

Научная статья

УДК 004.056.53

DOI:10.31854/1813-324X-2023-9-3-6-13



## Оценка качества матричного маскирования цифровых звуковых данных

Евгений Константинович Григорьев, ev.grig95@gmail.com

Александр Михайлович Сергеев, aleks.asklab@gmail.com

Санкт-Петербургский государственный университет аэрокосмического приборостроения,  
Санкт-Петербург, 190000, Российская Федерация

**Аннотация:** Рассмотрена задача обеспечения конфиденциальности звуковой информации, передаваемой по каналу связи с пакетной передачей. Анализ предметной области показал, что для обеспечения конфиденциальности переговоров используются, в основном, криптографические методы. Однако, наряду с ними, начинают применяться матричные методы защитного кодирования, с реализацией на программируемых логических интегральных схемах или процессорах цифровой обработки сигналов. Данные методы, используя случайные матрицы, накладывают дополнительные инструментальные ошибки при декодировании. Целью исследования является оценка качества защитного кодирования – маскирования звуковых данных квазиортогональными структурированными матрицами. Предложенный в работе метод маскирования цифровой звуковой информации квазиортогональными матрицами отличается от известных предсказуемыми результатами и простотой реализацией. Предложен подход оценки результата маскирования, альтернативный классическому использованию метрик. Он основан на анализе спектральной составляющей сигнала. Показано, что маскирование квадратной матрицей Мерсенна – Уолша приводит цифровую звуковую информацию, представленную в виде матрицы, к виду, близкому по спектру к белому шуму. Это надежно защищает ее в коммуникационном канале от несанкционированного доступа. Полученные результаты показывают перспективность применения предлагаемого метода и предполагают исследование влияния выбора структур ортогональных матриц и их размеров на результаты маскирования.

**Ключевые слова:** матричное маскирование, цифровая звуковая информация, качество маскирования, белый шум, шумоподобный сигнал

**Финансирование:** Исследование выполнено при финансовой поддержке Министерства науки и высшего образования Российской Федерации, соглашение № FSRF-2023-0003, «Фундаментальные основы построения помехозащищенных систем космической и спутниковой связи, относительной навигации, технического зрения и аэрокосмического мониторинга».

**Ссылка для цитирования:** Григорьев Е.К., Сергеев А.М. Оценка качества матричного маскирования цифровых звуковых данных // Труды учебных заведений связи. 2023. Т. 9. № 3. С. 6–13. DOI:10.31854/1813-324X-2023-9-3-6-13

## Quality Analysis of Matrix Masking of Digital Audio Data

Evgeny Grigoriev, ev.grig95@gmail.com

Aleksandr Sergeev, aleks.asklab@gmail.com

Saint-Petersburg State University of Aerospace Instrumentation,  
St. Petersburg, 190000, Russian Federation

**Abstract:** This article considered the guarantee of confidentiality task of audio information transmitted over a packet communication channel. Domain analysis showed, that in most cases cryptographical method used for guarantee of confidentiality of audio information, however, along with them, matrix methods of protective coding used, with implementation on FPGA or DSP processors. These methods, using random matrices, impose additional instrumental errors during decoding. The purpose of the study: is to assess the quality of protective coding – masking of audio data by quasi-orthogonal structured matrices. The proposed method of masking digital audio information by quasi-orthogonal matrices differs from the known ones in predictable results and simplicity of implementation. An alternative approach to the classical use of metrics is proposed for evaluating the result of masking. It is based on the analysis of the spectral component of the signal. It is shown that masking with a square Mersenne – Walsh matrix brings digital audio information, presented in the form of a matrix, to a form close in spectrum to white noise. This reliably protects it in the communication channel from unauthorized access. The obtained results showed that the proposed method is promising and suggests the study of the influence of the choice of orthogonal matrix structures and their sizes on the results of masking.

**Keywords:** matrix masking, digital sound information, masking quality, white noise, noise-like signal

**Funding:** The paper was prepared with the financial support of the Ministry of Science and Higher Education of the Russian Federation, grant agreement No. FSRF-2023-0003, “Fundamental principles of building of noise-immune systems for space and satellite communications, relative navigation, technical vision and aerospace monitoring”.

**For citation:** Grigoriev E., Sergeev A. Quality Analysis of Matrix Masking of Digital Audio Data. *Proc. of Telecommun. Univ.* 2023;9(3):6–13. (in Russ.) DOI:10.31854/1813-324X-2023-9-3-6-13

## Введение

Сегодня человеческая речь и, в частности телефонные переговоры, остается одним из основных каналов информационного взаимодействия между людьми. Развитие и введение в эксплуатацию новых цифровых систем связи направлено на совершенствование именно этого способа коммуникации людей. При этом приходится решать широкий круг задач, связанных со сжатием сигналов, преобразованием форматов, выбором протоколов, хранением и обеспечением конфиденциальности переговоров.

В качестве стержневой в настоящей статье рассмотрим задачу обеспечения конфиденциальности информации, передаваемой по каналу связи. Известны решения, основанные на аналоговом и цифровом скремблировании, при которых изменяется звуковой сигнал с целью сокрытия информационной составляющей речевого сообщения [1]. Однако анализ большинства современных источников показывает, что для обеспечения конфиденциальности переговоров используются, в основном, криптографические методы [2–7]. И наряду с ними прослеживается тема использования матричных [8, 9] или гибридных [10–12] методов защитного кодирования, с реализацией на программируемых логических интегральных схемах [13] или процессорах цифровой обработки сигналов.

Целью данной работы является оценка качества защитного кодирования – маскирования звуковых данных квазиортогональной структурированной матрицей на основе проведенных компьютерных экспериментов.

## Матрицы в защитном кодировании цифровых звуковых данных

В работе [8] используются методы Compressed Sensing [14] и Тёплицевы матрицы, формируемые на основе сдвиговых регистров в качестве матрицы измерений. Это удобно, поскольку на приемную сторону необходимо передать лишь  $(m + n - 1)$  элементов матрицы, где  $m$  – количество строк,  $n$  – количество столбцов. Однако итоговые результаты работы подобных методов зависят не только от используемой матрицы измерений, но и от выбора алгоритма оптимизации, а также разреживающей матрицы.

В работе [9] предлагается деление входного звукового файла на части и формирование из них квадратной матрицы размером  $n \times n$ . Полученная таким образом матрица умножается на секретный ключ – матрицу, формируемую из вещественных случайных чисел. Результат – преобразованное сообщение отправляется по каналу связи на приемную сторону, где обратное преобразование осуществляется умножением сообщения на матрицу, обратную матрице-ключу. Однако авторы не поясняют, каким образом матрица-ключ передается на приемную сторону, а также как при этом решаются потенциальные проблемы вычисления обратной матрицы, связанные, например, с плохой обусловленностью или погрешностями округления.

В работах [10–12] используются хаотические матрицы, при работе с которыми возникают проблемы интерпретации полученных результатов, а также сильная зависимость от начальных условий.

В работах [15–18] рассматривается применение матричных преобразований для маскирования –

преобразования для защиты изображений или кадров видеопоследовательностей от несанкционированного ознакомления. Результат матричного двустороннего умножения изображений на квазиортогональные матрицы интерпретируется как «шумоподобный» [15].

### Алгоритм матричного маскирования цифровых звуковых данных

Как известно, если длина ключа системы шифрования совпадает с длиной сообщения, методов восстановления шифрованного сообщения не существует. Наше предложение по защите звуковых цифровых данных основано на подходе, реализующем данное утверждение. Однако отличие реализации от известных способов с применением матриц [8–12] состоит в том, что:

- исходное сообщение формируется в виде матрицы размера  $n \times n$ , путем распределения блоков цифровых звуковых данных последовательно по строкам, но  $n$  – не является произвольным, а кратно объему данных, передаваемых, например, в пакетах при передаче по IP-сетям;

- преобразование осуществляется только путем математического умножения матрицы сообщения на матрицу-ключ справа и результат представляет собой матрицу того же размера  $n \times n$ ;

- матрица-ключ является структурированной ортогональной и процесс маскирования/демаскирования «почти» симметричен – восстановление выполняется умножением на транспонированную матрицу слева;

- возможно использование матрицы-ключа как размера  $n \times n$ , так любого меньшего размера, кратно  $n$ , что расширяет выбор и повышает гибкость реализации.

Извлечение полезной информации из элементов матрицы после преобразования невозможно. Их значения определяются не только матрицей-ключом, но и цифровыми отсчетами звукового сигнала в строке, поскольку каждый элемент представляет собой сумму парных произведений элементов строки сообщения и столбца матрицы-ключа [17].

Преобразование на передающей стороне осуществляется умножением матрицы исходного сообщения  $X_n$  размера  $n \times n$  на матрицу-ключ  $M_n$  того же размера в виде:

$$Y_n = X_n M_n, \quad (1)$$

где  $Y_n$  – передаваемый в канале защищенный аудиосигнал в цифровом виде.

Обратное преобразование на приемной стороне осуществляется по выражению:

$$X_n = M_n^{-1} Y_n. \quad (2)$$

Использование для маскирования ортогональных матриц  $M_n$ , для которых  $M_n^{-1} = M_n^T$ , упрощает обратное преобразование по (2). В качестве матрицы-ключа могут быть использованы матрицы Адамара, порядки которых кратны  $4t$ , где  $t$  – натуральное число, а также матрицы Мерсенна, существующие на порядках  $(4t - 1)$ . Как те, так и другие существуют в структурированных видах, в том числе по Уолшу [19].

Преобразования (1 и 2), составляющие полный их цикл вне коммуникационного канала, при использовании матриц Мерсенна могут вносить только инструментальную погрешность умножения целочисленных значений на вещественные коэффициенты матриц  $M_n$  и  $M_n^T$ , сводимую в современных вычислителях к нулю. Поэтому восстановленный на приемной стороне звуковой сигнал соответствует исходному. Использование матриц Адамара, элементы которых имеют значения 1 и –1, таких погрешностей в преобразования не вносит.

### Эксперименты по маскированию цифровых звуковых данных

Эксперименты по маскированию несжатых аудиофайлов формата .wav, взятыми из датасета «UrbanSound8K» [20], проводились с использованием матриц Мерсенна – Уолша. Частота дискретизации аудиофайлов составляет 48 КГц. Файлы, в которых количество отсчетов превышает количество элементов матрицы-ключа, были обрезаны для выравнивания их длин.

Файлы, с которыми проводились эксперименты, приведены в таблице 1.

ТАБЛИЦА 1. Описание входных данных

TABLE 1. Input Data Description

Файл из датасета [16]	Краткое описание содержимого
108362-2-0-23.wav	Разговор двух собеседников
7383-3-0-0.wav	Лай собаки
24074-1-0-2.wav	Звуковой сигнал автомобиля
26270-9-0-35.wav	Концерт на городской площади
40722-8-0-8.wav	Речь на фоне сирены
46669-4-0-37.wav	Высокочастотный писк
57320-0-0-0.wav	Пение птиц
59277-0-0-5.wav	Низкочастотный гул
196087-2-0-0.wav	Детский смех

Компьютерный эксперимент с оценкой параметров преобразований проводился по приведенному ниже алгоритму. В качестве матрицы-ключа использовалась квадратная двухуровневая матрица Мерсенна – Уолша размера  $511 \times 511$  со значениями элементов, равных 1 и –1, где  $b = 0,9188$ . Портрет указанной матрицы приведен на рисунке 1.

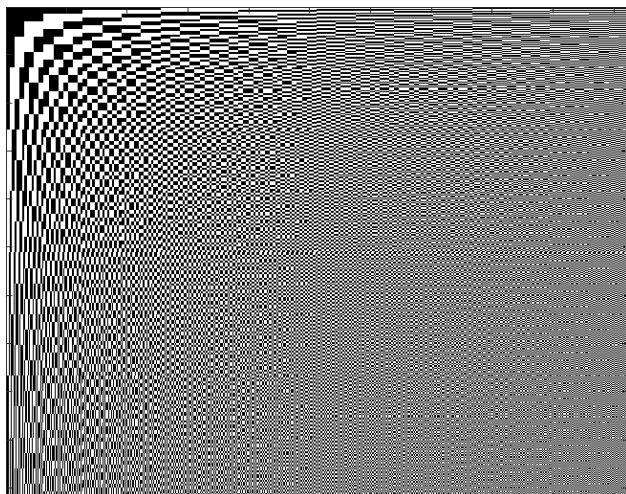


Рис. 1. Портрет матрицы-ключа

Fig. 1. Portrait of Key Matrix

1) На вход программы преобразования подавался звуковой сигнал из файлов (см. таблицу 1).

2) Вычислялся амплитудный спектр.

3) В случае необходимости количество отсчетов аудиофайла подгонялось под размер матрицы-ключа.

4) Входной звуковой файл преобразовывался в матрицу с распределением блоков данных последовательно по строкам – матрица звукового сигнала формировалась размером  $511 \times 511$ .

5) Матрица с содержимым звукового файла умножалась на матрицу-ключ по формуле (1) с формированием маскированного звукового файла.

6) Для маскированного звукового файла вычислялись метрики: среднеквадратическая ошибка MSE (аббр. от англ. Mean Squared Error) и отношение сигнал-шум (SNR, аббр. от англ. Signal-to-Noise Ratio).

7) Вычислялась амплитудно-частотная характеристика (АЧХ) маскированного звукового сигнала.

8) С маскированным звуковым файлом производилось обратное преобразование по формуле (2) с формированием демаскированного звукового сигнала.

9) Для демаскированного звукового сигнала вычислялись метрики MSE, SNR, а также АЧХ.

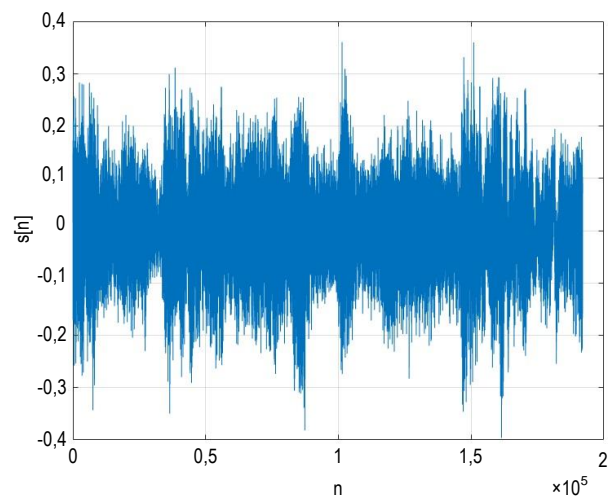
Эксперименты проводились с использованием специального программного обеспечения, реализованного на языке MATLAB [21, 22].

В качестве примера рассмотрим результаты маскирования и демаскирования звукового файла 108362-2-0-23.wav. На рисунке 2 приведены графики отсчетов исходного входного звукового сигнала, маскированного по формуле (1) и демаскированного по формуле (2).

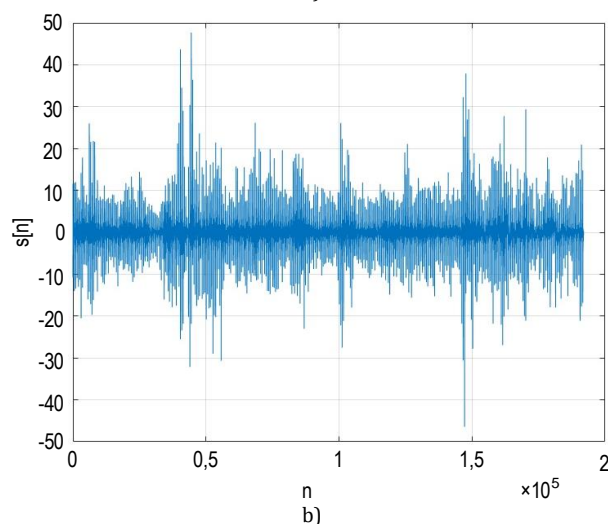
Из рисунка 2 видно следующее:

– во-первых, график исходного и демаскированного сигналов совпадают, подтверждая симметричность преобразования;

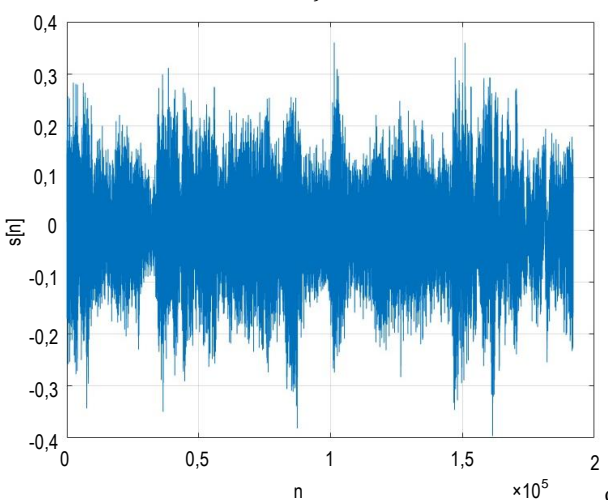
– во-вторых, маскирующее преобразование усиливает амплитуду входного сигнала.



a)



b)



c)

Рис. 2. Графики отсчетов входного (a), маскированного (b) и демаскированного (c) сигналов

Fig. 2. Samples of Input (a), Masked (b) and Demasked (c) Signals



В таблице 2 приведены классические метрики звуковых сигналов: MSE и SNR. Отрицательные значения SNR для маскированных сигналов говорят о том, что их амплитуда значительно выше амплитуды исходных сигналов. Для демаскированных сигналов метрики MSE и SNR близки к машинному нулю.

ТАБЛИЦА 2. Объективные метрики качества

TABLE 2. Objective Quality Metrics

Файл из датасета [16]	Сигнал			
	Маскированный		Демаскированный	
	MSE	SNR, дБ	MSE	SNR, дБ
108362-2-0-23.wav	2,0100	-26,7326	1,2415e-29	9,6433e-16
7383-3-0-0.wav	2,2712		1,1413e-29	9,6433e-15
24074-1-0-2.wav	6,3564		2,9602e-29	-1,4465e-15
26270-9-0-35.wav	23,6375		2,2560e-28	9,6433e-16
40722-8-0-8.wav	4,7825		3,0260e-29	3,8573e-15
46669-4-0-37.wav	1,1140		2,7322e-30	-3,3751e-15
57320-0-0-0.wav	0,8823		5,4861e-30	-2,8930e-15
59277-0-0-5.wav	13,4536		1,2646e-28	9,6433e-16
196087-2-0-0.wav	1,2740		6,4893e-30	-8,1968e-15

Однако, классические метрики MSE и SNR не определяют качество маскирования входного сигнала, поскольку на слух из файлов с самым низким и самым высоким значениями MSE (57320-0-0-0.wav и 26270-9-0-35.wav, соответственно) невозможно определить звук исходного сигнала.

Анализ предметной области показывает, что метрик вычисления качества искажения (маскирования) звука не существует. Поэтому в рамках данной работы нами предложен альтернативный подход к определению качества маскирования звукового сигнала. Он основывается на оценке близости АЧХ звукового сигнала к АЧХ белого шума. Поскольку субъективно из белого шума невозможно что-либо услышать, а объективно – затруднительно извлечь какую-либо информацию.

В качестве примера приведены АЧХ входного звукового сигнала из файла 108362-2-0-23.wav, а также маскированного и демаскированного сигналов (рисунок 3).

Анализ приведенных на рисунке 3 графиков показывает, что:

- АЧХ маскированного сигнала достаточно равномерно распределена на всем диапазоне частот;
- процедура маскирования подавила все спектральные компоненты входного сигнала, которые были сосредоточены в диапазоне до 5 КГц.

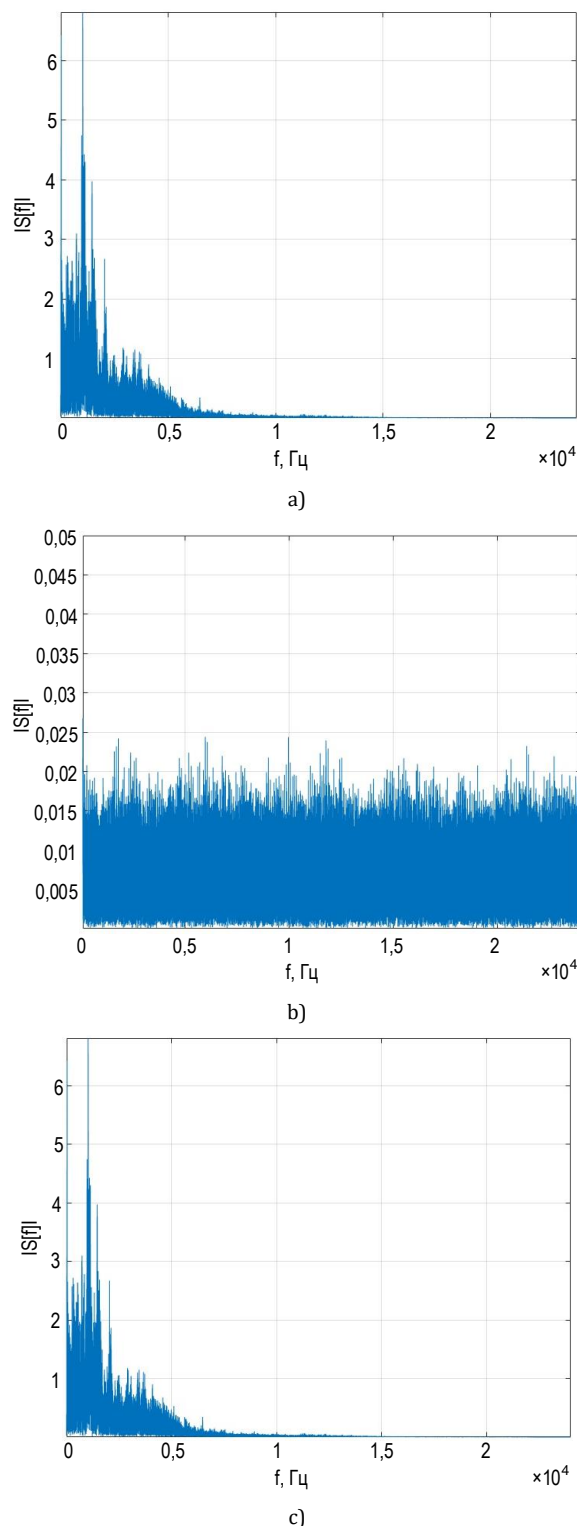


Рис. 3. Графики АЧХ входного (а), маскированного (б) и демаскированного (с) сигналов

Fig 3. Amplitude Spectrum of Input (a), Masked (b) and Demasked (c) Signals

На рисунке 4 для сравнения приведены АЧХ маскированного сигнала и белого гауссовского шума с нулевым математическим ожиданием и среднеквадратическим отклонением (СКО), равным СКО маскированного звукового сигнала.

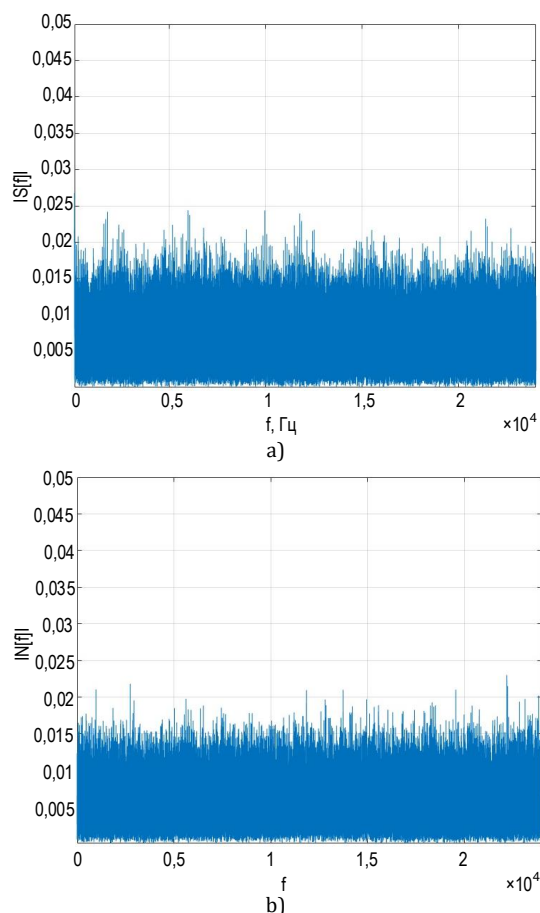


Рис. 4. Сравнение АЧХ маскированного сигнала (а) и белого гауссовского шума (б)

Fig. 4. Amplitude Spectrum of Masked Signal (a) and White Gaussian Noise (b) Compare

Спектр маскированного звукового сигнала близок к спектру белого гауссовского шума, СКО между ними составляет  $2,1379 \cdot 10^{-05}$ .

Эксперименты по матричному маскированию других звуковых файлов из таблицы 1 показали аналогичные результаты.

В случае маскирования звуковых файлов можно также воспользоваться вариантом двухстороннего матричного маскирования [15, 17], при котором на передающей стороне осуществляется умножение матрицы исходного сообщения  $\mathbf{X}_n$  размера  $n \times n$  на матрицу-ключ того же размера  $\mathbf{M}_n$  слева и транспонированную матрицу ключ  $\mathbf{M}_n^T$  справа:

$$\mathbf{Y}_n = \mathbf{X}_n \mathbf{M}_n \mathbf{M}_n^T, \quad (3)$$

Обратное преобразование на приемной стороне осуществляется по выражению:

$$\mathbf{X}_n = \mathbf{M}_n^{-1} \mathbf{Y}_n (\mathbf{M}_n^T)^{-1}. \quad (4)$$

В данном варианте осуществляется наиболее полное перемешивание фрагментов матрицы исходного сообщения, что соответствующим образом отображается на объективных метриках, которые для двухстороннего маскирования звуковых файлов приведены в таблице 3.

ТАБЛИЦА 3. Объективные метрики качества для двухстороннего маскирования звуковых файлов

TABLE 3. Objective Quality Metrics for Two Side Audiofiles Masking

Файл из датасета [16]	Сигнал			
	Маскированный		Демаскированный	
	MSE	SNR, дБ	MSE	SNR, дБ
108362-2-0-23.wav	949,1217	-53,4653	1,6724e-29	5,7860e-15
7383-3-0-0.wav	1,0678e+03		1,6213e-29	1,0608e-14
24074-1-0-2.wav	2,9936e+03		4,1723e-29	-3,3751e-15
26270-9-0-35.wav	1,1092e+04		2,9338e-28	-3,8573e-15
40722-8-0-8.wav	2,2713e+03		4,0415e-29	1,1572e-14
46669-4-0-37.wav	523,4474		5,2276e-30	-4,8216e-15
57320-0-0-0.wav	418,9160		7,4647e-30	-2,8930e-15
59277-0-0-5.wav	6,3379e+03		1,6126e-28	1,1572e-14
196087-2-0-0.wav	599,0425		9,0774e-30	-8,1968e-15

Однако в данном случае пропорционально увеличиваются и вычислительные затраты алгоритма, в связи с этим для ускорения вычислительных процессов целесообразно использовать матрицы порядков, равных матрице, сформированной из исходного сообщения. Это становится возможным благодаря расширению класса ортогональных матриц четных порядков, используемых для маскирования цифровой информации, квазиортогональными матрицами Мерсенна, Эйлера, Ферма и т. д. [15, 16].

## Заключение

Для защитного преобразования цифровой звуковой информации – маскирования – применение матричного умножения с использованием квазиортогональных матриц отличается от известных подходов с использованием случайных матриц предсказуемыми результатами и простотой реализации.

Маскирование квадратной матрицей Мерсенна – Уолша размера  $n$  приводит цифровую звуковую информацию к виду, близкому по спектру к белому шуму, что надежно защищает ее в коммуникационном канале от несанкционированного доступа. Размер матриц  $n$  следует для IP- и других систем с пакетной передачей данных выбирать кратным длине пакета.

Полученные результаты показывают перспективность применения предлагаемого метода и предполагают исследование влияния выбора структур ортогональных матриц и их размеров на результаты маскирования.

## Список источников

1. Владимиров С.С., Когновицкий О.С. Обработка широкополосных последовательностей Гордона – Миллса – Велча с использованием двойственного базиса на основе двух регистров // Труды учебных заведений связи. 2019. Т. 5. № 2. С. 49–58. DOI:10.31854/1813-324X-2019-5-2-49-58
2. Advanced encryption standard (AES) // FIPS 197. URL: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf> (дата обращения 22.03.2023)
3. Rahman Md. M., Saha T.K., Bhuiyan Md. A. Implementation of RSA Algorithm for Speech Data Encryption and Decryption // International Journal of Computer Science and Network Security. 2012. Vol. 12. Iss. 3. PP 74–82.
4. Gnanajeyaraman R., Prasad K. Audio encryption using higher dimensional chaotic map // International Journal of Recent Trends in Engineering. 2009. Vol. 1. Iss. 2. PP. 103–107.
5. Hassan N.A., Al-Mukhtar F.S., Ali E.H. Encrypt Audio File using Speech Audio File As a key // Proceedings of the 2nd International Scientific Conference of Al-Ayen University (ISCAU-2020, Thi-Qar, Iraq, 15–16 July 2020). IOP Conference Series: Materials Science and Engineering. 2020. Vol. 928 032066. PP. 79–84. DOI:10.1088/1757-899X/928/3/032066
6. Farsana F.J., Devi V.R., Gopakumar K. An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams // Applied Computing and Informatics. 2020. Vol. 16. Iss. 2. DOI:10.1016/j.aci.2019.10.001
7. Adhikari S., Karforma S. A novel audio encryption method using Henon–Tent chaotic pseudo random number sequence // International Journal of Information Technology. 2021. Vol. 13. PP. 1463–1471. DOI:10.1007/s41870-021-00714-x
8. Cai C., Bai E., Jiang X.Q., Wu Y. Simultaneous Audio Encryption and Compression Using Parallel Compressive Sensing and Modified Toeplitz Measurement Matrix // Electronics. 2021. Vol. 10. Iss. 23. P. 2902. DOI:10.3390/electronics10232902
9. Al-laham M.M. A Method for Encrypting and Decrypting wave Files // International Journal of Network Security & Its Applications. 2018. Vol. 10. Iss. 4. PP. 11–21.
10. Abdallah H.A., Meshoul S.A. Multilayered Audio Signal Encryption Approach for Secure Voice Communication // Electronics. 2023. Vol. 12. Iss. 1. P. 2. DOI:10.3390/electronics12010002
11. Hameed Y.M., Ali N.H.M. An efficient audio encryption based on chaotic logistic map with 3D matrix // Journal of Theoretical and Applied Information Technology. 2018. Vol. 96. Iss. 16. PP. 5142–5152.
12. Luis M., Daniel L., Isabel A., Deicy A. A new multimedia cryptosystem using chaos, quaternion theory and modular arithmetic // Multimedia Tools and Applications. 2023. DOI:10.1007/s11042-023-14475-1
13. Ge X., Sun G., Zheng B., Nan R. FPGA-Based Voice Encryption Equipment under the Analog Voice Communication Channel // Information. 2021. Vol. 12. Iss. 11. PP. 456. DOI:10.3390/info12110456
14. Donoho D.L. Compressed sensing // IEEE Transactions on Information Theory. 2006. Vol. 52. Iss. 4. PP. 1289–1306. DOI:10.1109/TIT.2006.871582
15. Востриков А.А., Сергеев М.Б., Литвинов М.Ю. Маскирование цифровой визуальной информации: термин и основные определения // Информационно-управляющие системы. 2015. №5(78). С. 116–123. DOI:10.15217/issn1684-8853.2015.5.116
16. Vostrikov A., Sergeev M. Expansion of the Quasi-Orthogonal Basis to Mask Images // Proceedings of the 8th International KES Conference on Intelligent Interactive Multimedia Systems and Services (KES-IIMSS-15, Sorrento, Italy, 17–19 June 2015). Smart Innovation, Systems and Technologies. Vol. 40. Cham: Springer, 2015. PP. 161–168. DOI:10.1007/978-3-319-19830-9\_15
17. Sergeev A. M., Grigoriev E. K. Quasi-orthogonal Structured Mersenne Matrices for Masking Digital Video and Audio Data in Distributed Systems // Proceedings of the International Conference on Information Processes and Systems Development and Quality Assurance (IPSQDA-2023). 2023. PP. 57–59.
18. Сергеев А.М. Связь симметрии и антисимметрии квазиортогональных циклических матриц с простыми числами // Труды учебных заведений связи. 2022. Т. 8. № 4. С. 14–19. DOI:10.31854/1813-324X-2022-8-4-14-19
19. Балонин Н.А., Балонин Ю.Н., Востриков А.А., Сергеев М.Б. Вычисление матриц Мерсенна – Уолша // Вестник компьютерных и информационных технологий. 2014. № 11. С. 51–55.
20. UrbanSound8K dataset. URL: <https://urbansounddataset.weebly.com/urbansound8k.html> (дата обращения 04.04.2023)
21. Григорьев Е.К., Сергеев М.Б., Сергеев А.М. Программа маскирования и демаскирования звуковой цифровой информации. Модуль маскирования. Свидетельство о регистрации программы для ЭВМ № RU 2023614623 от 03.03.2023. Оpubл. 03.03.2023.
22. Григорьев Е.К., Сергеев М.Б., Сергеев А.М. Программа маскирования и демаскирования звуковой цифровой информации. Модуль демаскирования. Свидетельство о регистрации программы для ЭВМ № RU 2023614622 от 03.03.2023. Оpubл. 03.03.2023.

## References

1. Vladimirov S., Kognovitsky O. Dual Basis Based Processing of Wideband Gordon – Mills – Welch Sequences Based on Two Linear Registers. *Proceed. of Telecom. Universities*. 2019;5(2):49–58. (in Russ.) DOI:10.31854/1813-324X-2019-5-2-49-58
2. FIPS 197. Advanced encryption standard (AES). URL: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf> [Accessed 22d March 2023]
3. Rahman M., Saha K., Bhuiyan A. Implementation of RSA Algorithm for Speech Data Encryption and Decryption. *International Journal of Computer Science and Network Security*. 2012;(12)3:74–82.
4. Gnanajeyaraman R., Prasad K. Audio encryption using higher dimensional chaotic map. *International Journal of Recent Trends in Engineering*. 2009;1(2):103–107.
5. Hassan N.A., Al-Mukhtar F.S., Ali E.H. Encrypt Audio File using Speech Audio File As a key. *Proceedings of the 2nd International Scientific Conference of Al-Ayen University, ISCAU-2020, 15–16 July 2020, Thi-Qar, Iraq. IOP Conference Series: Materials Science and Engineering*. 2020;928 032066:79–84. DOI:10.1088/1757-899X/928/3/032066


6. Farsana J., Devi R., Gopakumar K. An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams. *Applied Computing and Informatics*. 2020;16(2). DOI:10.1016/j.aci.2019.10.001
7. Adhikari S., Karforma S. A novel audio encryption method using Henon–Tent chaotic pseudo random number sequence. *International Journal of Information Technology*. 2021;13:1463–1471. DOI:10.1007/s41870-021-00714-x
8. Cai C., Bai E., Jiang X.Q., Wu Y. Simultaneous Audio Encryption and Compression Using Parallel Compressive Sensing and Modified Toeplitz Measurement Matrix. *Electronics*. 2021;10(23):2902. DOI:10.3390/electronics10232902
9. Al-laham M.M. A Method for Encrypting and Decrypting wave Files. *International Journal of Network Security & Its Applications*. 2018;10(4):11–21.
10. Abdallah H.A., Meshoul S.A. A Multilayered Audio Signal Encryption Approach for Secure Voice Communication. *Electronics*. 2023;12(1):2. DOI:10.3390/electronics12010002
11. Hameed Y.M., Ali N.H.M. An efficient audio encryption based on chaotic logistic map with 3D matrix. *Journal of Theoretical and Applied Information Technology*. 2018;96(16):5142–5152.
12. Luis M., Daniel L., Isabel A., Deicy A. A new multimedia cryptosystem using chaos, quaternion theory and modular arithmetic. *Multimedia Tools and Applications*. 2023. DOI:10.1007/s11042-023-14475-1
13. Ge X., Sun G., Zheng B., Nan R. FPGA-Based Voice Encryption Equipment under the Analog Voice Communication Channel. *Information*. 2021;12(11):456. DOI:10.3390/info12110456
14. Donoho D.L. Compressed sensing. *IEEE Transactions on Information Theory*. 2006;52(4):1289–1306. DOI:10.1109/TIT.2006.871582
15. Vostrikov A.A., Sergeev M.B., Litvinov M.Yu. Masking of Digital Visual Data: the Term and Basic Definitions. *Information and Control Systems*. 2015;5(78):116–123. (in Russ.) DOI:10.15217/issn1684-8853.2015.5.116.
16. Vostrikov A., Sergeev M. Expansion of the Quasi-Orthogonal Basis to Mask Images. *Proceedings of the 8th International KES Conference on Intelligent Interactive Multimedia Systems and Services, KES-IIMSS-15, 17–19 June 2015, Sorrento, Italy. Smart Innovation, Systems and Technologies, vol.40*. Cham: Springer; 2015. p.161–168. DOI:10.1007/978-3-319-19830-9\_15
17. Sergeev A. M., Grigoriev E. K. Quasi-orthogonal Structured Mersenne Matrices for Masking Digital Video and Audio Data in Distributed Systems. *Proceedings of the International Conference on Information Processes and Systems Development and Quality Assurance, IPSQDA-2023*. 2023. p.57–59.
18. Sergeev A. Interrelation of Symmetry and Antisymmetry of Quasi-Orthogonal Cyclic Matrices with Prime Numbers. *Proc. of Telecom. Universities*. 2022;8(4):14–19. (in Russ.) DOI:10.31854/1813-324X-2022-8-4-14-19
19. Balonin A., Balonin U., Vostrikov A., Sergeev M. Computation of Mersenne – Walsh Matrices. *Herald of computer and information technologies*. 2014;11:51–55. (in Russ.)
20. UrbanSound8K dataset. URL: <https://urbansounddataset.weebly.com/urbansound8k.html> [Accessed 04th April 2023]
21. Grigoriev E.K., Sergeev M.B., Sergeev A.M. *The program for masking and demasking sound digital information. Masking module*. Patent RF, no. 2023614623, 03.03.2023. (in Russ.)
22. Grigoriev E.K. Sergeev M.B. Sergeev A.M. *The program for masking and demasking sound digital information. Demasking module*. Patent RF, no. 2023614622, 03.03.2023. (in Russ.)

Статья поступила в редакцию 10.04.2023; одобрена после рецензирования 24.04.2023; принята к публикации 20.05.2023.


The article was submitted 10.04.2023; approved after reviewing 24.04.2023; accepted for publication 20.05.2023.

## Информация об авторах:

**ГРИГОРЬЕВ**  
**Евгений Константинович**

ассистент кафедры вычислительных систем и сетей Санкт-Петербургского государственного университета аэрокосмического приборостроения  
 <https://orcid.org/0000-0001-5981-4074>

**СЕРГЕЕВ**  
**Александр Михайлович**

кандидат технических наук, доцент кафедры вычислительных систем и сетей Санкт-Петербургского государственного университета аэрокосмического приборостроения  
 <https://orcid.org/0000-0002-4788-9869>