УДК 004.042

А. А. Востриков, Ю. Н. Балонин

МАТРИЦЫ АДАМАРА — МЕРСЕННА КАК БАЗИС ОРТОГОНАЛЬНЫХ ПРЕОБРАЗОВАНИЙ ПРИ МАСКИРОВАНИИ ВИДЕОИЗОБРАЖЕНИЙ

Рассматривается процедура маскирования изображений с использованием М-матриц как ортогонального базиса. Предлагается на этапе спектрального разложения изображения использовать оригинальные двухуровневые ортогональные симметричные М-матрицы порядков, соответствующих последовательности Мерсенна, для которой не существует матриц Адамара.

Ключевые слова: *ортогональные матрицы, М-матрицы, матрицы Адамара, матрицы Адамара — Мерсенна, числа Мерсенна, обработка видеоизображений.*

Стремительное развитие технологий, связанных с передачей видеопотоков по сетям общего пользования, привело к необходимости создания надежной защиты видеоинформации от несанкционированного доступа и подмены. Разработано множество безупречных систем защиты, которые успешно и широко применяются на практике [1]. Однако большинство традиционных систем не могут напрямую использоваться для защиты цифровой видеоинформации в системах реального времени, поскольку базируются на алгоритмах шифрации и требуют значительных вычислительных затрат.

В работах [2—4] представлена альтернативная технология маскирования видеоизображений, при которой разрушение кадров видеопоследовательности до уровня шума обеспечивается на передающей стороне распределенной системы, а восстановление кадров — на приемной стороне. При использовании данной технологии актуальность маскируемой информации сохраняется в течение непродолжительного времени; эта технология предполагает также упрощение схемы преобразования на основе криптографических примитивов [4].

В монографии [5] вводится понятие стрип-оператора, позволяющего применить матричные методы кодирования видеоинформации на основе базисов ортогональных преобразований. В отличие от традиционных базисов, здесь основное значение имеют качества, определяемые экстремальными свойствами базисных наборов. Таковы, например, матрицы Адамара, оптимальные в смысле нейтрализации последствий воздействия точечных помех при передаче данных по каналам связи [6].

Кроме дискретности значений элементов матрицы Адамара, удобной при выполнении процедуры маскирования изображений с использованием цифровых устройств, не менее важную роль играет оригинальность базиса, обеспечивающая „скрытность“ получаемых преобразованных данных. Современное состояние процессоров цифровой обработки сигналов, характеризующееся увеличением производительности и структурной ориентацией на выполнение операции свертки в формате вещественных чисел, позволяет использовать более полные базисы, включая n-уровневые M-матрицы [7, 8].

В работах [9, 10] предложены версии малоуровневых (двух- и трехуровневых — по количеству фиксированных значений элементов матрицы) ортогональных матриц. Эти матрицы имеют нечетные порядки, соответствующие последовательностям Мерсенна и Ферма. Последовательность Мерсенна, задаваемая формулой $n = 2^k - 1$, начинается с чисел 1, 3, 5, 15, 31, … и принадлежит подмножеству чисел вида $4k - 1$. Последовательность Ферма, определяемая формулой $n = 2^{2^k} + 1$, начинается с чисел 3, 5, 17, 257, 65537, 4294967297, … и принадлежит

подмножеству чисел вида $4k+1$. В работах [11, 12] эти понятия обобщены и дополнены матрицами смежных порядков.

В настоящей статье предлагается новый подход, заключающийся в замене используемых хорошо известных базисов при сжатии кадров видеоизображений (например, на основе дискретного преобразования Фурье) на базисы, основанные на недавно открытом классе вычисляемых ортогональных матриц Адамара — Мерсенна.

Матрицы порядков, соответствующих последовательности Мерсенна, вычисляются с помощью модифицированной процедуры Сильвестра

$$\mathbf{S}_{2n} = \begin{pmatrix} \mathbf{M}_n & \mathbf{M}_n \\ \mathbf{M}_n & \mathbf{M}_n^* \end{pmatrix},$$

отличающейся от классической тем, что двухуровневая матрица $\mathbf{M}_n^*$ образована перестановкой местами ее уровней a=1 и $-b$, где b=1/2 при n=3, а в остальных случаях $b = \dfrac{q-\sqrt{4q}}{q-4}$, где $q=n+1$ — порядок матрицы Адамара. Для матриц Адамара при b=1 это приводит лишь к смене знаков всех элементов. Здесь и далее индекс „n“ соответствует порядку матрицы.

Матрицы Адамара — Мерсенна образованы дополнением к указанной основе строки и столбца:

$$\mathbf{M}_{2n+1} = \begin{pmatrix} -\lambda & e^T \\ e & \mathbf{S}_{2n} \end{pmatrix},$$

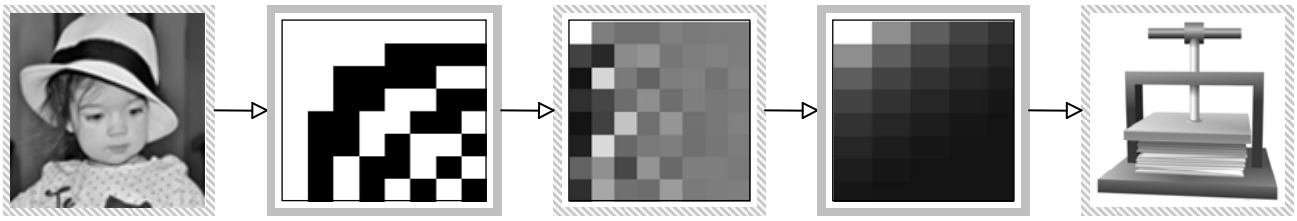
где $\lambda = -a$ — собственное число; e — собственный вектор матрицы $\mathbf{S}_{2n}$, половину элементов которого составляют элементы $-b$, другую половину — элементы a; таким образом, элементы собственного вектора находятся не численно, а аналитически.

Итерации начинаются с матрицы

$$\mathbf{M}_3 = \begin{pmatrix} a & -b & a \\ -b & a & a \\ a & a & -b \end{pmatrix}.$$

Предложенная вычислительная схема компактна и позволяет находить матрицы, альтернативные матрицам Адамара, но на нечетных значениях порядков.

Типичная последовательность этапов обработки изображения на основе матричного преобразования приведена на рис. 1.



Изображение | Преобразование Фурье | Спектральное разложение | Фильтрация | Сжатие

Рис. 1

Использование дискретного преобразования Фурье обеспечивает получение спектра изображения с низкочастотной областью, сосредоточенной в левом верхнем углу преобразованной матрицы. Применение затем фильтра устраняет высокочастотную область спектра, а статистическая обработка по Хаффману устраняет избыточность.

В алгоритме маскирования все этапы, представленные на рис. 1, сохраняются, однако матрица дискретного преобразования Фурье заменяется оригинальной матрицей ортогональ-

ного базиса. Это позволяет, во-первых, сохранить принципиальную возможность сжатия маскируемой информации, например, адаптацией процедуры фильтрации к структурным особенностям базиса, что способствует неразличимости маскированного и немаскированного видеопотоков по каналу связи. Во-вторых, неизвестная матрица и ключ маскирования в виде вектора перестановки строк и столбцов, неизвестные третьей стороне, способствуют, как показало исследование программных реализаций маскиратора [13] и демаскиратора изображений [14], надежной защите видеоизображения от перехвата и подмены.

На рис. 2, *а*, *б* приведены портреты оригинальных ортогональных симметричных матриц Адамара — Мерсенна порядков 15 и 63 соответственно [9], найденные при помощи специального программного обеспечения — исследовательского программного комплекса MMatrix [15]. На рисунке белое поле соответствует элементу матрицы со значением уровня a ($a = 1$), черное поле — элементу со значением уровня $-b$ ($|b| < 1$). Эти матрицы отличаются, в общем, от матриц Адамара вещественным значением одного из уровней, зависящим от размерности, а также тем, что они существуют на нечетных порядках. Вместе эти отличия приводят к существенному усложнению задачи демаскирования видеопотока третьей стороной. Пример выполнения процедуры маскирования и демаскирования изображения представлен на рис. 3.

а) *б*)

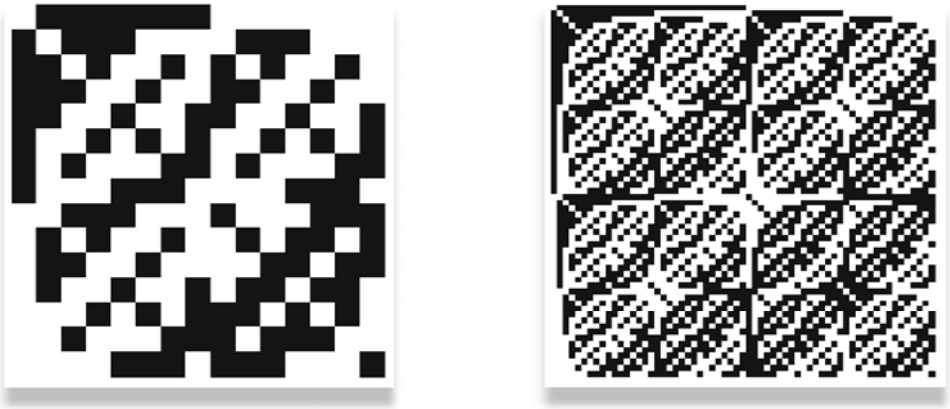
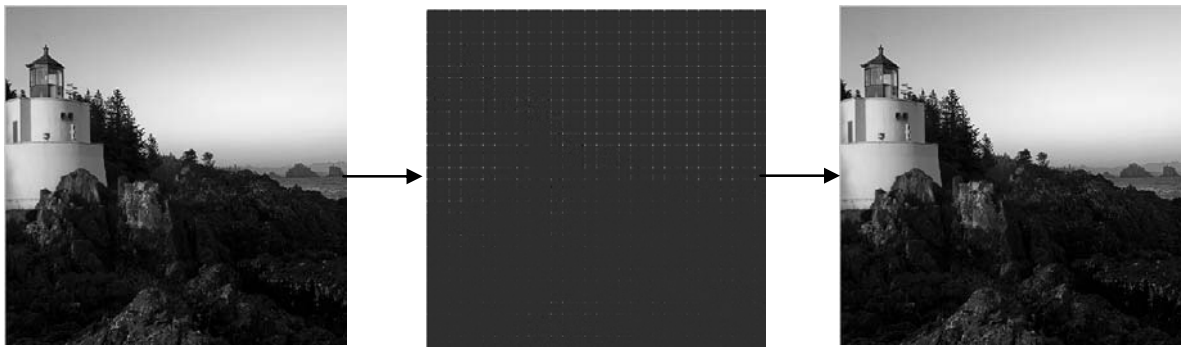


Рис. 2



Исходное изображение — Маскированное изображение — Восстановленное изображение

Рис. 3

Дополнительный аргумент рациональности использования базисов, построенных на последовательностях Мерсенна, Ферма, Эйлера [9—11], среди которых матрицы Адамара — Мерсенна отличает их близость к матрицам Адамара, состоит в том, что алгоритм их построения фрактален и матрицы, при определенной структуре алгоритма, обладают повышенной чувствительностью к изменению разрядной сетки процессора и начальным данным.

Усложнение задачи маскирования видеоизображений заключается в том, что матрица ортогонального преобразования не вычисляется заранее, а является результатом работы алгоритма, и по открытому каналу в качестве ключа передаются только настройки для ее вычисления. Не менее важны при этом и рекурсивные процедуры увеличения порядка матрицы.

Итак, в процессе поиска для алгоритмов маскирования изображений оригинальных базисов нечетных порядков, близких к матрицам Адамара по свойствам, выделен предпочтительный класс двухуровневых матриц, называемых матрицами Адамара — Мерсенна. Порядок этих матриц равен числам Мерсенна вида $2^k - 1$, а их элементы с ростом значений целочисленного аргумента k стремятся к значениям $\{1, -1\}$, как и у матриц Адамара.

Практическое применение таких матриц целесообразно в задачах повышения степени помехоустойчивости и защищенности при передаче видеоизображений. Использование для сжатия изображений алгоритма, устраняющего избыточность исходной информации (см. рис. 1), в этом случае одновременно приводит к формированию защищенного массива. При этом следует отметить, что матричные методы преобразования информации очень практичны, поскольку предполагают эффективную реализацию в современных микропроцессорных структурах, ориентированных на цифровую обработку сигналов.

СПИСОК ЛИТЕРАТУРЫ

1. *Ерош И. Л., Сергеев А. М., Филатов Г. П.* О защите цифровых изображений при передаче по каналам связи // Информационно-управляющие системы. 2007. № 5(30). С. 20—22.
2. *Литвинов М. Ю., Беззатеев С. В., Трояновский Б. К., Филатов Г. П.* Выбор алгоритма преобразования, обеспечивающего изменение структуры изображения // Информационно-управляющие системы. 2006. № 6(25). С. 2—6.
3. *Litvinov M. Y., Sergeev A. M.* Problems on formation protected digital images // Proc. of the XI Intern. Symp. on Problems of Redundancy in Information and Control Systems. St. Petersburg, 2007. P. 202.
4. *Литвинов М. Ю.* Алгоритмы маскирующих преобразований видеоинформации: Автореф. дис. … канд. техн. наук. СПб, 2009.
5. *Мироновский Л. А., Слаев В. А.* Стрип-метод преобразования изображений и сигналов. СПб: Политехника, 2006. 163 с.
6. *Van Lint J. H., Seidel J. J.* Equilateral point sets in elliptic geometry // Indagationes Mathematicae. 1966. Vol. 28. P. 335—348.
7. *Балонин Н. А., Сергеев М. Б.* М-матрицы // Информационно-управляющие системы. 2011. № 1. С. 14—21.
8. *Балонин Ю. Н., Сергеев М. Б.* М-матрица 22-го порядка // Информационно-управляющие системы. 2011. № 5. С. 87—90.
9. *Балонин Н. А., Сергеев М. Б., Мироновский Л. А.* Вычисление матриц Адамара — Мерсенна // Информационно-управляющие системы. 2012. № 5. С. 92—94.
10. *Балонин Н. А., Сергеев М. Б., Мироновский Л. А.* Вычисление матриц Адамара — Ферма // Информационно-управляющие системы. 2012. № 6. С. 90—93.
11. *Балонин Н. А., Сергеев М. Б.* О двух способах построения матриц Адамара — Эйлера // Информационно-управляющие системы. 2013. № 1. С. 7—10.
12. *Балонин Н. А.* О существовании матриц Мерсенна 11-го и 19-го порядков // Информационно-управляющие системы. 2013. № 2. С. 90—91.
13. Свид. о гос. регистрации программы для ЭВМ № 20126188124. Программа „Маскиратор изображений“/Software “Images masking” / *М. Б. Сергеев, Н. А. Балонин, Ю. Н. Балонин, А. А. Востриков.* 27.09.2012 г.
14. Свид. о гос. регистрации программы для ЭВМ № 2012618700. Программа „Демаскиратор изображений“/Software “Images recovering” / *М. Б. Сергеев, Н. А. Балонин, Ю. Н. Балонин, А. А. Востриков*. 24.09.2012 г.

15. Свид. о гос. регистрации программы для ЭВМ № 2012614356. Программа поиска М-матриц / *М. Б. Сергеев, Н. А. Балонин, Ю. Н. Балонин*. 16.05.2012 г.

Сведения об авторах

Антон Александрович Востриков — канд. техн. наук, доцент; Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, НИИ информационно-управляющих систем; заместитель директора; E-mail: vostricov@mail.ru

Юрий Николаевич Балонин — Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра вычислительных систем и сетей; программист; E-mail: yuraball@mail.ru

Рекомендована
НИИ информационно-управляющих систем

Поступила в редакцию
01.07.13 г.