

Матрицы Адамара в космической связи

С. Т. Хвоц

АО «Электронная компания «Элкус»

Аннотация: Рассматриваются исторические аспекты возникновения задачи помехоустойчивого кодирования изображений на примере доставки фотографий поверхности Марса на Землю. На примере обобщения ортогональных матриц квазиортогональными показывается расширение представительства матриц для использования в преобразовании изображений для передачи в каналах связи с помехами.

Ключевые слова: матрицы Адамара, адамарово кодирование, коды Рида-Соломона, ортогональные матрицы, квазиортогональные матрицы, помехоустойчивое кодирование изображений.

Введение

Матрицы Адамара \mathbf{H} [1 – 3] порядка n с элементами 1 и -1 ортогональны в смысле $\mathbf{H}^T \mathbf{H} = n\mathbf{I}$, где \mathbf{I} – единичная матрица. В этом качестве они использовались в технологии обеспечения космической связи, как минимум, дважды. Эти два различных использования иногда путают, считая, что адамаровы матрицы идут на смену кодов Рида-Соломона, хотя последние порождены, как раз, использованием этих весьма примечательных матриц, чем и вызвана необходимость пояснения.

В статье 1960 г. Ирвин Рид и Густав Соломон [4] писали «...когда мы публиковали статью, теория кодирования не являлась предметом обсуждения». Очевидно, что авторы, занимаясь редким для тех лет математическим программированием, не представляли себе влияния, которое окажет их статья на исследования космоса в четыре последующих десятилетия.

Цель настоящей работы – показать применение матриц для помехозащищенного кодирования изображений при передаче по телекоммуникационным каналам.

История вопроса

Напомним, что первый подвижный робот на Марс доставил СССР 2 декабря 1971 года. Это был советский аппарат со станции «Марс-3», разработанной и изготовленной НПО им. С. А. Лавочкина. Ее изображение представлено на рис. 1.

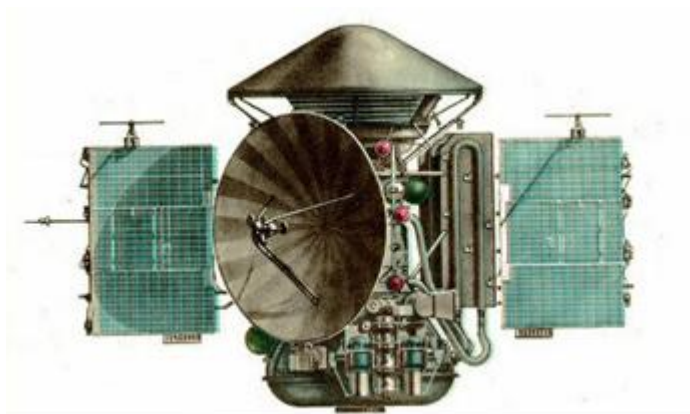


Рис. 1. Автоматическая межпланетная станция «Марс-3»
(изображение из источника [5])

Сейчас имеются подробные карты поверхности Марса, одна из которых представлена на рис. 2. Но более 50 лет назад советский аппарат совершил по тем временам феноменальную, первую в истории успешную посадку на Марс! Система доставки сработала четко и аппарат доставил в район кратеров небольшой самоходный прибор ПРОП-М. Его система «зрения» состояла из двух датчиков препятствий, расположенных на длинных стержнях, а за ним со стороны наблюдала видеокамера спускаемого модуля, кадр передачи от которой представлен на рис. 3.

Очевидно, качество связи (см. рис.3), достаточное для передачи изображений с Луны, для космической связи с поверхности Марса при наличии большого количества помех в канале передачи оказалось непригодным [6].

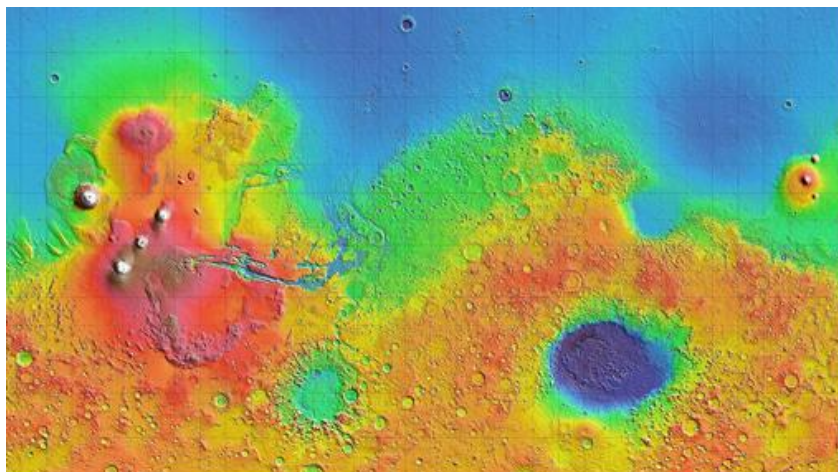


Рис. 2. Карта поверхности Марса (изображение из источника [5])

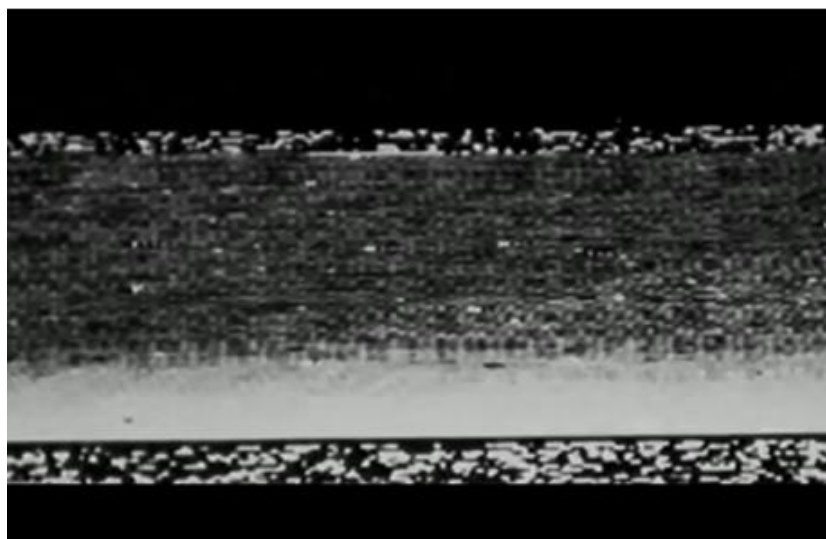


Рис. 3. Кадр, полученный с видеокамеры спускаемого модуля
(изображение из источника [7])

Прибывший к Марсу позже аппарат американской миссии «Маринер 9» (см. рис. 4) такой задачи, как посадка, не имел, но его камерой была сформирована и передана первая фотография с поверхности Марса, фрагмент которой приведен на рис. 5.

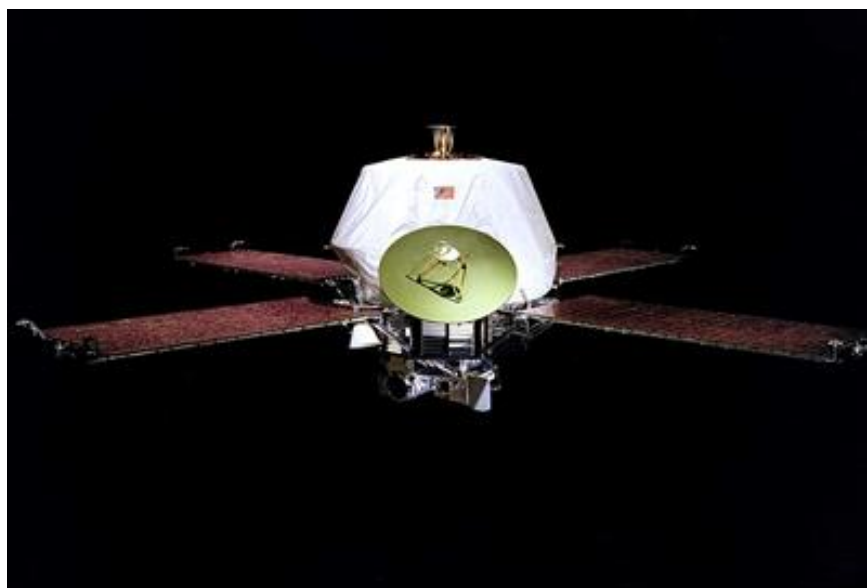


Рис. 4. Аппарат миссии Маринер 9 (изображение из источника [8])

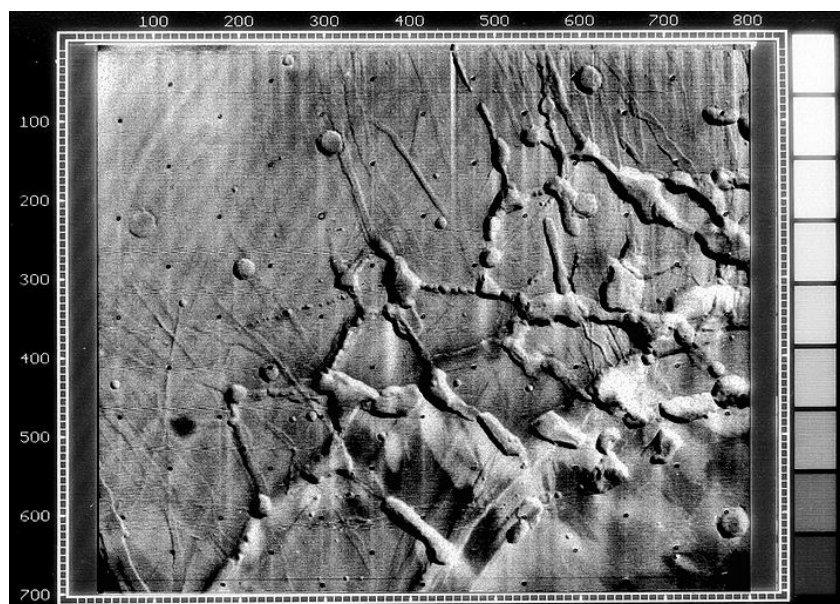


Рис. 5. Первое изображение Марса с орбиты (взято из источника [9])

Для этого телевизионный сигнал переводился в дискретный вид и кодировался матрицами Адамара.

Применение в кодировании матриц Адамара

Пример матрицы Адамара порядка 32, полученной известным итерационным по сути методом Сильвестра, приведен на рис. 6.

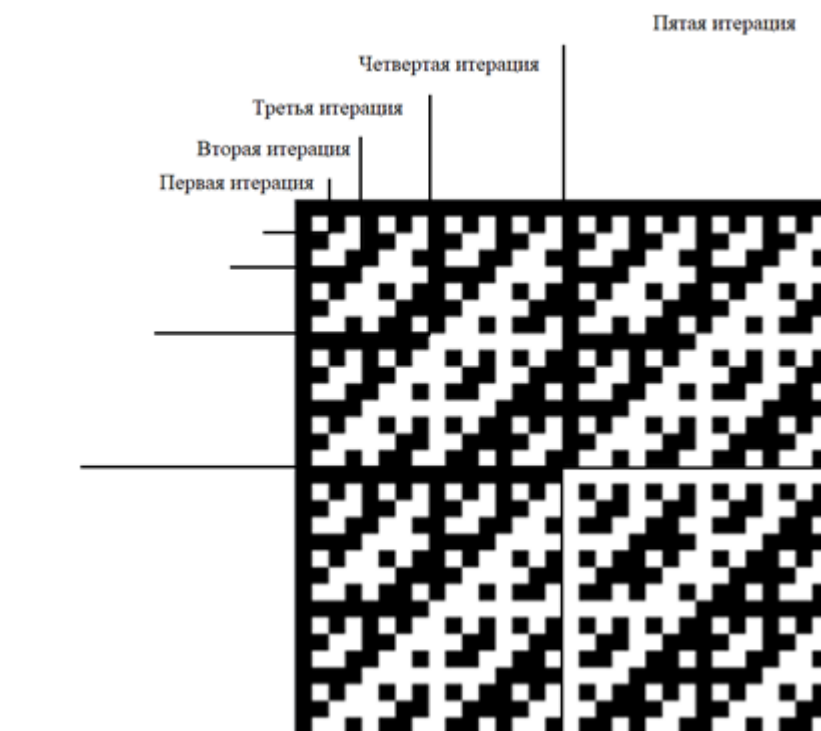


Рис. 6. Портрет матрицы Адамара порядка 32, конструируемой по методу Сильвестра

Причины применения матриц порядков, равных целым степеням 2 банальны – итерационный метод Сильвестра, который основан на дублировании начальных матриц в себя, начиная с 1 или с -1 , является одним из самых известных и простых методов их построения.

Первая итерация (см. рис. 6) – квадрат 2×2 , где клетка черно цвета соответствует элементу со значением 1, а белая клетка – элементу со значением -1 . На второй итерации квадрат 2×2 повторяется трижды и один раз (в правом нижнем углу) с инверсией знаков ее элементов. Затем то же самое производится с квадратом 4×4 и т.д. Таким образом возникает

фрактальная структура, где каждый следующий столбец отличается от всех предыдущих знаками половины его элементов. Это связано с важнейшим инвариантом ортогональных массивов, используемым при дихотомии.

Система связи, в которой вместо уровня яркости передается столбец чисел, гарантировала высокую степень его защиты от искажений в канале космической связи. Чтобы узнать номер принятого столбца значений, на приемной стороне, нужно всего лишь умножить его на транспонированную матрицу. В силу ортогональности ненужные столбцы имеют нулевые значения элементов.

При наличии помех, искажающих, например, один элемент сообщения, получается небольшое число на внедиагональном элементе произведения НТН. Произведение же на искомый столбец дает значение n .

Во времена передачи данных Маринером это был простой, практичный и надежный метод обеспечить многократное дублирование. А поскольку матрицы Адамара имеют разные структуры и часть из них получают в арифметике полей Галуа, то предложение Рида и Соломона смотрелось едва ли не повторением того, что уже имелось, но в несколько другой форме.

Многообразие порядков матриц для кодирования

Очевидно, что методом Сильвестра можно получить матрицы порядков $n = 2k$, где k – целое число. Однако гипотеза Адамара состоит в том, что предполагается существование таких матриц на порядках 1, 2 и далее на всех порядках, кратных четырем. Принимая на веру это утверждение, зададимся вопросом, а что делать при кодировании последовательностей, отличающихся длиной от порядков, указанных в гипотезе Адамара?

Анализ литературы показывает огромное количество многолетних исследований самого факта существования матриц Адамара [1, 10], их возможных структур [11, 12], нахождения зависимостей между их порядками

[13] и др.

Однако, начиная с 2011, наблюдается рост числа публикаций, посвященных тем же вопросам, но для квазиортогональных матриц, обобщающих матрицы Адамара [14].

Определение. Квазиортогональная матрица \mathbf{A} порядка n [10] – это квадратная матрица, удовлетворяющая уравнению $\mathbf{A}^T \mathbf{A} = \omega(n)\mathbf{I}$, где $\omega(n)$ – функция, определяющая тип матрицы.

Иными словами, квазиортогональная матрица – это матрица с вещественными элементами 1 и $-b$ в ней или образующих ее блоках. Инверсия знака при блоках не меняет состав базисных элементов. Профессор Дж. Себерри предложила называть матрицы критскими, подчеркивая нецелочисленность значений их элементов [1].

Результаты исследований показывают, что такие матрицы существуют на всех остальных порядках, что открывает возможности кодирования в канале сообщений любой длины.

Схожесть таких матриц и обобщение можно проследить на следующем примере. Для матриц Адамара порядков $n = 2k$ их ядром являются матрицы Мерсенна [14] порядков $4t - 1$, где t – натуральное число. В данную последовательность входят порядки, равные числам последовательности Мерсенна.

На рис.7 приведен портрет циклической матрицы Мерсенна порядка 7 ($23 - 1$), где каждый столбец, кроме первого, получен сдвигом предыдущего.

Если в данной матрице отрезать от столбцов верхушку, первые три строки (показатель при 2), то полученные коды столбцов будут отличаться на 1, не совпадая. Это свойство используется в генераторах вихрей Мерсенна [15] для формирования алфавита из букв, коды для которых дает все та же матрица Адамара.

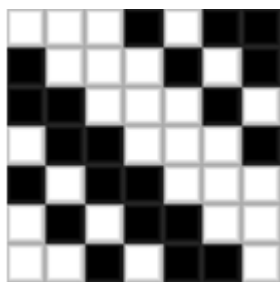


Рис. 7. Портрет матрицы Мерсенна порядка 7

Однако размер соответствующей матрицы растет стремительно, к тому же, нелегко заказать сколько-нибудь простое варьирование генератора кодов. Матрицы Адамара и подсказали выход из положения. Обычное введение в коды Рида-Соломона начинается объяснением того, как устроена арифметика полей, часто с излишними подробностями. Сама идея кодирования никак с этим не связана, она базируется на том, что элементы конечного поля Галуа соотносятся с векторами коэффициентов полиномов.

До дублирования размер этих векторов невелик, так как требуется передать ограниченное значение уровней яркости с матрицы видеокамеры. При кодировании необходимо лишь умножить эти полиномы малого порядка на некий полином, почти все равно какой, но увеличивающий их размер.

С ростом порядка, увеличивается число вариаций полиномов, используемых для ограничения порядка. Это как растягивание резинки с нанесенными на нее отметками – чем больше тянешь, тем более они расходятся. Возникает большая кодовая дистанция между ними, и теперь не всякая помеха в состоянии перевести одну точку в другую. В канале космической связи передаются увеличенные векторы. «Растягивать» мы можем разным образом.

И все-таки, как матрицы Адамара вернулись как незаменимый инструмент в технику передачи изображений? Эти матрицы, и сходные с

ними ортогональные и квазиортогональные матрицы родственны изображениям, которые тоже матрицы. Следовательно, их можно друг на друга умножать. При совпадении размеров прямо, а если размер изображения больше, то разбивая его на блоки. Результат произведения называется спектром. В самом деле, матрица синусов и косинусов Фурье, это тоже ортогональная матрица, и умножение на нее дает спектр.

Сегодня матрицы Адамара используются в помехоустойчивом кодировании изображений, передаваемых по открытым каналам связи с импульсными помехами. Метод, использующий матрицы Адамара и предложенный профессорами Мироновским Л. А. и Слаевым В. А. [16], получил название стрип-метод, поскольку его основа – «разрезание» всего изображения на полосы шириной, равной порядку используемых матриц.

Разумеется, кодами Рида-Соломона такое кодирование невозможно. Они заняты на нижнем уровне, передачей уровней яркости точек изображения, или двумерного спектра изображения. Верхний уровень помехоустойчивого кодирования и маскирования в космической связи обеспечивают матрицы семейства Адамара. Ведь не имея на руках матрицы, третья сторона не сможет увидеть то, что передается. Это называется маскирование [17], и чем шире семейство матриц, которое используется, тем сложнее третьей стороне понять содержимое изображения или кадров видеопотока.

Заключение

Ортогональные и обобщающие их квазиортогональные матрицы как математические объекты одновременно являются важными элементами в задачах помехоустойчивого кодирования. Они обладают рядом полезных свойств, делающих их применение эффективным: существуют на порядках, отвечающих числам натурального ряда; имеют различные симметрии,

способствующие их экономному хранению или оперативному вычислению; содержат ограниченное количество значений элементов, что облегчает вычисления с ними.

Применение квазиортогональных матриц в кодировании особенно востребовано при передаче информации по открытым каналам связи при наличии помех.

В целом, понимание теории квазиортогональных матриц и методов их использования является важным аспектом в области создания систем и средств защитного преобразования информации.

Литература

1. Jennifer S., Yamada M. Hadamard Matrices: Constructions using number theory and linear algebra. Wiley, 2020. 384 p.
2. Horadam K. J. Hadamard matrices and their applications. Princeton University Press, 2007. 263 p.
3. Colbourn C.J., Dinitz J. H. Handbook of Combinatorial Designs. Chapman and Hall/CRC, 2007. 967 p.
4. Reed I., Solomon G. Polynomial Codes over Certain Finite Fields // Journal of the Society for Industrial and Applied Mathematics. Vol. 8. № 2. pp. 300–304.
5. Схема Марс-3, URL: triptonkosti.ru/3-foto/shema-mars-3-83-foto.html (Дата обращения – 05.12.2023).
6. Лейтон Р. Поверхность Марса // Успехи физических наук. 1971. Т. 103. Вып. 4. С. 755-768.
7. Покорение Марса: первым был советский спускаемый аппарат, URL: ria.ru/20161202/1482684836.html (Дата обращения – 05.12.2023).

8. Mariner 9: Opening The Martian Frontier, URL: origins.osu.edu/milestones/november-2016-mariner-9-opening-martian-frontier?language_content_entity=en (Дата обращения – 07.12.2023).

9. Shalom E. La conjecture de Hadamard (I) – Images des Mathématiques, CNRS. 2012, URL: images.math.cnrs.fr/La-conjecture-de-Hadamard-I.html (accessed: 17.05.2022). (Дата обращения – 05.12.2023).

10. Балонин Н. А., Сергеев М. Б. Специальные матрицы: псевдообратные, ортогональные, адамаровы и критские. СПб.: Политехника, 2019. 196 с.

11. Хвощ С. Т. Матрицы Адамара как источник тестов квантовых компьютеров // Инженерный вестник Дона, 2023, №3. URL: ivdon.ru/ru/magazine/archive/n3y2023/8265 (Дата обращения – 05.12.2023).

12. Сергеев А. М. О классификации структурированных квазиортогональных матриц для преобразования изображений //Информация и космос. 2023. № 4. С. 63 – 69.

13. Балонин Н.А., Сергеев М.Б., Востриков А.А. О двух предикторах цепочек вычисляемых квазиотогональных матриц // Автоматика и вычислительная техника. 2015. № 3. С. 42 – 48.

14. Сергеев А. М. Обобщенные матрицы Мерсенна и гипотеза Балонины // Автоматика и вычислительная техника. 2014. № 4. С. 35–43

15. Matsumoto M., Nishimura T. Mersenne twister: A 623-dimensionally equidistributed uniform pseudorandom number generator // ACM Trans. on Modeling and Computer Simulations. 1998. Vol. 8. № 1. pp. 3 – 30.

16. Мироновский Л. А., Слаев В. А. Стрип-метод преобразования изображений и сигналов. СПб.: Политехника, 2006. 163 с.

17. 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.

References

1. Jennifer S., Yamada M. Hadamard Matrices: Constructions using number theory and linear algebra. Wiley, 2020. 384 p.
 2. Horadam K. J. Hadamard matrices and their applications. Princeton University Press, 2007. 263 p.
 3. Colbourn C.J., Dinitz J. H. Handbook of Combinatorial Designs. Chapman and Hall/CRC, 2007. 967 p.
 4. Reed I., Solomon G. Journal of the Society for Industrial and Applied Mathematics. Vol. 8. № 2. pp. 300 – 304.
 5. Skhema Mars-3 [The Mars-3 scheme], URL: triptonkosti.ru/3-foto/shema-mars-3-83-foto.html (accessed: 05.12.2023).
 6. Lejton R. Uspekhi fizicheskikh nauk. 1971. Vol. 103. № 4. pp. 755 – 768.
 7. Pokorenie Marsa: pervym byl sovetskij spuskaemyj apparat [The Conquest of Mars: the first was the Soviet lander], URL: ria.ru/20161202/1482684836.html (accessed: 05.12.2023).
 8. Mariner 9: Opening The Martian Frontier. URL: origins.osu.edu/milestones/november-2016-mariner-9-opening-martian-frontier?language_content_entity=en (accessed: 07.12.2023).
 9. Shalom E. La conjecture de Hadamard (I) – Images des Mathématiques, CNRS. 2012. URL: images.math.cnrs.fr/La-conjecture-de-Hadamard-I.html (accessed: 05.12.2023).
 10. Balonin N.A., Sergeev M.B. Special'nye matricy: psevdootbratnye, ortogonal'nye, adamarovy i kritskie [Special matrices: pseudo-inverse, orthogonal, Hadamard and Cretan]. St. Petersburg: Polytechnica, 2019. 196 p.
 11. Hvoshch S. T. Inženernyj vestnik Dona. 2023. №3. URL: ivdon.ru/ru/magazine/archive/n3y2023/8265 (accessed: 05.12.2023).
 12. Sergeev A. M. Informaciya i kosmos. 2023. № 4. pp. 63 – 69.
-



13. Balonin N. A., Sergeev M. B., Vostrikov A. A. Avtomatika i vychislitel'naya tekhnika. 2015. № 3. pp. 42 - 48.
14. Sergeev A. M. Avtomatika i vychislitel'naya tekhnika. 2014. № 4. pp. 35 – 43.
15. Matsumoto M., Nishimura T. ACM Trans. on Modeling and Computer Simulations. 1998. Vol. 8. № 1. pp. 3 – 30.
16. Mironovskij L. A., Slaev V. A. Strip-metod preobrazovaniya izobrazhenij i signalov [Strip-method for converting images and signals]. St. Petersburg: Polytechnica, 2006. 163 p.
17. Vostrikov A.A., Sergeev M.B., Litvinov M.Yu. Informacionno-upravlyayushchie sistemy. 2015. № 5. pp. 116 – 123.

Дата поступления: 16.12.2023

Дата публикации: 25.01.2024