Скремблирование цифровых изображений

А.Н. Земцов, В.Ю. Цыбанов

Волгоградский государственный технический университет

Аннотация: В работе анализируется использование преобразования В.И. Арнольда для скремблирования цифровых изображений. Предлагаемый алгоритм реализован в составе разрабатываемой библиотеки Luka обработки медицинских изображений в формате DICOM, и обеспечивает дополнительную криптографическую и стеганографическую защиту персональных данных пациента. Рассматриваются вопросы оценки эффективности разработанного программного модуля с помощью индекса структурного сходства.
Ключевые слова: Преобразование Арнольда, скремблирование, пиковое отношение сигнала к шуму, среднеквадратичное отклонение, индекс структурного сходства.

Под скремблированием понимают преобразование данных с целью получения новых свойств у результирующей последовательности, например, равновероятную встречаемость «1» и «0». Скремблеры используются как отдельный этап в алгоритмах криптографии и стеганографии [1], что позволяет повысить устойчивость алгоритма к преднамеренным внешним воздействиям. С развитием инфокоммуникационных технологий становится невозможным обеспечить абсолютный контроль каналов передачи данных, поэтому вопросы защиты информации становятся все более актуальными.

Цифровые изображения характеризуются значительной визуальной избыточностью [2]. Под цифровым изображением понимается дискретное поле f_{ij} – матрица значений $m \times n$, $f_{ij} = f(x_i, y_j)$. Таким образом, изображение f – исходное изображение, т.е. матрица фиксированных значений $f(x, y)$ взятых в фиксированных точках (x_i, y_j), т.е. $f(x_i, y_j)$ – значения пикселей исходного изображения, а $g(x_i, y_j)$ – значения пикселей полученного в результате обработки изображения.

В 1960-х гг. известный советский математик Владимир Игоревич Арнольд для иллюстрации двумерного отображения, фазовое пространство которого представляет собой поверхность тора, предложил изображение в

виде головы кота [3]. Оператор отображения описывается системой уравнений:

$$\begin{matrix} x_{n+1} = x_n + y_n \\ y_{n+1} = x_n + 2 \cdot y_n \end{matrix} (\mathrm{mod}\ N) = T \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\mathrm{mod}\ N), \quad (1)$$

где $T \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ – матрица преобразования, причем, $\det T = 1 \cdot 2 - 1 \cdot 1 = 1$, и мера любой области изображения сохраняется. Результат вычисления преобразования Арнольда показан на рисунке 1.

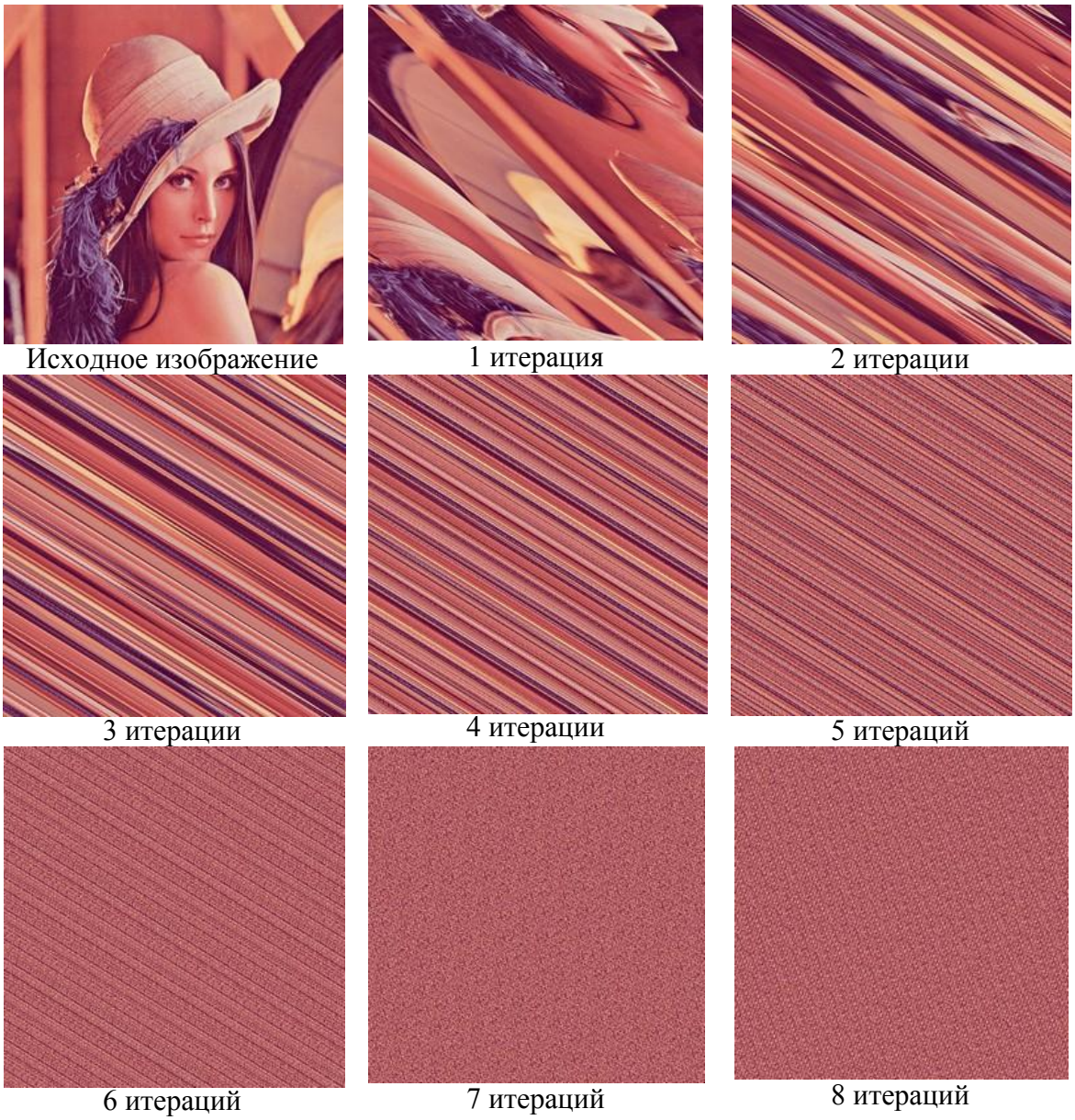

Рис. 1. – Результат вычисления преобразования Арнольда

Информацию о состоянии здоровья пациента относят к специальным категориям персональных данных. Описанное отображение реализовано в виде программного модуля в составе разрабатываемой библиотеки Luka для защиты медицинских изображений в формате DICOM, а также для популярного формата изображений стандартов JPEG [4] и JPEG 2000 [5], в том числе, с использованием преобразования Ле Галла [6]. Разрабатываемая библиотека используется для визуализации конкретных анатомических структур пациента из стандартных медицинских исследований. Информация о состоянии здоровья пациента встраивается в медицинские изображения [7]. Поддержка форматов JPEG и JPEG 2000 необходима для простоты работы врача-диагноста, позволяя обеспечить предварительный поиск и просмотр, быстрый совместный анализ результатов исследований, упрощенное формирование отчетов и т.п. Совместный доступ к персональным данным пациента предполагает передачу данных по сети, в том числе, посредством веб-технологий [8], и введение рекомендаций по использованию дополнительных криптографических и стеганографических средств [9].

Для оценки вносимых искажений можно использовать среднеквадратичное отклонение Mean Square Error [10], $MSE = \frac{1}{m \cdot n} \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \left| f(x_i, y_j) - g(x_i, y_j) \right|^2$, или метрику Root Mean Square [11], которая является разновидностью среднеквадратичного отклонения, и представляется в следующем виде:

$$RMS = \sqrt{\frac{1}{m \cdot n} \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \left| f(x_i, y_j) - g(x_i, y_j) \right|^2} \quad (2)$$

Согласно этой метрике в изображение были внесены сильные искажения при малозначительном понижении яркости на несколько процентов, которое не может быть зарегистрировано с помощью человеческой системы восприятия. С другой стороны, зашумленные

изображения, а также содержащие муар, будут оцениваться как незначительно искаженные.

Другая методика измерения сходства двух изображений заключается в вычислении индекса структурного сходства Structural SIMilarity index (SSIM) [7], которая была разработана в качестве замены метрик среднеквадратичного отклонения и пикового отношения сигнала к шуму, как не учитывающих особенности человеческой системы восприятия. Полученные значения индекса структурного сходства показаны на рисунке 2.

Вычисление индекса структурного сходства основывается не на усредненном попиксельном отклонении, а на сравнении блоков пикселей 8×8 пикселей, которое производится по трем компонентам: яркости, контрасту и структурной похожести. Полученные значения используются для вычисления итогового результата, когда значение индекса структурного сходства представляет собой интегральную функцию яркости, контрастности и структурной похожести $SSIM(x,y) = f\big(l(x,y), c(x,y), s(x,y)\big)$, где $l(x,y)$ – показатель сравнения интенсивности (яркости), $c(x,y)$ – показатель сходства контрастности, $s(x,y)$ – показатель структурного сходства.

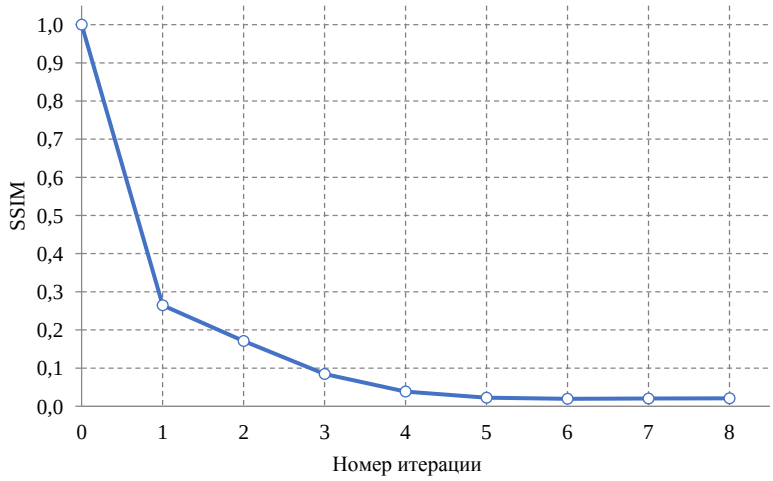

Рис. 2. – Зависимость индекса структурного сходства от номера итерации

Предлагаемый алгоритм скремблирования цифровых изображений, основанный на преобразования В.И. Арнольда, демонстрирует свою эффективность, обеспечивая дополнительную криптографическую и стеганографическую защиту персональных данных пациента. Уже на 1-й итерации изображение существенно искажается, что подтверждается оценками экспериментальных данных. Начиная с 4-й итерации, можно считать, что корреляция с исходным изображением носит несущественный характер.

Литература

1. Shih F.Y. Digital Watermarking and Steganography: Fundamentals and Techniques, Second Edition, CRC Press, 2017. 270 p.
2. Donoho D.L. Compressed sensing // IEEE Transactions on Information Theory. 2006. 52(4). pp.1289-1306.
3. Volos C., Jafari S., Kengne J. Nonlinear Dynamics and Entropy of Complex Systems with Hidden and Self-excited Attractors, MDPI, 2019. 290 p.
4. Shi Y.Q., Sun H. Image and Video Compression for Multimedia Engineering Fundamentals, Algorithms, and Standards, Third Edition CRC Press, 2019.
5. ISO/IEC 15444-1 ITU-T Rec. T.800, Information Technology – JPEG 2000 Image Coding System: Core Coding System, 2019. 196 p.
6. Zemtsov A.N. Medical image coding using Le Gall transform // Information Technologies in Science, Management, Social Sphere and Medicine, 2017. pp. 148-151.
7. Земцов А.Н., Аль-Макреби И.М. Исследование устойчивости цифровых водяных знаков-логотипов, внедряемых в статические изображения // Инженерный вестник Дона, 2015, № 2, ч.2. URL: ivdon.ru/ru/magazine/archive/n2p2y2015/2963.
8. Идрисова Ж.В., Кудусова М.И., Идигова Л.С. Социальные сервисы web 2.0 как составляющая информатизации образовательных организаций //

Инженерный вестник Дона, 2019, № 1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5648.

9. Галушка В.В., Петренкова С.Б., Дзюба Я.В., Панченко В.А. Сетевая стеганография на основе ICMP-инкапсуляции // Инженерный вестник Дона, 2018, № 4. URL: ivdon.ru/ru/magazine/archive/n4y2018/5306.
10. Newlin D.R., Seldev C.C. Medical image denoising using different techniques // International Journal of Scientific Research. 2020. 9(3). pp. 1061-1066.
11. Земцов А.Н., Аль-Макреби И.М. Об оценке вносимых искажений методом маркирования в низкочастотной области вейвлет-спектра изображения // Инженерный вестник Дона, 2015, № 2, ч.2. URL: ivdon.ru/ru/magazine/archive/n2p2y2015/2962.

References

1. Shih F.Y. Digital Watermarking and Steganography: Fundamentals and Techniques, Second Edition, CRC Press, 2017. 270 p.
2. Donoho D.L. IEEE Transactions on Information Theory. 2006. 52(4). pp.1289-1306.
3. Volos C., Jafari S., Kengne J. Nonlinear Dynamics and Entropy of Complex Systems with Hidden and Self-excited Attractors, MDPI, 2019. 290 p.
4. Shi Y.Q., Sun H. Image and Video Compression for Multimedia Engineering Fundamentals, Algorithms, and Standards, Third Edition CRC Press, 2019.
5. ISO/IEC 15444-1 ITU-T Rec. T.800, Information Technology – JPEG 2000 Image Coding System: Core Coding System, 2019. 196 p.
6. Zemtsov A.N. Information Technologies in Science, Management, Social Sphere and Medicine, 2017. pp. 148-151.
7. Zemtsov A.N., Al-Makrebi I.M. Inzhenernyj vestnik Dona, 2015, № 2-2. URL: ivdon.ru/ru/magazine/archive/n2p2y2015/2963.
8. Idrisova Zh.V., Kudusova M.I., Idigova L.S. Inzhenernyj vestnik Dona, 2019, № 1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5648.

9. Galushka V.V., Petrenkova S.B., Dzyuba YA.V., Panchenko V.A. Inzhenernyj vestnik Dona, 2018, № 4. URL: ivdon.ru/ru/magazine/archive/n4y2018/5306.
10. Newlin D.R., Seldev C.C. International Journal of Scientific Research. 2020. 9(3). pp. 1061-1066.
11. Zemtsov A.N., Al-Makrebi I.M. Inzhenernyj vestnik Dona, 2015, № 2-2. URL: ivdon.ru/ru/magazine/archive/n2p2y2015/2962.