


Комплексное повышение эффективности радиоэлектронных устройств и систем передачи информации с OFDM на основе нелинейных систем с динамическим хаосом

М.Ю. Зуев 

Казанский национальный исследовательский технический университет имени А.Н. Туполева – КАИ
420111, Россия, г. Казань,
ул. К. Маркса, 10

Аннотация – В данной статье представлены результаты моделирования системы передачи информации с OFDM с использованием цифровых радиоэлектронных устройств, реализующих метод скремблирования передаваемых сигналов и маскирования передаваемой информации. В качестве источников маскирующих сигналов в работе рассматриваются псевдослучайные последовательности, полученные с помощью генераторов, построенных на основе модифицированных систем с динамическим хаосом. Получены оценки вероятности битовой ошибки рассматриваемой системы передачи информации, оценен пик-фактор сигналов, корреляционные характеристики скремблированной и исходной информации, получена оценка энтропии передаваемой информации. Результаты работы могут быть использованы при проектировании современных систем передачи информации с целью повышения безопасности передаваемой информации и снижения пик-фактора формируемых сигналов.

Ключевые слова – псевдослучайная последовательность; OFDM; скремблирование сигналов; маскирование информации; информационная безопасность; пик-фактор.

Введение

В настоящее время в области систем телекоммуникаций и радиосвязи наблюдается тенденция по разработке малогабаритных портативных устройств передачи информации и снижению их энергопотребления. Все большую актуальность приобретают вопросы повышения информационной безопасности, улучшения энергетической и спектральной эффективности современных систем передачи информации, а также устройств, работающих в коммуникационных линиях device-to-device, vehicle-to-vehicle, machine-to-machine и т. д. [1].

Повышение требований к конфиденциальности передачи информации делает актуальным использование хаотической динамики в системах связи (маскирование информации динамическим хаосом, переключение хаотических режимов и т. д.) [2]. В отличие от аналоговых реализаций радиоэлектронных динамических систем с хаотической динамикой цифровые реализации этих систем на основе процедур численного интегрирования дифференциальных уравнений позволяют получить воспроизводимость характеристик как на передающем, так и на приемном концах канала связи. Одним из возможных вариантов повышения эффективности радиоэлектронных устройств с хаотической динамикой является формирование

квазирезонансных управляющих воздействий на параметры динамических систем. Таким образом можно улучшить статистические характеристики формирователей сигналов, генерируемых нелинейными системами с динамическим хаосом [1; 3]. Оценки статистических характеристик систем с динамическим хаосом, функционирующих в условиях квазирезонансных воздействий, приведены в работах [4–7]. Для решения задачи комплексного повышения эффективности радиоэлектронных устройств и систем передачи информации с OFDM и упрощения их реализации на основе цифровой техники вместо воспроизводимых генераторов хаоса, в которых операции производятся с плавающей или фиксированной запятой, более привлекательными являются генераторы псевдослучайных сигналов, в которых операции производятся над целочисленными полями Галуа $GF(2^P)$ [8].

Одними из наиболее известных методов улучшения энергетической эффективности современных систем связи с OFDM являются использование дискретного преобразования Фурье, адаптивного предсказания информации, блочного и сверточного кодирования [9; 10].

В работе [11] представлен метод скремблирования полезной информации последовательностями, полученными на основе динамического хаоса, используемого для повышения информационной безопасности на физическом уровне (TRANSEC)

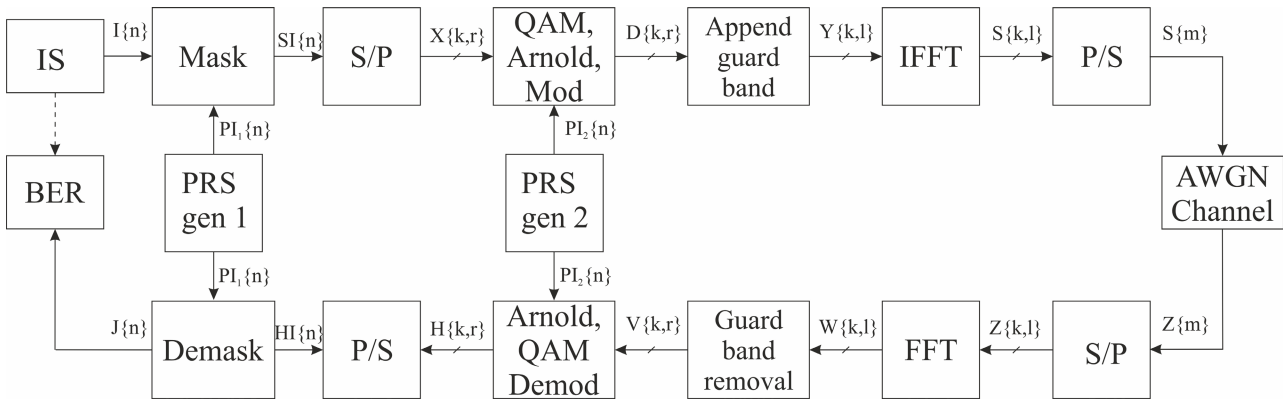


Рис. 1. Структурная схема исследуемой OFDM-системы, используемая для статистического моделирования
Fig. 1. Block diagram of the investigated OFDM system used for statistical modeling

и уменьшения значения пик-фактора (PAPR) в оптической системе передачи информации на основе OFDMA.

В статье [12] предложен метод снижения PAPR, заключающийся в обработке поднесущих частот группового спектра и повороте сигнального созвездия с помощью матрицы предкодирования. Функция предкодирования реализуется таким образом, чтобы амплитудные выбросы сигнала не появлялись в одно и то же время. Для этого разрабатывается одна основная часть функции, а остальная порождается циклическими сдвигами излучения в интервале времени, равном периоду. В статье произведена оценка эффективности снижения PAPR такими функциями, как: дискретное преобразование Хартли, дискретное косинусное преобразование, дискретное синусное преобразование, быстрое преобразование Уолша – Адамара, дискретное преобразование Фурье, представлена имитационная модель с использованием полученных функций предкодирования.

В работе [13] предлагается метод адаптивного кодирования с предварительным искажением. Метод кодирования используется для исправления ошибок, а также снижения пик-фактора, а метод предварительного искажения обеспечивает такую форму передаваемых данных или входного сигнала усилителя (предыскаженного сигнала), чтобы выходной сигнал усилителя был менее искажен. Предварительное искажение также улучшает спектр плотности мощности передаваемого сигнала и характеристику битовой ошибки.

Проблема комплексного повышения эффективности радиоэлектронных устройств и систем передачи информации включает в себя проблемы энергетической эффективности и информационной безопасности на физическом уровне (TRANSEC).

Задача разработки новых методов и средств повышения энергетической эффективности и информационной безопасности для систем передачи информации с ортогональным частотным мультиплексированием является актуальной из-за высокой спектральной эффективности, способности работать в условиях многолучевого распространения радиоволн и высокой пропускной способности этих систем.

Целью работы является анализ возможности комплексного повышения эффективности функционирования радиотехнических устройств и систем передачи информации с OFDM на основе использования нелинейных систем с динамическим хаосом, реализованных над конечным полем Галуа $GF(2^p)$.

1. Описание структурной схемы, используемой для статистического моделирования

В данной работе рассматривается модель системы связи с OFDM, в которой передаваемая информация скремблируется с помощью псевдослучайных последовательностей, сформированных на основе системы Лоренца, реализованной над полем $GF(2^p)$:

$$\begin{cases} X_{i+1} = X_i \oplus t \cdot c \cdot (X_i \oplus Y_i), \\ Y_{i+1} = Y_i \oplus t \cdot (r \cdot X_i \oplus Y_i \oplus X_i \cdot Z_i), \\ Z_{i+1} = Z_i \oplus t \cdot (b \cdot Z_i \oplus X_i \cdot Y_i), \end{cases} \quad (1)$$

где \oplus – операция исключающее «ИЛИ», « \cdot » – операция умножения, p – степень полинома, образующего поле, полином образующий поле $g(x) = x^{16} + x^{12} + x^3 + x + 1$.

Структурная схема исследуемой модели системы передачи информации с OFDM, используемая для оценки вероятностных и энергетических характеристик, приведена на рис. 1.

В работе рассматривается сопоставление одно-контурного и двухконтурного методов повышения эффективности функционирования устройств и систем передачи информации с OFDM. Первый метод заключается в одноконтурном скремблировании сигнального QAM созвездия с помощью преобразования Арнольда, коэффициентами которого являются элементы псевдослучайной последовательности, формируемой на основе системы Лоренца, реализованной над полем Галуа. Второй метод состоит в маскировании исходной информации с помощью псевдослучайных последовательностей, также получаемой на основе системы Лоренца и скремблировании сигнального QAM созвездия с помощью преобразования Арнольда.

На структурной схеме (рис. 1) IS – источник информации формирует исходный байтовый поток $I\{n\}$, затем блок маскирования (Mask) маскирует этот поток последовательностью $PI_1\{n\}$, сформированной целочисленным генератором псевдослучайных последовательностей (PRS gen 1), полученный байтовый массив $SI\{n\}$ последовательно-параллельным преобразователем (S/P) преобразуется в матрицу $X\{k, r\}$, которая квадратурно-амплитудным модулятором (QAM mod) преобразуется в квадратурный сигнал, который затем с помощью преобразования Арнольда (Arnold Mod) скремблируется с массивом $PI_2\{n\}$, сформированным целочисленным генератором псевдослучайных последовательностей (PRS gen 2), к полученному массиву $D\{k, r\}$ добавляется защитная полоса (Append guard band), над матрицей $Y\{k, l\}$ производится построчное обратное преобразование Фурье IFFT, полученный массив $S\{k, l\}$ параллельно-последовательным преобразователем преобразуется в одномерный массив $S\{m\}$, затем с помощью блока (AWGN Channel) производится имитация канала связи с аддитивным белым гауссовым шумом.

На приемной стороне оцифрованная принятая смесь сигнала с шумом $Z\{m\} = S\{m\} + G_n\{m\}$ (где $G_n\{m\}$ – реализация шума) проходит последовательно-параллельное преобразование S/P, затем полученный массив построчно пропускается через блок прямого преобразования Фурье (FFT), в блоке (Guard interval removal) производится удаление защитного интервала $V\{k, r\}$, затем, используя массив $PI_2\{n\}$, сформированный целочисленным генератором псевдослучайных последовательностей (PRS gen 2), производится обратное преобразование Арнольда (Arnold Demod) полученного ком-

плексного массива, после которого производится квадратурная демодуляция (QAM demod) принятого сигнала, полученный символьный массив $H\{k, r\}$ последовательно-параллельным преобразователем преобразуется в массив $HI\{n\}$, перемешивая который с последовательностью $PI_1\{n\}$, сформированной целочисленным генератором псевдослучайных последовательностей (PRS gen 1), производится демаскирование полученного сигнала (Demask), полученный в результате преобразований массив $J\{n\}$ в блоке BER сравнивается с исходным битовым потоком $I\{n\}$, затем оценивается зависимость вероятности ошибки от E_b/N_0 .

Отличие исследуемой структурной схемы от используемой в классической системе передачи информации с OFDM состоит в добавлении маски, сформированной генератором псевдослучайных последовательностей с помощью преобразования Арнольда и посимвольного скремблирования.

Реализация генераторов PRS gen1, PRS gen2 на основе системы Лоренца над полем Галуа и в программируемой логической интегральной схеме была рассмотрена в работах [5; 6; 8]. Преимуществом генераторов, реализованных на поле Галуа, является отсутствие операций с плавающей либо фиксированной точкой, что обеспечивает их реализацию в относительно простых устройствах, имеющих низкую стоимость.

Требованиями, предъявляемыми к скремблирующим последовательностям, генерируемым данными генераторами, являются равномерность формируемых чисел с доверительной вероятностью не менее 0,95 и период автокорреляционной функции не менее 100 000 отсчетов.

В работе для анализа характеристик устройств комплексного повышения эффективности систем передачи информации используется метод компьютерного моделирования в среде Matlab.

2. Оцениваемые показатели

В современных системах передачи информации возникновение ошибок является неизбежным. Ошибки являются следствием воздействия аддитивных шумов и помех, искажений, связанных с многолучевым распространением радиоволн, частотной, фазовой или символьной рассинхронизации. В связи с этим при проектировании и разработке систем передачи информации следует учитывать комплекс характеристик этих систем [14]. В качестве характеристик, оценивающих эффективность решения задач улучшения инфор-

мационной безопасности, в работе используются: коэффициент корреляции между соседними столбцами и строками C , энтропия маскированной информации $H(x)$ и степень скремблирования SD . Для оценки возможности повышения энергетической эффективности взяты такие характеристики, как: пик-фактор $PAPR$ и кумулятивная функция распределения сигнала (CCDF).

Функция BER является вероятностью ошибочного приема при передаче одного бита информации, усредненной для статистически большого объема передаваемой информации, и используется для верификации разработанной статистической модели системы. Например, в случае QAM-модуляции и канала с аддитивным белым гауссовым шумом BER может быть теоретически оценена как:

$$BER \leq \frac{1}{\log_2 M} \left[1 - \left(1 - 2 \operatorname{erf} \left(\sqrt{\frac{3 \log_2 M E_b}{M-1 N_0}} \right) \right)^2 \right], \quad (2)$$

где erf – интеграл ошибок, M – число позиций для многопозиционных видов модуляции, E_b – энергия, необходимая для передачи одного бита информации, N_0 – спектральная плотность мощности белого шума в канале.

Одним из основных показателей степени улучшения информационной безопасности системы является коэффициент корреляции (3). Коэффициент корреляции между соседними парами векторов хаотической перестановки используется для оценки способности противостоять статистической атаке [1], оценивается по следующей формуле:

$$C(u, v) = \frac{\sum_{i=1}^N (u_i - E(u))(v_i - E(v))}{\sqrt{\sum_{i=1}^N (u_i - E(u))^2} \sqrt{\sum_{i=1}^N (v_i - E(v))^2}}, \quad (3)$$

где u и v – сгенерированные перестановки, порожденные хаотическими последовательностями; N – число перестановок; $E(u)$ и $E(v)$ – средние значения u и v , соответственно.

В то же время степень скремблирования (SD) также используется для оценки безопасности систем защиты информации. Чем больше степень скремблирования, тем лучше маскируется исходная информация. В работе [1] SD оценивается по следующей формуле:

$$SD = \frac{\sum_{t=1}^T \sum_{n=1}^N R(t, n)}{TN} 100 \%, \quad (4)$$

$$R(t, n) = \begin{cases} 0, & c_n(t) = w_n(t), \\ 1, & c_n(t) \neq w_n(t), \end{cases} \quad (5)$$

где $c_n(t)$ и $w_n(t)$ – символы QAM до и после скремблирования соответственно; T – количество дискретных отсчетов; t – номер отсчета; n – индекс поднесущей.

Энтропия является мерой неопределенности информационной системы, в частности это функция непредсказуемости появления какого-либо символа первичного алфавита. Чем больше независимость сформированной информации, тем система считается более безопасной с точки зрения информационной безопасности. Выделяют общую и локальную энтропию.

Общая энтропия оценивается как:

$$H(X) = - \sum_{i=1}^m p(x_i) \log(p(x_i)). \quad (6)$$

Вычисление локальной энтропии сводится к нахождению для каждого отсчета изображения энтропии его окрестности – фрагмента размером $m \times n$:

$$H(X) = - \sum_{i=1}^m \sum_{j=1}^n p(e_{i,j}) \log(p(e_{i,j})), \quad (7)$$

событием ($e_{i,j}$) считается конкретное значение яркости пикселя, вероятность его ($p(e_{i,j})$) оценивается подсчетом количества вхождений этого значения по всему фрагменту изображения размером $m \times n$ и делением на количество пикселей во фрагменте.

Известным недостатком систем передачи информации, в которых применяется OFDM, является высокое отношение пиковой мощности к средней ее величине – высокий пик-фактор ($PAPR$) сигнала, который оценивается по следующей формуле:

$$PAPR_{dB} = 10 \log_{10} \frac{|x|_{peak}^2}{x_{rms}^2}, \quad (8)$$

где x_{peak}^2 – квадрат максимальной амплитуды, x_{rms}^2 – квадрат среднего значения амплитуды сигнала. Поэтому в данной работе выполнены оценки пик-фактора сигналов, полученных при моделировании схемы, приведенной на рис. 1.

Для оценки распределения получаемых значений пик-фактора формируемых сигналов удобно использовать кумулятивную функцию распределения (CCDF).

В качестве модели исходной информации с целью наглядного представления используются 8-битные изображения: перца, женщины, а также изображения клеток разной интенсивности и размера. Размер передаваемых изображений составлял 256×256 пикселей. Следует отметить,

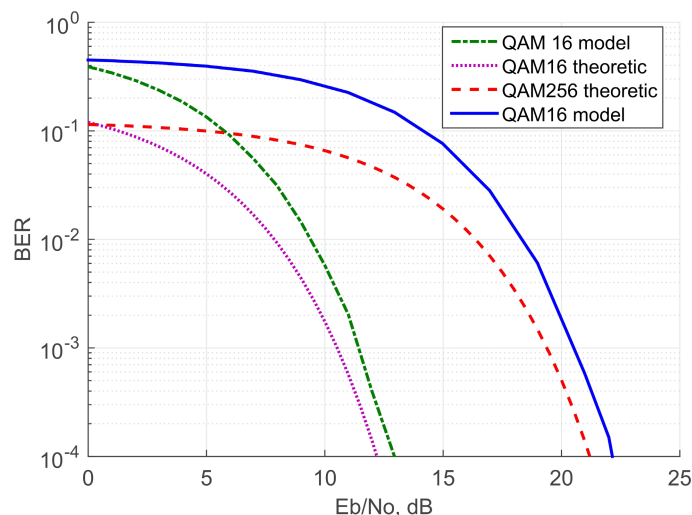


Рис. 2. Зависимости оценки вероятности битовой ошибки от отношения сигнал/шум E_b/N_0
 Fig. 2. Dependences of the estimate of the bit error probability on the signal-to-noise ratio E_b/N_0

что значения пик-фактора (8), оцененные в работе и использованные для построения CCDF, рассчитаны по массиву всей информации, несущей изображение.

3. Результаты компьютерного моделирования

В эксперименте в системе связи информация об изображении передавалась с помощью 256 поднесущих, а в качестве модуляции использовались QAM-16 и QAM-256. К квадратурам передаваемого сигнала добавлялся аддитивный белый гауссов шум AWGN. Затем полученные символы сигнального созвездия с помощью преобразования Арнольда скремблировались со псевдослучайной последовательностью.

С целью верификации разработанной модели в статье проведены оценки вероятности ошибки на бит BER от отношения энергии на бит к спектральной плотности мощности шума E_b/N_0 для OFDM-сигнала, маскированного псевдослучайной последовательностью, полученные зависимости приведены на рис. 2.

Из рис. 2 теоретически достижимые (theoretic) и полученные методом статистического моделирования (model) зависимости вероятности битовой ошибки от энергии на бит к спектральной плотности мощности близки, что подтверждает соответствие исследуемой модели системе связи с OFDM [15].

На рис. 3 показаны передаваемые изображения женщины, перца, мелко и крупнозернистой клетки.

На рис. 3, а содержится изображение женщины, используемое в эксперименте по оценке пик-

фактора, на рис. 3, б приведено изображение клетки размером 4 пикселя, используемое для оценки пик-фактора, на рис. 3, в приведено изображение клетки размером 16 пикселей, на рис. 3, г – изображение до передачи по каналу связи, д – скремблированное изображение в канале связи, е – маскированное и прошедшее скремблирование изображение. Рис. 3 иллюстрирует, что в процессе передачи изображения по каналу связи производится скремблирование формируемого сигнала и маскирование передаваемой информации, после которых невозможно визуально восстановить очертания передаваемого изображения рис. 3, е, а следовательно, будет затруднительно восстановить информацию, скрытую исследуемыми методами. При этом следует учитывать, что для QAM-16 одноконтурный метод рис. 3, д не так эффективен, как двухконтурный (рис. 3, е).

Для определения влияния коррелированности передаваемой информации на пик-фактор сигнала в работе проведена оценка зависимости среднего значения пик-фактора от зернистости (размера клетки) передаваемого изображения до и после скремблирования сигнала (рис. 4).

Из рис. 4 видно, что при увеличении размера клетки увеличивается значение пик-фактора формируемого сигнала. Показано, что после скремблирования информации во всех экспериментах наблюдается снижение значения пик-фактора сформированных сигналов.

В целях анализа влияния формы передаваемой информации при экспериментальных проверках было проведено сопоставление оценок значений CCDF для изображений, несущих смысловую ин-

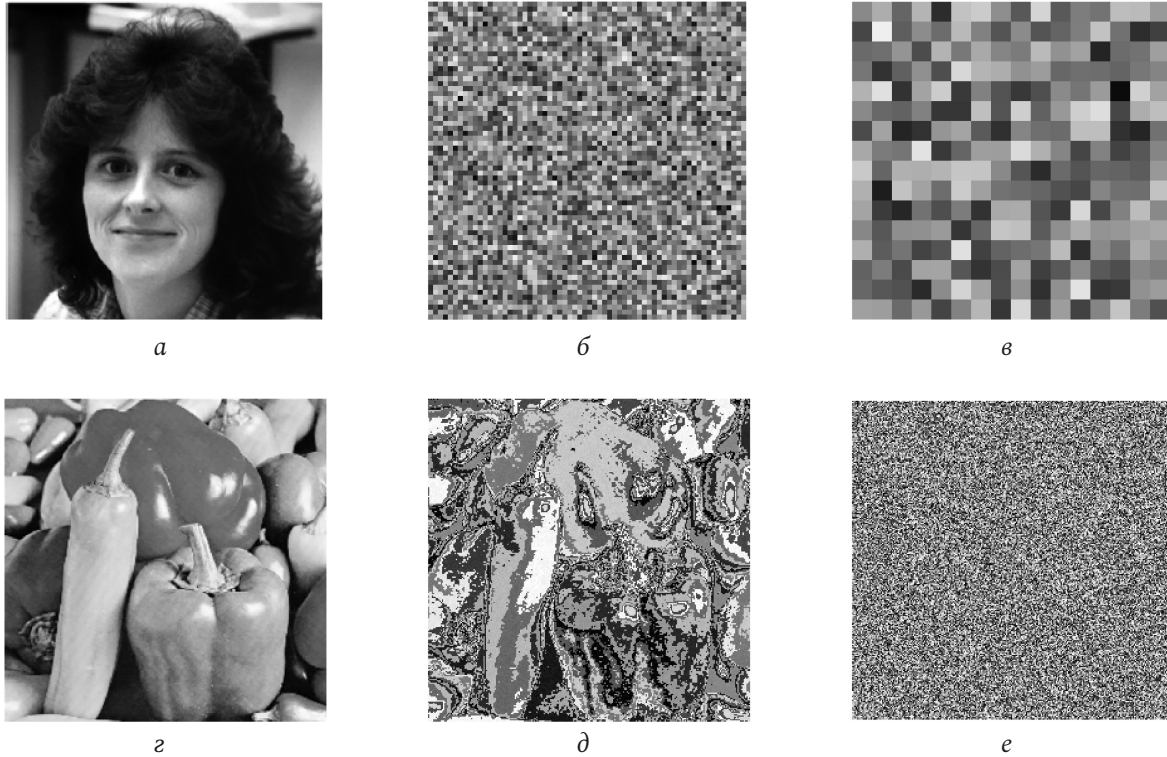


Рис. 3. Исходные фотографии и результаты их преобразования
Fig. 3. Initial photos and the results of their scrambling

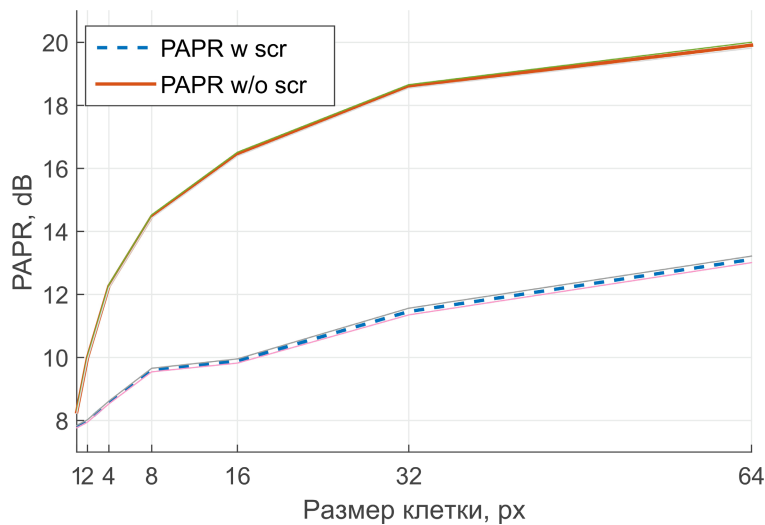


Рис. 4. Зависимость пик-фактора от размера клетки
Fig. 4. Dependence of the peak-to-average power ratio on the cell size

формацию, а также мелко- и крупнозернистых изображений.

На рис. 5 приведены кумулятивные функции распределения пик-фактора OFDM-сигнала, несущего информацию об изображении, с размерностью обратного преобразования Фурье 256 и исходного сигнала QAM-16.

Из рис. 5 видно, что для скремблированных сигналов при передаче изображения типа перца (pepper) значение пик-фактора принимаемых сиг-

налов превышает 15,5 дБ с вероятностью не более 0,001, выигрыш составляет 1 дБ, для изображения типа женщины (woman) пик-фактор принимаемых сигналов превышает 13,5 дБ с вероятностью не более 0,001 и выигрыш составляет 3 дБ. Для маскированной информации и скремблированных сигналов при передаче изображения типа перца (pepper) значение пик-фактора принимаемых сигналов превышает 11 дБ с вероятностью не более 0,001, выигрыш составляет 5 дБ, для изо-

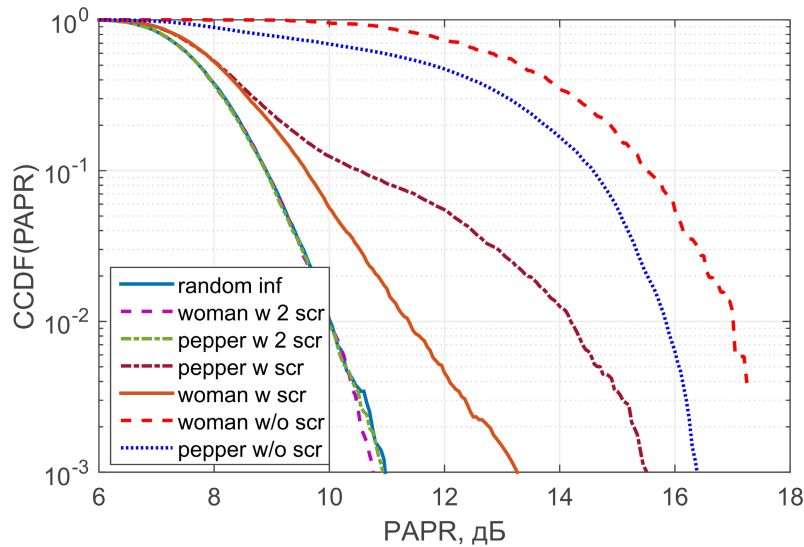


Рис. 5. Кумулятивная функция распределения
 Fig. 5. Cumulative distribution function

бражения типа женщины (woman) пик-фактор принимаемых сигналов превышает 11 дБ с вероятностью не более 0,001 и выигрыш составляет 7 дБ. Из приведенных зависимостей видно, что на снижение пик-фактора формируемых сигналов в одноконтурной схеме влияет форма исходной информации. В двухконтурной схеме влияние информации на пик-фактор формируемого сигнала минимально.

Немаловажную роль в современных системах коммуникаций играет информационная безопасность. Скремблирование позволяет повысить конфиденциальность информации и тем самым улучшить информационную безопасность. Для скремблирования на передающей и приемной сторонах системы связи используются идентичные псевдослучайные последовательности. Несанкционированный пользователь как постороннее лицо не имеет информации о начальных условиях, используемых генератором для формирования псевдослучайных последовательностей и не может демаскировать передаваемую информацию.

В таблице приведены результаты оценок характеристик информационной безопасности и улучшения энергетической эффективности, полученные при проведении экспериментов по передаче изображения, приведенного на рис. 3, 2, рассматриваемыми методами.

Из таблицы видно, что для одноконтурной схемы маскирования изображения получены приемлемые результаты по снижению пик-фактора как для QAM-16, так и для QAM-256, степень скремблирования для двухконтурной схемы достигает значений не менее 97 %. Общая энтропия увели-

Таблица. Характеристики информационной безопасности и улучшения энергетической эффективности
 Table. Characteristics of information security and energy efficiency improvements

Передаваемое изображение	Маскированное изображение	Дважды маскированное изображение	Передаваемое изображение	Маскированное изображение	Дважды маскированное изображение
QAM-16			QAM-256		
Энтропия			Энтропия		
7,749	7,974	7,997	7,749	7,978	7,998
Локальная энтропия			Локальная энтропия		
6,685	7,583	7,813	6,685	7,801	7,910
Пик-фактор			Пик-фактор		
17,93	13,09	10,4	20,14	11,3 ~ 11,8	9,8 ~ 10,5
Степень скремблирования			Степень скремблирования		
0	0,73	0,97	0	0,95	0,99

чивается и для одноконтурной схемы позволяет достичь значений 7,974, для двухконтурной – 7,998, локальная энтропия увеличивается от значений 6,685 до 7,910 для двухконтурной схемы, что является подтверждением лучшего перемешивания передаваемой информации.

На рис. 6 приведены гистограммы распределения по градациям яркости исходного, маскиро-

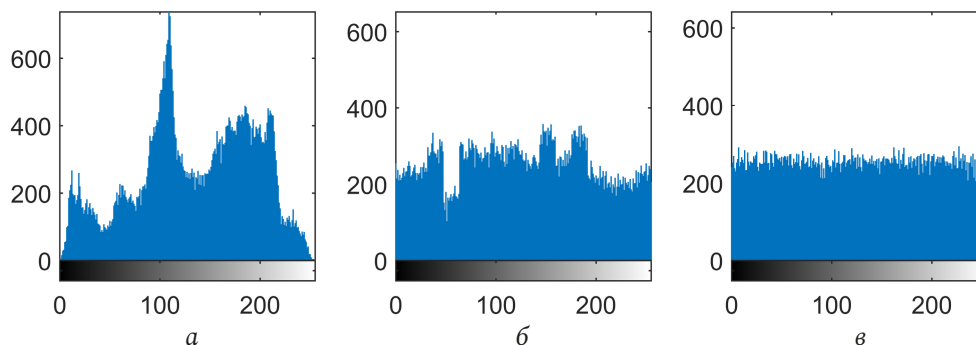


Рис. 6. Распределение градаций яркости исходного и маскированного изображений
Fig. 6. Distribution of shades of the original and masked images

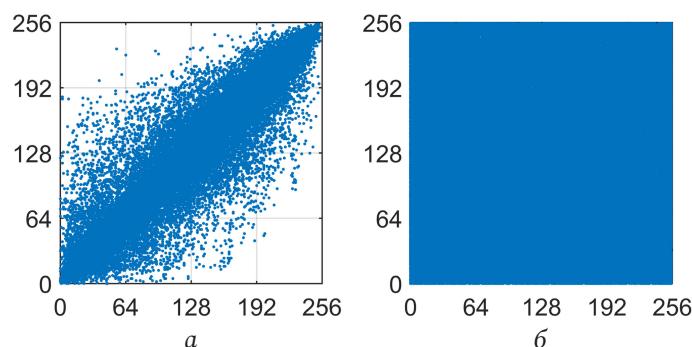


Рис. 7. Диаграмма рассеяния исходного и маскированного изображений
Fig. 7. Correlation diagram of the original and masked images

ванного и дважды маскированного изображения фотографии перца (рис. 3, з).

Из рис. 6, а видно, что передаваемое (исходное) изображение имеет сильно выраженные значения яркости, что может представлять полезную информацию для несанкционированного пользователя при приеме сигнала, на рис. 6, б видно, что передаваемая информация имеет менее выраженные значения яркости при использовании одноконтурной схемы, из рис. 6, в видно, что передаваемая информация не имеет выраженных значений яркости при использовании двухконтурной схемы, поэтому несанкционированное восстановление информации будет затруднено.

На рис. 7 отражены зависимости коэффициента корреляции исходного и маскированного изображений.

На рис. 7 приведены диаграммы рассеяния исходного и маскированного изображений. Из приведенных распределений видно, что на рис. 6, а можно выделить корреляцию между соседними строками изображения, которая пропадает при перемешивании информации (рис. 6, б). Аналогичные зависимости были получены при сопоставлении столбцов и диагональных линий изображения.

Заключение

В работе проведен анализ возможности комплексного повышения эффективности функционирования радиотехнических устройств и систем передачи информации с OFDM на основе использования нелинейных систем с динамическим хаосом, реализованных над конечным полем Галуа $GF(2^P)$. Основным результатом применения предлагаемых методов является комплексное повышение информационной безопасности и энергетической эффективности устройств и систем передачи информации на основе OFDM.

В работе выполнены оценки зависимостей вероятности битовой ошибки, пик-фактора, кумулятивной функции распределения, энтропии маскированного изображения, степени скремблирования информации и коэффициента корреляции исходного и скремблированного изображений. При одноконтурном методе маскирования степень скремблирования изображения составляет не менее 90 % для QAM-256 и не менее 70 % при QAM-16, в случае двухконтурного метода (скремблирования сигнала и маскирования изображения) – не менее 99 % для QAM-256 и 97 % для QAM-16. Энтропия маскированного монохромного изображения приближается к энтропии случайного источника сообщений.

Список литературы

1. A chaotic images encryption algorithm with the key mixing proportion factor / E. Dong [et al.] // 2008 International Conference on Information Management, Innovation Management and Industrial Engineering. 2008. P. 169–174. DOI: <https://doi.org/10.1109/ICIII.2008.25>
2. Дмитриев А.С., Панас А.И. Динамический хаос: новые носители информации для систем связи. М.: Изд-во физ.-мат. лит., 2002. 252 с.
3. Lerner I.M., Il'in V.I. New precision algorithm to effective memory estimation for channel with memory // 2020 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). 2020. P. 1–7. DOI: <https://doi.org/10.1109/SYNCHROINFO49631.2020.9166112>
4. Логинов С.С., Зуев М.Ю. Статистические характеристики генераторов псевдослучайных сигналов на основе систем Лоренца, Чуа и Дмитриева-Кислова, реализованных над конечным полем Галуа // Инженерный вестник Дона. 2018. № 4. С. 1–13. URL: <http://ivdon.ru/ru/magazine/archive/n4y2018/5358>
5. Loginov S.S., Zuev M.Y., Testing of generators of pseudo-random signals based on a Lorenz system, realized over a Galois finite field // 2018 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). 2018. P. 1–4. DOI: <https://doi.org/10.1109/SYNCHROINFO.2018.8457039>
6. Loginov S.S., Zuev M.Y. Chaotic systems based pseudo-random signal generators realized over a Galois Finite Field // 2019 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). 2019. P. 1–4. DOI: <https://doi.org/10.1109/SYNCHROINFO.2019.8814039>
7. Loginov S.S., Zuev M.Y., Agacheva Y.G. A pseudorandom signal generator based on the Lorentz system subjected to quasi-resonant action // 2020 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). 2020. P. 1–4. DOI: <https://doi.org/10.1109/WECONF48837.2020.9131530>
8. Zuev M.Y., Loginov S.S. Practical implementation of a pseudo-random signal generator based on the Lorenz system realized on FPGA // 2019 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). 2019. P. 1–4. DOI: <https://doi.org/10.1109/SYNCHROINFO.2019.8814209>
9. Шинаков Ю.С. Пик-фактор сигналов OFDM и нелинейные искажения в радиоборудовании систем беспроводного доступа // Цифровая обработка сигналов. 2012. № 4. С. 58–65. URL: http://www.dsps.ru/articles/year2012/jour12_4/art12_4_11.pdf
10. Han S.H., Lee J.H. An overview of peak-to-average power ratio reduction techniques for multicarrier transmission // IEEE Wireless Communications. 2005. Vol. 12, no. 2. P. 56–65. DOI: <https://doi.org/10.1109/MWC.2005.1421929>
11. Wei Z., Zhang C., Chen C. Chaos based IQ encryption for PAPR reduction and security enhancement in OFDMA PON system // Procedia Engineering. 2016. Vol. 140. P. 30–35. DOI: <https://doi.org/10.1016/j.proeng.2015.09.234>
12. Султанов А.Х., Мешков И.К., Ишмиряев А.А. Метод повышения энергетической эффективности систем OFDM, основанный на уменьшении пик-фактора // Физика волновых процессов и радиотехнические системы. 2018. Т. 21, № 3. С. 25–31. URL: <https://journals.ssau.ru/pwp/article/view/7014>
13. Sharma C., Tomar S.K., Gupta A.K. PAPR reduction in OFDM system using adapting coding technique with pre distortion method // WSEAS Transactions on Communications. 2011. Vol. 10. P. 255–262.
14. Lerner I.M., Fayzullin R.R. The study of features of functioning of channel with memory and APSK-N-signal. The possibilities of increasing its spectral efficiency // 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). 2019. P. 1–7. doi: <https://doi.org/10.1109/WECONF.2019.8840586>
15. Гаранин М.В., Журавлев В.И., Кунегин С.В. Системы и сети передачи информации. М.: Радио и связь, 2001. 336 с.

References

1. Dong E. et al. A chaotic images encryption algorithm with the key mixing proportion factor. 2008 *International Conference on Information Management, Innovation Management and Industrial Engineering*, 2008, pp. 169–174. DOI: <https://doi.org/10.1109/ICIII.2008.25>
2. Dmitriev A.S., Panas A.I. *Dynamic Chaos: New Information Carriers for Communication Systems*. Moscow: Izd-vo fiz.-mat. lit., 2002, 252 p. (In Russ.)
3. Lerner I.M., Il'in V.I. New precision algorithm to effective memory estimation for channel with memory. 2020 *Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*, 2020, pp. 1–7. DOI: <https://doi.org/10.1109/SYNCHROINFO49631.2020.9166112>
4. Loginov S.S., Zuev M.Yu. Statistical characteristics of pseudo-random signal generators based on Lorentz, Chua and Dmitriev-Kislov systems implemented over a finite Galois field. *Inzhenernyj vestnik Dona*, 2018, no. 4, pp. 1–13. URL: <http://ivdon.ru/ru/magazine/archive/n4y2018/5358> (In Russ.)
5. Loginov S.S., Zuev M.Y. Testing of generators of pseudo-random signals based on a Lorenz system, realized over a Galois finite field. 2018 *Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*, 2018, pp. 1–4. DOI: <https://doi.org/10.1109/SYNCHROINFO.2018.8457039>
6. Loginov S.S., Zuev M.Y. Chaotic systems based pseudo-random signal generators realized over a Galois Finite Field. 2019 *Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*, 2019, pp. 1–4. DOI: <https://doi.org/10.1109/SYNCHROINFO.2019.8814039>
7. Loginov S.S., Zuev M.Y., Agacheva Y.G. A pseudorandom signal generator based on the Lorentz system subjected to quasi-resonant action. 2020 *Wave Electronics and its Application in Information and Telecommunication Systems (WECONF)*, 2020, pp. 1–4. DOI: <https://doi.org/10.1109/WECONF48837.2020.9131530>

8. Zuev M.Y., Loginov S.S. Practical implementation of a pseudo-random signal generator based on the Lorenz system realized on FPGA. *2019 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*, 2019, pp. 1–4. DOI: <https://doi.org/10.1109/SYNCHROINFO.2019.8814209>
9. Shinakov Yu.S. Crest factor of OFDM signals and nonlinear distortions in radio equipment of wireless access systems. *Tsifrovaja obrabotka signalov*, 2012, no. 4, pp. 58–65. URL: http://www.dsps.ru/articles/year2012/jour12_4/art12_4_11.pdf (In Russ.)
10. Han S.H., Lee J.H. An overview of peak-to-average power ratio reduction techniques for multicarrier transmission. *IEEE Wireless Communications*, 2005, vol. 12, no. 2, pp. 56–65. DOI: <https://doi.org/10.1109/MWC.2005.1421929>
11. Wei Z., Zhang C., Chen C. Chaos based IQ encryption for PAPR reduction and security enhancement in OFDMA PON system. *Procedia Engineering*, 2016, vol. 140, pp. 30–35. DOI: <https://doi.org/10.1016/j.proeng.2015.09.234>
12. Sultanov A.H., Meshkov I.K., Ishmiyarov A.A. OFDM system energy efficiency increasing method based on peak-factor decrease. *Physics of Wave Processes and Radio Systems*, 2018, vol. 21, no. 3, pp. 25–31. URL: <https://journals.ssau.ru/pwp/article/view/7014> (In Russ.)
13. Sharma C., Tomar S.K., Gupta A.K. PAPR reduction in OFDM system using adapting coding technique with pre distortion method. *WSEAS Transactions on Communications*, 2011, vol. 10, pp. 255–262.
14. Lerner I.M., Fayzullin R.R. The study of features of functioning of channel with memory and APSK-N-signal. The possibilities of increasing its spectral efficiency. *2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF)*, 2019, pp. 1–7. DOI: <https://doi.org/10.1109/WECONF.2019.8840586>
15. Garanin M.V., Zhuravlev V.I., Kunegin S.V. *Information Transmission Systems and Networks*. Moscow: Radio i svjaz', 2001, 336 p. (In Russ.)

Physics of Wave Processes and Radio Systems

2022, vol. 25, no. 1, pp. 55–64

DOI 10.18469/1810-3189.2022.25.1.55-64

Received 1 November 2021
Accepted 3 December 2021

Complex improvement of the efficiency of radio electronic devices and information transmission systems with OFDM based on nonlinear systems with dynamic chaos

Maxim Yu. Zuev 

Kazan National Research Technical University named after A.N. Tupolev – KAI
10, Karl Marx Street,
Kazan, 420111, Russia

Abstract – This article presents the results of modeling a communication system with OFDM using the methods of scrambling the transmitted signals and masking the transmitted information. The paper considers a method of scrambling the transmitted information with pseudo-random sequences obtained by a generator built on the basis of modified dynamic systems. Estimates of the probability of a bit error of the communication system under consideration are obtained, the peak-factor of signals, the correlation characteristics of the scrambled and initial information are estimated, and the entropy of the transmitted information. The results of the article can be used in the design of modern communication systems in order to increase the security of transmitted information and reduce the peak to average power ratio of the generated signals.

Keywords – pseudo-random sequence; OFDM; signal scrambling; information masking; information security; peak to average power ratio.

Информация об авторе

Зуев Максим Юрьевич, инженер, окончил аспирантуру кафедры электронных и квантовых средств передачи информации Казанского национального исследовательского технического университета им. А.Н. Туполева – КАИ (КНИТУ-КАИ), г. Казань, Россия.

Область научных интересов: динамический хаос, радиоэлектронные динамические системы, системы связи с ортогональным мультиплексированием, широкополосные системы связи.

E-mail: maxzv93@mail.ru

ORCID: <https://orcid.org/0000-0002-1570-4751>

Information about the Author

Maxim Yu. Zuev, engineer, post-graduate student of the Department of Electronic and Quantum Means of Information Transmission, Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan, Russia

Research interests: dynamic chaos, radioelectronic dynamic systems, communication systems with orthogonal multiplexing, wideband communication systems.

E-mail: maxzv93@mail.ru

ORCID: <https://orcid.org/0000-0002-1570-4751>