Инженерный вестник Дона, №1 (2024)
ivdon.ru/ru/magazine/archive/n1y2024/8967

Метод обеспечения конфиденциальности данных с применением ортогональных матриц

М.Б. Сергеев, Т.М. Татарникова, А.М. Сергеев, В.В. Боженко

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Аннотация: Обсуждается актуальность применения ортогональных матриц в симметричных системах криптографической защиты информации. Приводится схема организации матричного маскирования цифровых данных. Демонстрируются примеры и результаты маскирования и демаскирования звукового файла и изображения.
Ключевые слова: ортогональная матрица, маскирование сообщения, алгоритм маскирования/демаскирования, амплитудно-частотная характеристика, белый шум.

Введение

Совершенствование теории ортогональных и экстремальных матриц открывает новые возможности по формированию библиотеки уникальных ортогональных матриц, которые все чаще находят применение в задачах обеспечения конфиденциальности данных, включая оцифрованные изображения и аудиофайлы [1].

Анализ большинства современных источников показывает, что для обеспечения конфиденциальности, используются, в основном, криптографические методы [2,3]. Наряду с ними прослеживается тема использования матричных [4,5] или гибридных [6,7] методов защитного кодирования, с реализацией на программируемых логических интегральных схемах или процессорах цифровой обработки сигналов.

Исторически первым шифром, основанным на использовании матриц, является шифр Хилла: алгоритм, лежащий в его основе, заменяет каждые m последовательных букв открытого текста m буквами шифрованного текста. Таким образом, подстановка определяется m линейными уравнениями:

$$\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{pmatrix} \times \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_m \end{pmatrix}, \quad (1)$$

где $\mathbf{C} = \|c_i\|$ – матрица-столбец букв шифрованного текста;

$\mathbf{P} = \|p_i\|$ – матрица-столбец букв открытого текста;

$\mathbf{K} = \|k_{ij}\|$ – матрица-ключ шифрования.

Для дешифрования применяется матрица $\mathbf{K}^{-1}$, для которой справедливо:

$$\mathbf{K} \times \mathbf{K}^{-1} = \mathbf{I}, \quad (2)$$

где $\mathbf{K}^{-1}$ – матрица, обратная **K**;

I – единичная матрица.

В общем виде криптосистема, основанная на применении матриц, представляется соотношениями:

$$\mathbf{C} = E(\mathbf{P}) = \mathbf{K} \times \mathbf{P}, \quad (3)$$

где E – функция шифрования.

$$\mathbf{P} = D(\mathbf{C}) = \mathbf{K}^{-1} \times \mathbf{C} = \mathbf{K}^{-1} \times \mathbf{K} \times \mathbf{P} = \mathbf{P}, \quad (4)$$

где D – функция дешифрования.

Преимущество криптосистемы (3), (4) заключается в полном маскировании частоты вхождения отдельных символов, и чем выше порядок матрицы, тем больше информации о различиях в значениях частоты появления символов и их сочетаний скрывается в шифрованном сообщении. Благодаря этому свойству, шифрование с применением матриц также называется маскированием, а обратный процесс - демаскированием.

В настоящее время идеи криптосистемы (3), (4) распространяются на оцифрованные изображения и звук, а в качестве матрицы-ключа используются ортогональные матрицы высших порядков. Причин этому несколько:

– для ортогональной матрицы **K** справедливо условие $\mathbf{K}^{-1}=\mathbf{K}^{T}$, где $\mathbf{K}^{T}$ – транспонирование матрицы **K**;

– при совпадении порядка матрицы **K** с размером изображения или аудиофайла шифр становится абсолютно стойким;

– криптосистема является симметричной, что обеспечивает скорость шифрования, соответствующую выполнению операции умножения, например, на программируемых логических интегральных схемах;

– по закрытому каналу на принимающую сторону передается не сама матрица-ключ, а только ее параметры, достаточные для синтеза матрицы $\mathbf{K}^{-1}$.

Платой за высокую скорость шифрования является необходимость создания закрытого канала для передачи секретной информации принимающей стороне.

Описание криптосистемы, реализующей матричное маскирование цифровых данных

На рис. 1 приведена общая схема процесса маскирования цифровых данных с применением ортогональных матриц [8].

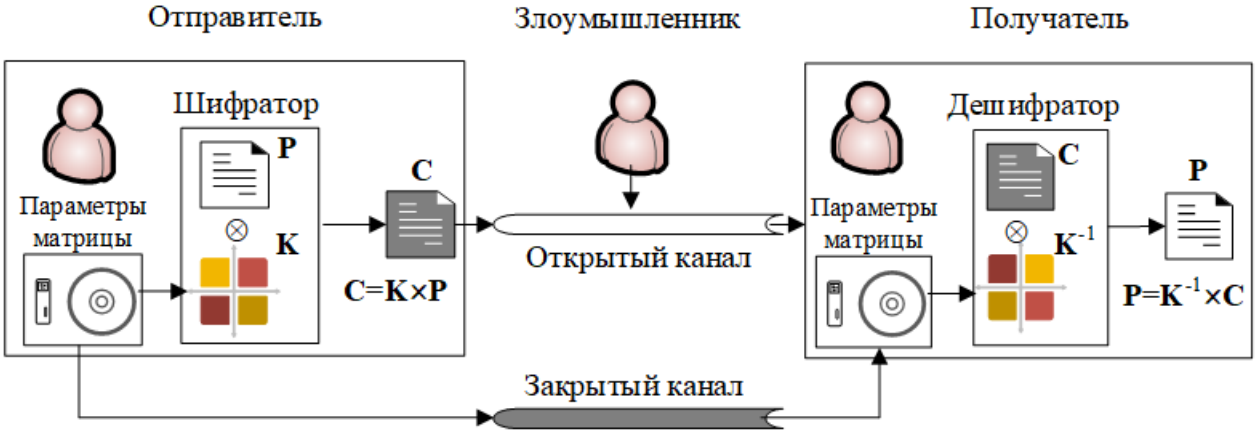

Рис. 1. Схема процесса маскирования цифровых данных с применением ортогональных матриц

Основными этапами процесса маскирования являются:

На стороне отправителя – шифрование:

– синтез ортогональной матрицы-ключа **K** порядка n;

– формирование открытого сообщения (изображения, аудиофайла) в виде матрицы размера $n \times n$. Целесообразно выбирать порядок матрицы, равный длине пакета, передаваемого по сети;

– шифрование путем математического умножения матрицы открытого сообщения **P** на матрицу-ключ **K** с получением результата в виде матрицы маскированного сообщения **C** того же размера $n \times n$.

На стороне получателя – дешифрование:

– синтез ортогональной матрицы-ключа **K** порядка n по известным параметрам, полученным по закрытому каналу;

– вычисление матрицы $\mathbf{K}^{-1}$ путем транспонирования матрицы-ключа **K** порядка n;

– дешифрование путем математического умножения матрицы маскированного сообщения **C** на матрицу $\mathbf{K}^{-1}$ с получением результата в виде матрицы открытого сообщения **P** размера $n \times n$.

Криптосистема (3), (4) может быть реализована, например, на матрицах Адамара, порядки которых кратны $4t$, где t – натуральное число, а также матрицах Мерсенна, существующих на порядках $4t - 1$. Как те, так и другие существуют в структурированных видах, в том числе по Уолшу. Такие структурированные матрицы имеют преимущества, поскольку известны алгоритмы их синтеза, в том числе высоких порядков [9].

Подготовка открытого сообщения – аудиофайла – сводится к выбору частоты дискредитации, например, 48 КГц и формированию построчных сэмплов с количеством точек отсчета, равным n. Если количество сэмплов окажется меньше n, то пустые строки матрицы **P** заполняются нулями.

Подготовка открытого сообщения – изображения – сводится к приведению размера изображения, например, $d \times l$ к размеру матрицы **P**, где центры изображения и матрицы совпадают. Образовавшиеся пустые строки матрицы **P** также заполняются нулями. Идея маскирования изображения восходит к визуальной криптографии, предложенной М. Наором и А. Шамиром на EUROCRYPT в 1994 году. Идея продемонстрирована с помощью прозрачных пленок, которые являются слоями оригинального изображения. В предлагаемом в статье методе слои изображения и ортогональной матрицы накладываются друг на друга с помощью графических редакторов.

Эксперименты по маскированию цифровых данных

Для проведения экспериментов были разработаны программы, реализованные на языке C++.

В качестве примера рассмотрим результаты маскирования и демаскирования звукового файла 108362-2-0-23.wav из датасета «UrbanSound8K» по адресу kaggle.com/datasets/chrisfilo/urbansound8k. На рис. 2 приведены графики амплитудно-частотных характеристик входного звукового сигнала, маскированного и демаскированного сигналов.

Оценку качества маскирования аудиофайла или изображения звукового сигнала предлагается выполнять по близости амплитудно-частной характеристики звукового сигнала к амплитудно-частотной характеристике белого шума [10]. Рис. 2*г* демонстрирует визуальное сходство с маскированным сигналом на рис. 2*б*. Спектр маскированного звукового сигнала близок к спектру белого гауссовского шума, среднеквадратическое отклонение между ними составляет $2{,}1379 \cdot 10^{-05}$.

На рис. 3 приведены результаты маскирования изображения:

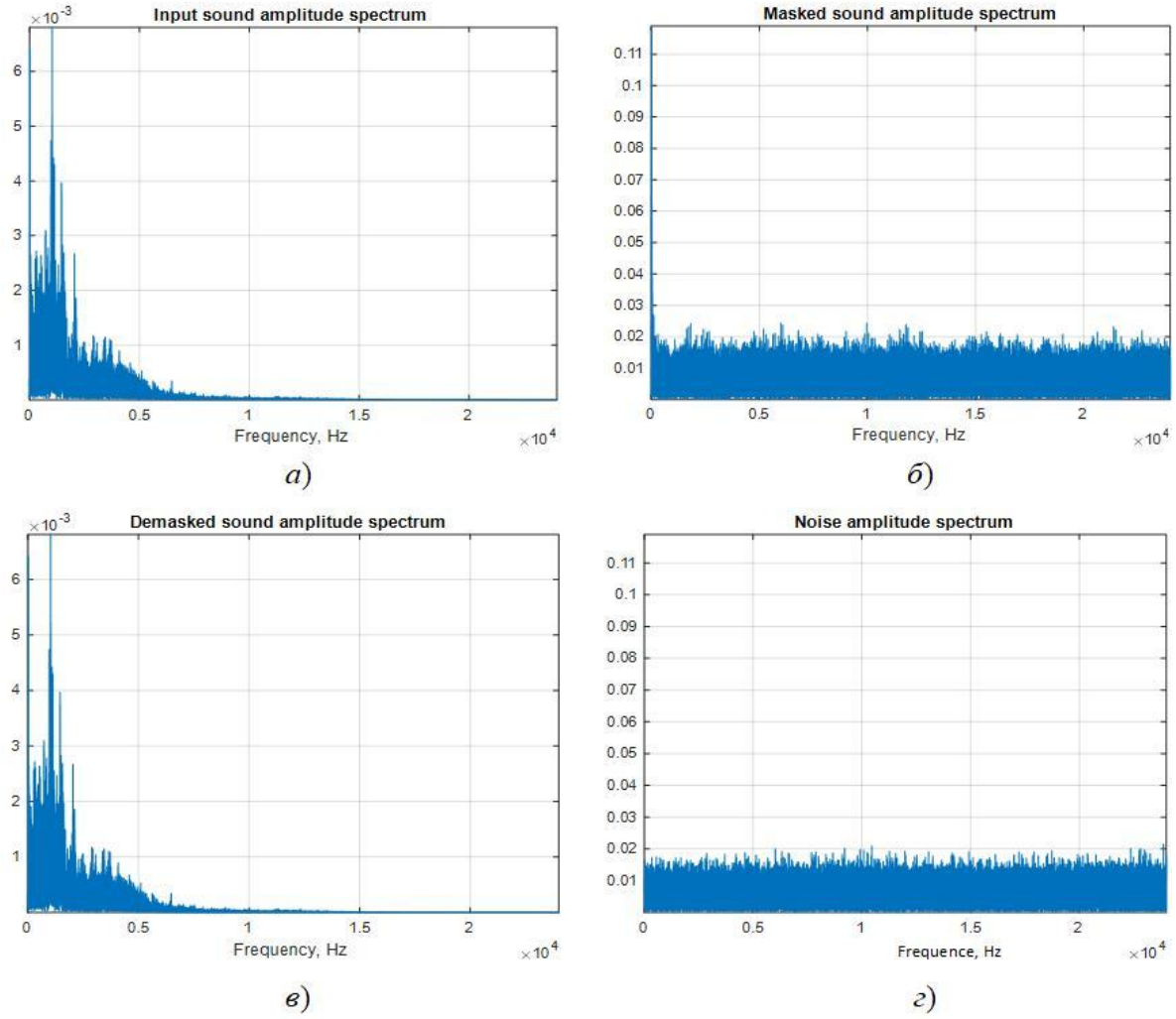

Рис. 2 – Графики отсчетов: *а*) входной сигнал; *б*) маскированный сигнал; *в*) демаскированный сигнал; *г*) белый шум

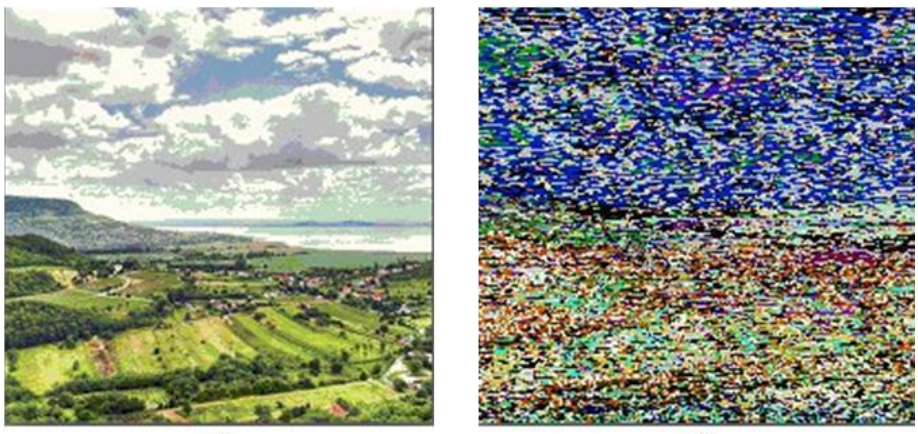

Рис. 3. Маскирование: *а*) открытое изображение; *б*) маскированное изображение

Исследования показывает, что выбор порядка матрицы-ключа влияет на качество маскирования. Так, для при совпадении порядка матрицы **K** с размером аудиофайла, шифр становится абсолютно стойким. А для изображения маскирование является предварительным этапом до шифрования, позволяющим скрыть частоту сигналов.

Выводы

Защитное преобразование цифровой информации – маскирование – выполняется по симметричной схеме шифрования, что делает применение матричного умножения с использованием ортогональных матриц предсказуемыми результатами и простотой реализации.

Маскирование цифровой звуковой информации к виду, близкому по спектру к белому шуму надежно защищает ее в коммуникационном канале от несанкционированного доступа.

Маскирование изображения можно использовать как предварительный этапом до шифрования, позволяющим скрыть частоту сигналов.

Литература

1. Luis M., Daniel L., Isabel A. A new multimedia cryptosystem using chaos, quaternion theory and modular arithmetic // Multimedia Tools and Applications. 2023. Vol. 82. pp. 35149-35181.

2. Abdallah H.A., Meshoul S.A. Multilayered Audio Signal Encryption Approach for Secure Voice Communication // Electronics. 2023. N 12. P. 2.

3. Al-laham M.M.A Method for Encrypting and Decryptingwave Files // International Journal of Network Security & Its Applications. 2018. Vol. 10, N 4. pp. 11-21.

4. Hameed Y.M., Ali N. M. An efficient audio encryption based on chaotic logistic map with 3D matrix // Journal of Theoretical and Applied Information Technology. 2018. N 96. pp. 5142-5152.

5. Farsana F.J., Devi V.R., Gopakumar K. An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams. URL: doi.org/10.1016/j.aci.2019.10.001 (дата обращения 11.09.2023).

6. Балонин Ю.Н., Востриков А.А., Куртяник Д.В., Сергеев А.М. Обогащение набора последовательностей в задаче поиска блоков симметричных матриц Адамара // Инженерный вестник Дона. 2023. № 1. URL: ivdon.ru/ru/magazine/archive/n1y2023/8155

7. Сергеев А.М. О совмещении изображений и способах их реализации // Инженерный вестник Дона. 2022. № 8. URL: ivdon.ru/ru/magazine/archive/n8y2022/7832.

8. Бескид П.П., Татарникова Т.М. О Некоторых подходах к решению проблемы авторского права в сети интернет // Ученые записки Российского государственного гидрометеорологического университета. 2010. № 15. С. 199-210.

9. Аракелов Г.Г., Грибов А.В., Михалёв А.В. Прикладная гомоморфная криптография: примеры // Фундаментальная и прикладная математика. – 2016. Т.21, № 3. С. 25–38.

10. Столбов М.Б. Алгоритм оценки отношения сигнал/шум речевых сигналов // Научно-технический вестник информационных технологий, механики и оптики. 2012. № 6 (82). С. 67-72.

References

1. Luis M., Daniel L., Isabel A. Multimedia Tools and Applications. 2023. Vol. 82. pp. 35149-35181.

2. Abdallah H.A., Meshoul S.A. Electronics. 2023. No. 12. p. 2.

3. Al-laham M.M.A International Journal of Network Security & Its Applications. 2018. Vol. 10. No. 4. pp. 11-21.

4. Hameed Y.M., Ali N. M. Journal of Theoretical and Applied Information Technology. 2018. No. 96. pp. 5142-5152.

5. Farsana F.J., Devi V.R., Gopakumar K. URL: doi.org/10.1016/j.aci.2019.10.001 (accessed 11/09/2023).

6. Balonin N.A., Vostrikov A.A., Kurtyanyk D.V., Sergeev A.M. Inzhenernyj vestnik Dona. 2023. № 1. URL: ivdon.ru/ru/magazine/archive/n1y2023/8155.

7. Sergeev A.M. Ttrudy uchebnykh zavedeniy svyazi. 2022. Inzhenernyj vestnik Dona. 2023. № 8. URL: ivdon.ru/ru/magazine/archive/n8y2022/7832.

8. Beskid P.P., Tatarnikova T.M. Uchenyye zapiski Rossiyskogo gosudarstvennogo gidrometeorologicheskogo universiteta. 2010. № 15. pp. 199-210.

9. Arakelov G.G., Gribov A.V., Mikhalev A. V. Fundamentalnaya i prikladnaya matematika. 2016. Vol. 21. № 3. pp. 25-38.

10. Stolbov M.B. Nauchno-Tehnicheskii Vestnik Informatsionnykh Tekhnologii, Mekhaniki i Optiki**.** 2012. № 6 (82). pp. 67-72.

Дата поступления: 5.12.2023

Дата публикации: 23.01.2024