УДК 004.932.2

ЦИФРОВОЕ МАСКИРОВАНИЕ МАТРИЦАМИ МЕРСЕННА И ЕГО ОСОБЫЕ ИЗОБРАЖЕНИЯ

**Балонин Ю.Н., Востриков А.А., Капанова Е.А., Сергеев А.М.,
Синицына О.И., Чернышев С.А.**

*Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Санкт-Петербург, e-mail: kaf44@guap.ru*

Рассмотрен вопрос обеспечения конфиденциальности цифровых изображений, передаваемых по открытым сетям, за счет использования метода матричного маскирования. Рассмотрен вопрос выбора квази-ортогональных матриц для двустороннего маскирования. Метод поиска матриц глобального и локального максимумов детерминанта ведется итерационной вычислительной процедурой, ориентированной на минимизацию максимального абсолютного значения элементов ортогональной матрицы. Исследуется вопрос инвариантности изображений, называемых особыми, в двустороннем матричном маскировании. Показано, что поиск особых изображений сводится к поиску перестановочных матриц с маскирующей матрицей. Рассмотрена задача выбора преобразующих матриц Мерсенна, приведены примеры конкретных «портретов» особых изображений для них. Рассмотренные преобразования и примеры полученных особых изображений относятся только к монохромным изображениям, поскольку только они представляются в виде матрицы, которая состоит из числовых значений отдельных пикселей.

Ключевые слова: цифровые изображения, двустороннее матричное маскирование, маскирующее преобразование изображений, оптимальные матрицы преобразования, квазиортогональные матрицы Мерсенна, особые изображения двустороннего маскирующего преобразования

MERSENNE MATRICES FOR DIGITAL MASKING METHOD AND ITS SPECIAL IMAGES

**Balonin Yu.N., Vostrikov A.A., Kapranova E.A., Sergeev A.M.,
Sinitsyna O.I., Chernyshev S.A.**

Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg, e-mail: kaf44@guap.ru

It is observed a matrix masking method used for solution of the question of confidentiality of digital images transmitted over open networks. It is given a choice of the quasi-orthogonal matrices for bilateral masking. Method to search global or local maximum determinant matrices is connected with an iterative computational procedure focused on the minimization of the maximum absolute values of the elements of an orthogonal matrix. We study so called special image invariances in a bilateral masking conversion. It is shown that the search for image invariances is reduced to finding special matrices permutated with matrix of the masking method. It is considered the task of selecting the Mersenne matrices for image transmission, the examples of concrete matrix «portraits» of specific images are given. The considered transformations and examples of the obtained special images refer only to monochrome images, since only they are represented in the form of a matrix that consists of numerical values of individual pixels.

Keywords: digital image, bilateral matrix masking, image masking conversion, the optimal transformation matrix, quasi-orthogonal Mersenne matrix, special images for bilateral masking conversion

Многие прикладные задачи распределенных систем сбора, хранения и передачи видеoinформации включают в себя не только процессы повышения ее качества, сжатия, преобразования форматов, но и сохранения ее конфиденциальности. Это характерно для систем мониторинга территорий, многофункциональных систем регистрации (МСР™), распределенных промышленных систем, видеосистем охраны и др., использующих открытые сети для построения их инфраструктуры [7].

В таких системах перед передачей исходное изображение полностью (или по фрагментам) преобразуется к шумоподобному виду – маскируется [6]. Преобразованное изображение передается по открытым сетям (в том числе и беспроводным), где оно оказывается под угрозой негласного несанкцио-

нированного использования. При получении преобразованного изображения на приемной стороне выполняется обратное преобразование, в результате которого происходит восстановление исходного изображения.

Одним из эффективных методов сохранения конфиденциальности является использование матричных операций в преобразовании изображений. Использование матричной арифметики характерно для обработки изображений как массива пикселей. Для преобразования могут быть использованы квадратные ортогональные по столбцам (строкам) матрицы Адамара [14], жакетные матрицы [13], матрицы Белевича [12]. В работах [1, 2, 4, 5, 8–10, 15] состав матриц и методы преобразования изображений значительно расширены новыми предложениями.

Рис. 1. Маскирование/демаскирование при передаче изображений

Во-первых, матрицы Адамара и Белевича, определенные исключительно на четных порядках вида $4t$ и $4t + 2$, где t – натуральное число, в основном уже известны либо легко подбираются. Во-вторых, современные видеосистемы оперируют с изображениями 4К, 8К и более, для которых нужны маскирующие ортогональные матрицы больших размеров с небольшим количеством значений элементов. В-третьих, нестандартные размеры изображений при использовании функции Quality Box требуют наличия квадратных матриц, в том числе нечетных порядков.

В настоящей работе рассматриваются варианты двустороннего матричного маскирования изображений с использованием квадратных квазиортогональных матриц Мерсенна, расширяющих класс матриц Адамара для нечетных порядков $4t - 1$ и имеющих так же, как и они, два значения элементов. Исследуется вопрос существования изображений, инвариантных к рассматриваемым преобразованиям – изображений, не изменяемых маскированием.

Двустороннее матричное маскирование

Схема маскирования/демаскирования передаваемых изображений в канале, в котором возможен несанкционированный доступ, показана на рис. 1. Здесь $\mathbf{M}$ – квадратная ортогональная матрица порядка n , $\mathbf{P}$ – исходное и восстановленное изображения.

Первый этап преобразования состоит в разбиении исходного изображения $\mathbf{P}$ на N одинаковых по размеру квадратных фрагментов размера $n \times n$, обозначенных как $\mathbf{X}$. Неполные фрагменты дополняются нулями до полных. Оператор, осуществляющий указанную фрагментацию изображения, обозначен на рис. 1 символом $\mathbf{S}$.

На втором этапе исходное изображение $\mathbf{P}$, разбитое на фрагменты, рассматривается как блочная матрица, состоящая из квадратных матриц вида $\mathbf{X}$. Для преобразования изображения столбцы, а затем строки ее фрагментов $\mathbf{X}$ умножаются на столбцы матрицы $\mathbf{M}$ (двустороннее матричное преобразование) согласно формуле

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

Сформированное из фрагментов $\mathbf{Y}$ изображение поступает в коммуникационный канал, передается и на приемном конце подвергается обратному двустороннему преобразованию для получения фрагментов исходной матрицы по формуле

$$\mathbf{X} = (\mathbf{M}^T)^{-1} \mathbf{Y} \mathbf{M}^{-1}. \quad (2)$$

Результирующее изображение $\mathbf{P}$ является итогом применения обратного оператора $\mathbf{S}^{-1}$, осуществляющего дефрагментацию из фрагментов вида $\mathbf{X}$ принятого изображения. В работах [5, 6] предлагается использовать ортогональные матрицы $\mathbf{M}$ ($\mathbf{M}^{-1} = \mathbf{M}^T$), так как это упрощает вычисления (2) до формулы $\mathbf{X} = \mathbf{M} \mathbf{Y} \mathbf{M}^T$, приведенной на рис. 1. В этом случае обратное преобразование совпадает с прямым с точностью до транспонирования маскирующей матрицы, а также отпадает необходимость отдельно хранить или вычислять обратную матрицу, что экономит память при непосредственной реализации метода в системе.

В качестве примера на рис. 2 приведены оригинальное изображение и результат его маскирования, полученный с использованием описанного выше способа.

Выбор ортогональных матриц маскирования

При разбиении исходного изображения на фрагменты с целью получения блочной матрицы изображения, выбирается размер блока изображения. Выбор делается исходя из размеров используемой для маскирования матрицы. Здесь решается задача определения матрицы $\mathbf{M}$, которая обеспечит лучшее приближение результата двустороннего умножения изображения к шумоподобному виду и обеспечит меньшее время преобразования всего исходного изображения.

Поскольку основная преследуемая маскированием цель – максимально уравнивать значения элементов преобразованной матрицы, то решается задача поиска в классе ортогональных матриц заданного размера таких матриц $\mathbf{M}$, у которых максимальный по модулю элемент минимален. Хорошо известное решение этой задачи относится к случаям,

когда размер матриц кратен четырем – это нормированные матрицы Адамара. Решение для четных размеров, не кратных четырем, дают так называемые конференц-матрицы, имеющие нулевую диагональ и остальные элементы равные ± 1 [1, 12].

Для нечетных порядков матриц общее решение задачи поиска ортогональных матриц с минимальным по модулю максимальным элементом получить несложно, но такие матрицы будут иметь большое число значений элементов (уровней). Число уровней оптимальных в указанном смысле ортогональных матриц линейно растет для $n = 3, 5, 7, 9, 11$, причем при $n = 13$ происходит структурное перестроение с резким ростом как претендентов на оптимум матриц, так и числа уровней. Соответственно, использование таких матриц проблематично.

В работе [3] предлагается заменить строго оптимальные матрицы локально оптимальными матрицами Мерсенна порядков $n = 2^k - 1$ и аналогичными для $n = 4t - 1$, которыми можно заменить строго оптимальные матрицы.

Матрицы Мерсенна

Приведем некоторые определения.

Определение 1. Ортогональной матрицей называется квадратная матрица A порядка n такая, что $A^T A = I$, где I – единичная матрица.

Определение 2. Квазиортогональной матрицей называется квадратная матрица A порядка n с ограниченными по модулю элементами $|a_{ij}| \leq 1$, такая, что $A^T A = \omega(n)I$, где I – единичная матрица, $\omega(n)$ – весовая функция.

Локальный максимум детерминанта квазиортогональной матрицы достигается, если любое достаточно малое по параметрам изменение матрицы не нарушает вида уравнения связи $A^T A = \omega(n)I$ при свободно заданном значении веса $\omega(n)$, но приводит к уменьшению детерминанта.

Допустимыми являются любые изменения параметров варьируемой матрицы, не нарушающие условие ортогональности ее столбцов. Весовая функция в задачах поиска условного максимума $|\det(A)|$ при ограничении вида $A^T A = \omega(n)I$ заранее не задана и сама является предметом поиска. В этом состоит важное их отличие от задачи поиска матриц Адамара с жестко заданным заранее весом $\omega(n) = n$.

Квазиортогональные матрицы порядков $n = 2^k$, вложенных в последовательность $4t$, выделены еще Сильвестром ввиду их орнаментальных свойств – способности создавать сложный фрактальный узор при исключительно простом правиле инверсии (транспонированием с масштабированием). Аналогично можно построить квазиортогональные матрицы порядков $n = 2^k - 1$, вложенных в последовательность $4t - 1$, и обладающих локальным максимумом детерминанта. Последовательность $2^k - 1$ называется последовательностью чисел Мерсенна.

Определение 3. Матрица Мерсенна [3, 11] – это квазиортогональная матрица M порядка n с элементами $a = 1$ и $-b$, где

$$b = \frac{t}{t + \sqrt{t}} \text{ для } n = 2^k - 1.$$

Классический способ построения матриц Адамара H_n порядков $n = 2^k$ основан на использовании итерационной формулы Сильвестра

$$H_{2n} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix},$$

где в качестве начального значения используется число $H_1 = 1$. Модифицированная формула Сильвестра [16] для вычисления матриц Мерсенна выглядит как

$$S_{2n} = \begin{pmatrix} M_n & M_n \\ M_n & M_n^* \end{pmatrix}.$$

Рис. 2. Оригинальное и маскированное изображения

Здесь матрица $\mathbf{M}_n^*$ образована не сменой знака, а перестановкой элементов a и $-b$. Полученная по этой формуле матрица $\mathbf{S}_{2n}$ симметрична, но ее порядок четен и на единицу меньше порядка следующей матрицы Мерсенна $\mathbf{M}_{2n+1}$. Для рекурсивного перехода от матрицы к матрице одного лишь удвоения порядка недостаточно, необходимо дополнительное окаймление матрицы $\mathbf{S}_{2n}$ добавлением строки и столбца

$$\mathbf{M}_{2n+1} = \begin{pmatrix} -\lambda & \mathbf{e}^T \\ \mathbf{e} & \mathbf{S}_{2n}^* \end{pmatrix}. \text{ Здесь } \lambda, \mathbf{e} - \text{соответственно собственное число и собственный вектор матрицы } \mathbf{S}_{2n}.$$

Полученная таким образом матрица будет симметричной и квазиортогональной. Справедливость положения следует непосредственно из условия ортогональности столбцов матрицы.

В окончательной версии алгоритма не требуется решать проблему собственных значений, поскольку если выбрать в качестве начальной симметричную матрицу

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

то собственное значение матрицы удвоенного порядка будет $\lambda = -a$. При этом половина компонент собственного вектора состоит из $-b$, остальная половина – из a .

Особые изображения двустороннего матричного маскирования

Пусть исходное изображение разбито на N одинаковых матриц $\mathbf{X}$ размером $n \times n$. Поставим задачу найти изображения, которые инвариантны к преобразованию (1), т.е. переводятся им в то же изображение с точностью до постоянного множителя – $\mathbf{M}^T$

$\mathbf{X}\mathbf{M} = \lambda \mathbf{X}$. Такие изображения называют собственными, корневыми или особыми изображениями преобразования. Число λ – соответствующим особым или корневым числом. Если исходное изображение совпадет с особым изображением используемого преобразования, то маскированное изображение совпадет с исходным и эффект маскирования достигнут не будет.

Ортогональные матрицы $\mathbf{M}$ с собственными значениями $|\lambda| = 1$ не усиливают изображения. При умножении на $\mathbf{M}$ слева поиск особых изображений сводится к стандартной задаче определения перестановочных друг с другом матриц $\mathbf{X}\mathbf{M} = \mathbf{M}\mathbf{X}$ (или $\mathbf{X}\mathbf{M} = -\mathbf{M}\mathbf{X}$).

Из матричной алгебры известно, что матрицы перестановочны (коммутируемы), если они построены на одинаковом наборе собственных векторов. Для симметричных матриц $\mathbf{M}$ собственные числа вещественны, а собственные векторы – ортогональны. В частности, коммутируема сама с собой матрица $\mathbf{X} = \mathbf{M}$, поскольку она, безусловно, построена на том же наборе собственных векторов, что и преобразующая матрица, и $\mathbf{M}^T \mathbf{X} = \mathbf{I}$ – единичная матрица. Иными словами, наиболее беззащитны изображения, похожие на преобразующую матрицу, и для успешного маскирования ей самой выгодно выглядеть хаотичной. Это качество разделяют между собой все матрицы расширяемого семейства Адамара, включая матрицы Мерсенна.

Пример

Для маскирования фрагментов изображения $\mathbf{P}$ будем использовать матрицы Мерсенна. На рис. 3 для примера приведены визуализированные в «портретах» матрицы Мерсенна порядков 7, 15, 31 и 255, на которых квадраты белого и черного цветов соответствуют значениям a и $-b$ элементов этих матриц.

Рис. 3. «Портреты» матриц Мерсенна порядков 7, 15, 31 и 255

Строки и столбцы матриц Мерсенна, как и матриц Адамара, ортогональны. Для применения в алгоритмах преобразования их нормируют так, чтобы фробениусовы нормы строк и столбцов были единичны. Каноническое разложение нормированной матрицы Мерсенна на матрицу собственных векторов V и диагональную матрицу собственных значений имеет вид $M = VDV^{-1}$. Собственные значения ортогональных матриц равны 1 или -1 .

Умножение на матрицу M можно рассматривать как умножение на ортогональную матрицу V^{-1} (поворот изображения), собственно кодирование при помощи знакопеременной матрицы $D = \text{diag}(1, -1, \dots, 1)$ и обратный поворот V . Особое изображение индифферентно к этому процессу, если состоит (частично) из инверсных операций: обратного поворота, любой диагональной матрицы D^* и поворота. При двустороннем преобразовании матрица $DD^*D = D^*$, т.е. не меняется. Отсюда следует алгоритм построения особых изображений, состоящий в вариации матрицы собственных чисел ортогональной матрицы M и ее реконструкции $P^* = VD^*V^{-1}$.

На рис. 4 приведены по два «портрета» вычисленных корневых изображений P^* для приведенных на рис. 3 матриц. Квадраты различного оттенка серого соответствуют визуализированным пикселям реального изображения.

Представленные изображения инвариантны по отношению к рассматриваемому преобразованию с использованием матриц Мерсенна. Они являются «портретами» объектов, которые не имеют отношения к множеству объектов реального мира – объектов, изображения которых передаются в рассматриваемых видеосистемах. Следовательно, можно смело утверждать, что матричное двустороннее маскирование матрицами Мерсенна может быть использовано в системах без каких-либо ограничений, вносимых изображениями, инвариантными к преобразованию (1).

Заключение

Расширение класса ортогональных матриц четных порядков, используемых для маскирования изображений, матрицами Мерсенна нечетных порядков позволяет расширить возможности при реализации систем.

Рис. 4. «Портреты» особых изображений для матриц Мерсенна порядков 7, 15, 31, 255

Для двустороннего матричного маскирования изображений матрицами Мерсенна, как и другими матрицами, существуют особые изображения, инвариантные по отношению к указанному преобразованию. Рассмотренный способ поиска особых изображений, проиллюстрированный конкретными примерами для матриц Мерсенна разных порядков, позволяет утверждать, что он может быть использован без ограничений. Особые изображения не являются портретами объектов реального мира.

Рассмотренные преобразования и примеры полученных особых изображений относятся только к монохромным изображениям, поскольку только они представляются в виде матрицы, которая состоит из числовых значений отдельных пикселей. Именно эта матрица и подвергается фрагментации при матричном преобразовании, если маскирующая матрица значительно меньше изображения.

Для цветных изображений маскирование применимо, но алгоритм реализации усложняется. Например, при представлении цветных изображений трехслойной матрицей RGB, маскированию будет подвергаться отдельно каждый из трех слоев матрицы изображения.

Работа выполнена при поддержке Минобрнауки РФ при проведении научно-исследовательской работы в рамках проектной части государственного задания в сфере научной деятельности по заданию № 2.2200.2017/ПЧ.

Список литературы

1. Балонин Н.А., Сергеев М.Б. Взвешенная конференц-матрица, обобщающая матрицу Белевича на 22-м порядке // Информационно-управляющие системы. – 2013. – № 5 (66). – С. 97–98.
2. Балонин Н.А., Сергеев М.Б. Матрица золотого сечения G10 // Информационно-управляющие системы. – 2013. – № 6 (67). – С. 2–5.
3. Балонин Н.А., Сергеев М.Б. Матрицы Мерсенна и Адамара // Информационно-управляющие системы. – 2016. – № 1 (80). – С. 2–15.
4. Балонин Ю.Н., Востриков А.А., Сергеев А.М., Егорова И.С. О взаимосвязях квазиортогональных матриц, построенных на известных последовательностях чисел // Труды СПИИРАН. – 2017. – Вып. 50. – № 1. – С. 209–223.
5. Востриков А.А., Мишура О.В., Сергеев А.М., Чернышев С.А. О выборе матриц для процедур маскирования и демаскирования изображений // Фундаментальные исследования. – 2015. – № 2–24. – С. 5335–5339.
6. Востриков А.А., Сергеев М.Б., Литвинов М.Ю. Маскирование цифровой визуальной информации: термин и основные определения // Информационно-управляющие системы. – 2015. – № 5. – С. 116–123.
7. Ерош И.Л., Сергеев А.М., Филатов Г.П. О защите цифровых изображений при передаче по каналам связи // Информационно-управляющие системы. – 2007. – № 5. – С. 20–22.
8. Balonin N.A., Sergeev M.B. Construction of Transformation Basis for Video and Image Masking Procedures // Frontiers in Artificial Intelligence and Applications. – 2014. – Vol. 262. – P. 462–467.
9. Balonin N.A., Sergeev M.B. Expansion of the Orthogonal Basis in Video Compression // Frontiers in Artificial Intelligence and Applications. – 2014. – Vol. 262. – P. 468–474.
10. Balonin N.A., Sergeev M.B. Quasi-Orthogonal Local Maximum Determinant Matrices // Applied Mathematical Sciences. – 2015. – Vol. 9. – № 8. – P. 285–293.
11. Balonin N., Sergeev M. Quasi-Orthogonal Matrices with Level Based on Ratio of Fibonacci Numbers // Applied Mathematical Sciences. – 2015. – Vol. 9. – № 85–88. – P. 4261–4268.
12. Belevitch V. Theorem of 2n-terminal Networks with Application to Conference Telephony // Electr. Commun. – 1950. – Vol. 26. – P. 231–244.
13. Finlayson K., Lee Moon-ho, J. Seberry and M. Yamada. Jacket Matrices Constructed from Hadamard Matrices and Generalized Hadamard // Australasian Journal of Combinatorics. – 2006. – Vol. 35. – P. 83–87.
14. Horadam K.J. Hadamard Matrices and Their Applications. – Princeton University Press, Princeton, NJ. – 2007. – 263 p.
15. Vostrikov A.A., Sergeev M.B. Expansion of the Quasi-Orthogonal Basis to Mask Images // Smart Innovation, Systems and Technologies. – 2015. – Vol. 40. – P. 161–168.