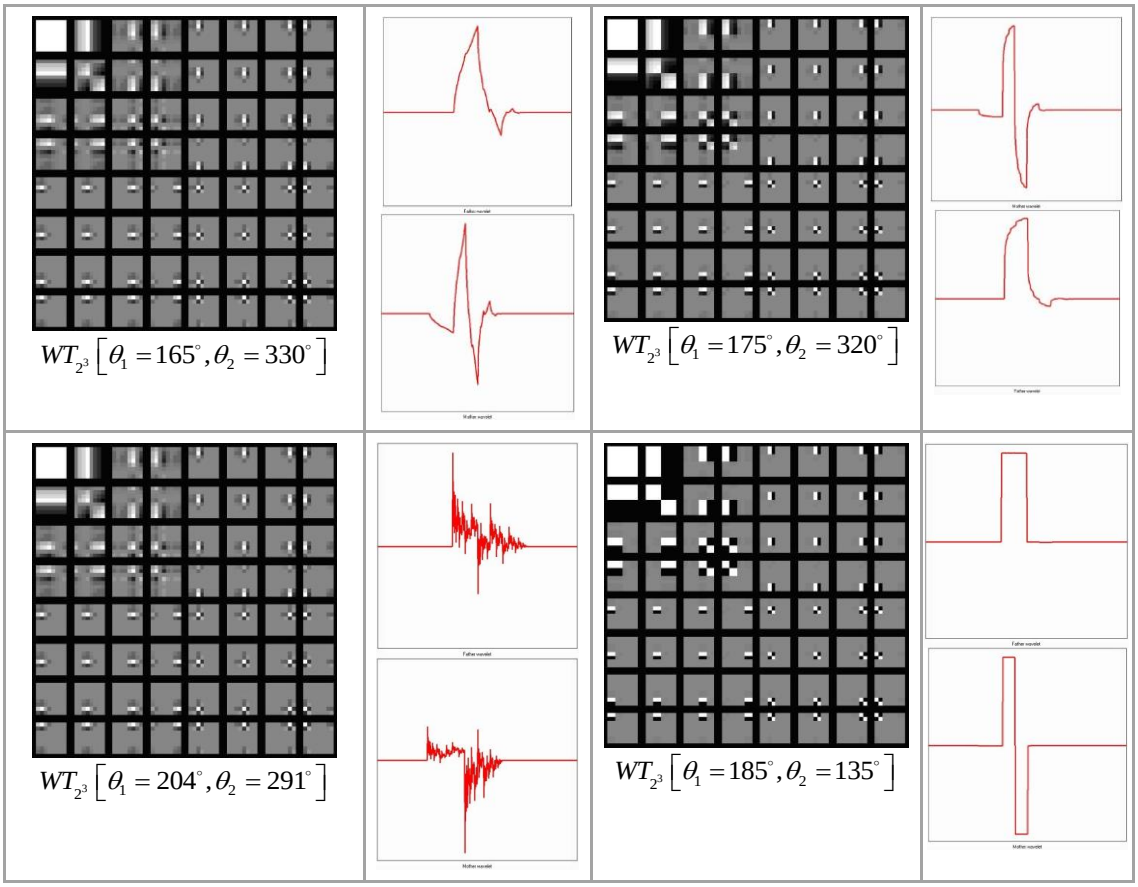


Рис 4. Двумерные базисные функции 2-параметрического вейвлет преобразования при различных значениях параметров и соответствующие им усредняющие функции (верхний красный график) и вейвлет всплески (нижний красный график)

Поиск пары ключей $(A_1,A_2,...,A_p)\in\mathbf{Tor}^p[0,2\pi]$ и $(b_1,b_2,...,b_N)\in\mathbf{B}_2^N$ (аналогового и цифрового) в пространстве ключей является трудной задачей для противника, например, при разархивации данных, сжатие которых осуществлялось с помощью МПП. Если же речь идет об OFDM ТКС, то используя МПП она может защитить себя путем изменения значений рабочих параметров по заранее известному передатчику и приемнику закону – детерминированному или псевдо-случайному (подобно тому, как современные ТКС меняют рабочую частоту), что в существенной мере усложняет задачу перехвата или подавления передаваемой информации. OFDM ТКС, основанная на МПП, а не на ДПФ, обладает дополнительными достоинствами по сравнению с классической ТКС: многопараметрические преобразования позволяют оптимизировать (и, следовательно, улучшить) технические характеристики системы (путем изменения параметров), таких как PAPR (peak to average power ratio), BER (bit error rate), SER (symbol error rate) и ISI (inter-symbol interference). Авторы заявки не знают научных трудов, посвященных анализу, синтезу и практическому применению подобных преобразований в междисциплинарных исследованиях.

В качестве приложения разрабатываемой теории МПП предлагается решение следующих трех междисциплинарных фундаментальных задач (МДФЗ).

МДФЗ №1: Разработка методов настойки МПП на решение оптимизационных задач теории цифровой обработки изображений. К их числу авторы проекта отнесли следующие три подзадачи (ПЗ):

ПЗ№1: Крипто-защищенное сжатие больших цифровых гиперспектральных данных ДЗЗ путем поиска таких значений рабочих параметров у МПП, при которых достигается минимальное значение энтропии спектра сигнала (изображения), которое означает, что при сжатии достигается максимальный коэффициент сжатия. На рис.5 представлен график зависимости энтропии двумерного спектра изображения «LENA» в 2-параметрическом вейвлет преобразовании. Видно, что график имеет несколько локальных минимумов. Соответствующие им параметры дают нам представление о том, какие реализации МПП могут дать максимальный коэффициент сжатия. Представляет интерес выяснить обладают ли другие МПП аналогичным свойством? Каким образом на подобное поведение влияют цифровые криптоключи $(b_1, b_2, ..., b_N) \in \mathbf{B}_2^N$?

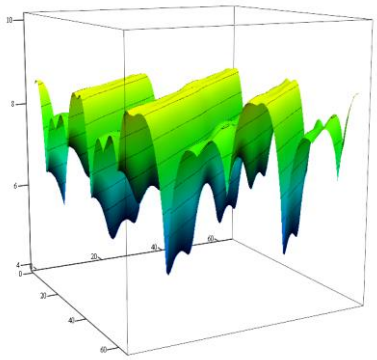


Рис 5. График зависимости энтропии двумерного спектра изображения «LENA» в двухпараметрическом вейвлет преобразовании.

ПЗ№2: Поиск такого оптимального МПП, которое минимизирует среднее внутриклассовое расстояние образов или максимизирует их межклассовое расстояние, что повышает вероятность правильного распознавания образов и их классификацию.

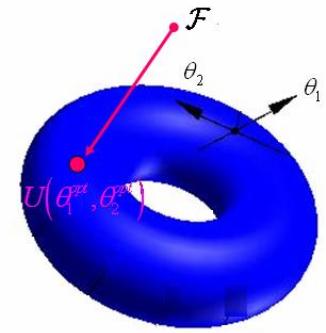


Рис 6. Двумерные базисные функции двух-параметрического вейвлет преобразования при различных значениях параметров и соответствующие им усредняющие функции (верхний красный график) и вейвлет всплески (нижний красный график)

ПЗ№3: Оптимальная аппроксимация многопараметрическим преобразованием $U(\theta_1, \theta_2, ..., \theta_p)$ (см. рис 6) наперед заданного одиночного преобразования F (у которого в настоящее время неизвестен быстрый алгоритм) путем нахождения соответствующих оптимальных значений параметров $(\theta_1^{opt}, \theta_2^{opt}, ..., \theta_p^{opt})$ (задача настройки МПП $U(\theta_1, \theta_2, ..., \theta_p)$ на заданное фиксированное преобразование F с целью нахождения у него быстрого алгоритма).

МДФЗ №2: Крипто-защищенное помехоустойчивое кодирование данных. В проекте синтезируются коды Рида-Соломона над конечными некоммутативными алгебрами Кэли-Дикссона, порождающие и проверочные матрицы которых совпадают с матрицами многопараметрического преобразования Фурье-Кэли-Диксона, оснащенными цифровыми ключами. Наличие быстрых алгоритмов у таких преобразований делает процедуры кодирования и декодирования вычислительно эффективными для законных пользователей. В противовес этому дешифрирование перехваченной шифрограммы для криптоаналитика представляется трудной задачей усугубленной наличием секретного цифрового ключа $(b_1, b_2, ..., b_N) \in \mathbf{B}_2^N$, связанного с некоммутативностью умножения в алгебре Кэли-Диксона.

МДФЗ №3: Разработка интеллектуальных OFDM телекоммуникационных систем помехо- и крипто-защищенной передачи больших цифровых видеоданных, основанных на быстрых МПП с аналоговыми и цифровыми криптоключами, которые используются вместо традиционного дискретного быстрого преобразования Фурье (БПФ). Разрабатываемые интеллектуальные OFDM телекоммуникационные системы будут способны оценивать состояние радиоканала и на основании полученной оценки перестраивать свою структуру с целью оптимизации своих тактико-технических характеристик для успешного противодействия пассивным и активным радиоатакам.

Предлагаемые подходы и методы, их обоснование для реализации цели и задачи проекта

В данном проекте мы интерпретируем мультиспектральные (*K*-канальные) изображения ДЗЗ не как векторно-значные, а как гиперкомплексно-значные т.е. как двумерные функции, принимающие значения в некоторой *K*-мерной гиперкомплесной алгебре **Alg**. Это позволяет нам перенести многие методы цифровой обработки изображений, основанные на использовании вещественных и комплексных чисел, на принципиально новую модель изображения в виде двумерной **Alg**-значной функции. Такой подход позволяет разработать достаточно эффективные алгоритмы обработки, сжатия и передачи гиперкомплексных изображений. Основной упор в проекте делается на построении математической теории многопараметрических преобразований и их применении при решении трех междисциплинарных фундаментальных задач (МДФЗ), перечисленных в п 4.3, а именно:

МДФЗ №1: Разработка стратегий настойки МПП на решение оптимизационных задача теории цифровой обработки изображений. К их числу авторы проекта отнесли следующие три подзадачи.

ПЗ№1: Крипто-защищенное сжатие больших цифровых гиперспектральных данных ДЗЗ путем поиска таких значений рабочих параметров у МПП, при которых достигается минимальное значение энтропии спектра сигнала (изображения), которое означает, что при сжатии достигается максимальный коэффициент сжатия. Наличие цифрового ключа $(b_1, b_2, ..., b_N) \in \mathbf{B}_2^N$ гарантирует высокую степень крипто-защищенности. При решении этой задачи мы предполагаем, что элементы изображения (гиперспектральные пиксели) являются не многомерными векторами, а многомерными гиперкомплексными числами, принадлежащими некоторой некоммутативной алгебре **Alg**, что и позволяет использовать некоммутативность умножения для создания цифрового ключа. В этом случае становятся безсмысленными многочисленные исследования, посвященные изучению сжимающих свойств известных и новых одиночных ортогональных преобразований.

ПЗ №2: Поиск такого оптимального МПП, которое минимизирует среднее внутриклассовое расстояние образов или максимизирует их межклассовое расстояние, что повышает вероятность правильного распознавания образов и их классификацию.

ПЗ №3: Оптимальная аппроксимация многопараметрическим преобразованием наперед заданного одиночного преобразования (у которого в настоящее время неизвестен быстрый алгоритм) путем нахождения соответствующих значений параметров у МПП (так называемая задача настройки на заданное фиксированное преобразование с целью нахождения у него быстрого алгоритма).

МДФЗ №2: Крипто-защищенное помехоустойчивое кодирование данных. Известно, что задача декодирования произвольного двоичного линейного кода, является NP-полной задачей. Однако, при наличии априорной информации о типе кода, задача декодирования перестает быть трудной и

может быть решена за полиномиальное время. Основная причина низкой криптостойкости систем шифрования, основанных на помехоустойчивых кодах, состоит в том, что все они используют коммутативные поля Галуа. Именно коммутативность основного поля является главным фактором низкой сложности задачи декодирования. В проекте синтезируются коды Рида-Соломона над конечными некоммутативными алгебрами Клиффорда и Кэли-Дикссона (**Alg=КА и Alg=КДА),** порождающие и проверочные матрицы которых совпадают с матрицами преобразования Фурье-Клиффорда или Фурье-Кэли-Диксона, оснащенными цифровыми ключами. Наличие быстрых алгоритмов у таких преобразований делает процедуры кодирования и декодирования вычислительно эффективными для законных пользователей. В противовес этому дешифрирование перехваченной шифрограммы для криптоаналитика представляется как задача декодирования произвольного линейного кода, которая является трудной задачей усугубленной наличием секретного цифрового ключа $\left(b_1, b_2, ..., b_N\right) \in \mathbf{B}_2^N$.

МДФЗ №3: Разработка интеллектуальных OFDM телекоммуникационных систем (ТКС) помехо- и крипто-защищенной передачи больших цифровых видеоданных, основанных на быстрых МПП с аналоговыми и цифровыми криптоключами, которые используются вместо традиционного дискретного быстрого преобразования Фурье (БПФ). Разрабатываемые интеллектуальные OFDM ТКС будут способны оценивать состояние радиоканала и на основании полученной оценки перестраивать свою структуру с целью оптимизации своих тактико-технических характеристик для успешного противодействия пассивным и активным радиоатакам.

Как известно, радиотехническая разведка предполагает последовательное выполнение трех основных задач: обнаружение факта работы радиоэлектронной или телекоммуникационной системы (обнаружение сигнала), определение структуры обнаруженного сигнала (на основе определения его параметров) и раскрытие содержащейся (передаваемой) в сигнале информации. Перечисленным задачам радиотехнической разведки могут быть противопоставлены три вида скрытности сигналов: структурная, информационная и энергетическая. Структурная скрытность характеризует способность противостоять мерам радиотехнической разведки, направленным на раскрытие сигнала (распознавание его формы), т.е. отождествление обнаруженного сигнала с одним из множества априорно известных сигналов. Следовательно, для увеличения структурной скрытности необходимо иметь по возможности большой ансамбль используемых сигналов и достаточно часто изменять форму сигналов.

Для решения этой задачи мы предлагаем использовать несколько типов многопараметрических преобразований $U^{(b_1, b_2, ..., b_N)}\left(\theta_1, \theta_2, ..., \theta_p\right) = \left[\mathrm{mp}_k^{b_k}\left(n \mid \theta_1, \theta_2, ..., \theta_p\right)\right]_{k,n=1}^{N}$, столбцы $\left\{\mathrm{mp}_k^{b_k}\left(n \mid \theta_1, \theta_2, ..., \theta_p\right)\right\}_{k=1}^{N}$ которых образуют многопараметрические поднесущие (subcarriers)

$$\mathrm{sub}_k^{b_k}\left(n \mid \theta_1, \theta_2, ..., \theta_p\right) = \mathrm{mp}_k^{b_k}\left(n \mid \theta_1, \theta_2, ..., \theta_p\right)$$

для интеллектуальной OFDM-ТКС. При изменении параметров меняется форма поднесущих, которые остаются при этом ортогональными. Поднесущие $\left\{\mathrm{sub}_k^{b_k}\left(n \mid \theta_1, \theta_2, ..., \theta_p\right)\right\}_{k=1}^{N}$ являются переносчиками информации. В классической OFDM-ТКС ими являются узкополосные гармонические сигналы

$$\mathrm{sub}_k(n) = \exp(j2\pi kn/N) = \cos(2\pi kn/N) + j\sin(2\pi kn/N),$$

идентификация которых средствами радиоэлектронной разведки не представляет особой трудности, что свидетельствует о крайне высокой уязвимости подобных систем к различного типа атакам (например, прослушивание и подавление). В классической OFDM ТКС, основанной на ДПФ, передаваемое сообщение преобразуется ДПФ с помощью быстрого преобразования Фурье (БПФ). Это эквивалентно модуляции гармонических поднесущих $\exp(j2\pi kn/N)$ символами передаваемого сообщения (обычно используется QAM или QPSK модуляции) и их суммировании в один групповой сигнал, который и передается на несущей частоте. В разрабатываемой Intelligent-OFDM ТКС передаваемое сообщение преобразуется **Alg**-значным МПП $U^{(b_1, b_2, ..., b_N)}\left(\theta_1, \theta_2, ..., \theta_p\right)$, которое также обладает быстрым алгоритмом, аналогичным БПФ. Это эквивалентно модуляции многопараметрических **Alg**-значных поднесущих символами сообщения и их суммировании в один групповой сигнал, который также передается на несущей частоте.

Форма поднесущих зависит от параметров МПП, меняя которые можно менять форму поднесущих, реализуя тем самым структурную скрытность ТКС. Например, если вместо ДПФ

использовать дробное преобразование Фурье (одно из самых простейших однопараметрических преобразований), то при изменении параметра от 0 до 2π поднесущие меняются от прямоугольных импульсов (используемых в TDM-ТКС) до классических комплексных гармоник (используемых в классической OFDM-ТКС). В промежутках между этими крайними значениями поднесущие имеют форму широкополосных Чирп-функций (ЛЧМ-сигналов) с различной базой. Более сложную форму поднесущие имеют, например, у МПП Голея и многопараметрических вейвлет преобразований. При некоторых значениях параметров они принимают вид хаотических δ-коррелированных сигналов.

Информационная скрытность в нашем подходе обеспечивается связкой из двух ключей для вхождения в Intelligent-OFDM ТКС. Как мы уже отмечали, количество параметров (углы, меняющие свои значения от 0 до 2π) может достигать 10000. Область значений параметров представляет собой 10000-мерный тор. Набор рабочих значений параметров являются первым ключом для вхождения в Intelligent-OFDM ТКС. Поиск этого ключа путем сканирования 10000-мерного куба является трудной задачей (значительно более трудной, чем сканирование 1-мерной радиочастотной оси).

Но даже, если этот ключ в процессе радиоэлектронной борьбы будет определен противником, то Intelligent-OFDM ТКС может изменить свои параметры и далее передавать конфиденциальную информацию на новых поднесущих (в новом ортогональном базисе), тем самым противодействуя радиоэлектронным атакам (перехвату или глушению). Intelligent-OFDM ТКС может защитить себя также путем изменения значений параметров по заранее известному передатчику и приемнику закону – детерминированному или псевдослучайному (подобно тому, как современные ТКС меняю рабочую частоту), что в существенной мере усложняет задачу перехвата или подавления передаваемой информации. Второй ключ формируется при использовании кватернионного многопараметрического преобразования (например, дробного кватернионного преобразования Фурье). Поднесущими такого преобразования являются кватернионно-значные «гармоники». Так как умножение кватернионов некоммутативно, то их модуляция и демодуляция может быть некоммутативной. В нашем подходе каждая гармоника оснащается ключом, который указывает с какой стороны значения кватернионно-значной поднесущей умножаются (с правой или левой). Если для передачи используется, например, 1024 поднесущие, то кватернионно-значное преобразование оснащается 1024 разрядным ключом. Конкретное значения ключа (число таких значений равно 2 в степени 1024) необходимо знать противнику для корректной демодуляции передаваемых конфиденциальных сообщений. Наличие связки из двух ключей делает систему информационно скрытной на физическом уровне. Энергетическая скрытность характеризует способность Intelligent-OFDM ТКС работать в условия, когда отношение сигнал/шум в канале связи меньше единицы. Хорошо известно, что энергетическая скрытность достигается использованием широкополосных ортогональных последовательностей (например, М-последовательностей) в качестве поднесущих. В нашем подходе это требование выполняется «автоматически», так как многопараметрические преобразования являются ортогональными и при определенных значениях параметров соответствующие им поднесущие являются широкополосными (шумоподобными) сигналами.

Такое сквозное использование многопараметрических преобразований при решении фундаментальных междисциплинарных задач цифровой обработки больших видеоданных в мировой практике применяется впервые. Оно позволяет разработать эффективные алгоритмы обработки, кодировании, приема и передачи гиперкомплексных изображений.

Фундаментальная научная проблема, на решение которой направлен проект, и фундаментальные задачи, вытекающие из нее, сформулированы в Приоритетных направлениях развития науки и техники в разделе «Информационно-телекоммуникационные технологии», а также в критических технологиях в разделах «**15.** Технологии обработки, хранения, передачи и защиты информации», «**19.** Технологии производства программного обеспечения». Она входит в перечень основных направлений технологической модернизации экономики России: «**3.** Космические технологии, прежде всего связанные с телеком-муникациями, включая ГЛОНАСС и программу развития наземной инфраструктуры», «**5.** Стратегические информационные технологии, включая вопросы создания суперкомпьютеров и разработки программного обеспечения».

Все подходы, которые будут использованы в данном проекте, основываются на новых теоретических результатах, полученных в ранее проведенных фундаментальных исследованиях, поддержанных РФФИ.