DOI 10.37882/2223-2966.2025.04.08

АРХИТЕКТУРА И ЗАДАЧИ ПРОГРАММНОГО КОМПЛЕКСА ПО ИЗУЧЕНИЮ И ТЕСТИРОВАНИЮ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ И ПРОГРАММНЫХ МОДЕЛЕЙ ШИФРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ХАОТИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

ARCHITECTURE AND TASKS OF A SOFTWARE COMPLEX FOR STUDYING AND TESTING STEGANOGRAPHIC SYSTEMS AND SOFTWARE ENCRYPTION MODELS USING CHAOTIC TRANSFORMATIONS

E. Golovkov

Summary. The article presents the architecture and tasks of a software complex for studying and testing steganographic systems and software encryption models using chaotic transformations. The complex enables testing various encryption methods, evaluating the imperceptibility and throughput of stegosystems, and analyzing chaotic maps such as the Arnold Map, Baker Map, DNA transformations, and sinusoidal maps. The main tasks of the complex include result visualization and comparative analysis of methods. The developed software complex demonstrates high versatility and applicability for scientific research in the fields of steganography and information security.

Keywords: steganographic systems, chaotic transformations, software complex, information security, data encryption.

Головков Евгений Владимирович
аспирант, Петербургский Государственный Университет Путей Сообщения Императора Александра I, г. Санкт-Петербург
golovkov-ev@mail.ru

Аннотация. В статье представлена архитектура и задачи программного комплекса для изучения и тестирования стеганографических систем и программных моделей шифрования с использованием хаотических преобразований. Комплекс позволяет проводить тестирование различных методов шифрования, оценивать незаметность и пропускную способность стегосистем, а также анализировать хаотические карты, такие как Карта Арнольда, Карта Бейкера, ДНК-преобразования и синусоидальные карты. Приведены основные задачи комплекса, включая визуализацию результатов и проведение сравнительного анализа методов. Разработанный программный комплекс демонстрирует высокую универсальность и применимость для научных исследований в области стеганографии и информационной безопасности.

Ключевые слова: стеганографические системы, хаотические преобразования, программный комплекс, информационная безопасность, шифрование данных.

Введение

С развитием цифровых технологий и сети Интернет, защита информации становится одной из самых актуальных проблем. Обмен данными в глобальных сетях требует эффективных методов защиты, особенно в условиях постоянных угроз утечек и атак на конфиденциальность данных. Одним из таких методов является стеганография — наука о скрытии информации в обычных носителях, таких как изображения, звуки и видео. В отличие от традиционного шифрования, стеганография обеспечивает скрытность сообщения, позволяя передавать его незаметно для третьих лиц, что делает этот метод важным инструментом в обеспечении безопасности данных.

Особое внимание в последние годы уделяется применению хаотических преобразований в стеганографии. Хаос, как математическое явление, характеризуется высокой чувствительностью к начальным условиям, что делает его отличным инструментом для создания криптографических алгоритмов и методов для стеганографии. Хаотические преобразования обладают свойствами непредсказуемости и случайности, что увеличивает уровень безопасности и устойчивости к различным видам атак.

Тем не менее, несмотря на потенциал хаотических преобразований в стеганографии, их использование требует комплексного подхода к тестированию и оценке эффективности. Для этого необходимо наличие специализированных программных комплексов, которые могли бы не только реализовывать эти преобразования, но и тестировать их на реальных данных, а также оценивать ключевые характеристики стеганографических систем, такие как незаметность, пропускная способность и устойчивость к атакам.

Целью данной работы является разработка программного комплекса для изучения и тестирования стеганографических систем и программных моделей шифрования, основанных на хаотических преобразованиях. В рамках этой работы будет представлен подход, который включает анализ различных хаотических карт, таких как Карта Арнольда, Карта Бейкера, ДНК-преобразования и синусоидальные карты. Комплекс позволит исследовать не только характеристики стегосистем, но и провести сравнительный анализ различных методов с точки зрения их безопасности и эффективности.

Материалы и методы

1. *Архитектура программного комплекса*

Разработанный программный комплекс для изучения и тестирования стеганографических систем и программных моделей шифрования хаотическими преобразованиями имеет модульную архитектуру, обеспечивающую гибкость, масштабируемость и удобство использования.

Ключевые элементы архитектуры включают:

1. Модуль управления системой.
- Основной компонент, координирующий работу всех остальных модулей. Обеспечивает выполнение основных задач и управление потоками данных между модулями.
2. Стеганографический модуль.
- Состоит из трёх подмодулей:
— Модуль сокрытия. Реализует алгоритмы внедрения скрытых сообщений в контейнеры.
— Модуль извлечения. Предназначен для восстановления скрытых сообщений из стегоконтейнеров.
— Модуль шифрования. Обеспечивает дополнительную защиту данных с использованием хаотических преобразований.
3. Модуль управления алгоритмами.
- Служит связующим звеном между алгоритмами и стеганографическим модулем. Позволяет интегрировать и управлять различными алгоритмами обработки данных.
4. Модуль управления элементами пользовательского интерфейса (UI).
- Обеспечивает взаимодействие пользователя с системой, включая визуализацию результатов и настройку параметров.
5. Модуль вспомогательных функций.
- Включает в себя инструменты для логирования, обработки ошибок и выполнения сервисных операций.

Архитектура обеспечивает взаимодействие всех модулей, что позволяет проводить полный цикл тестирования стеганографических систем — от внедрения и шиф-

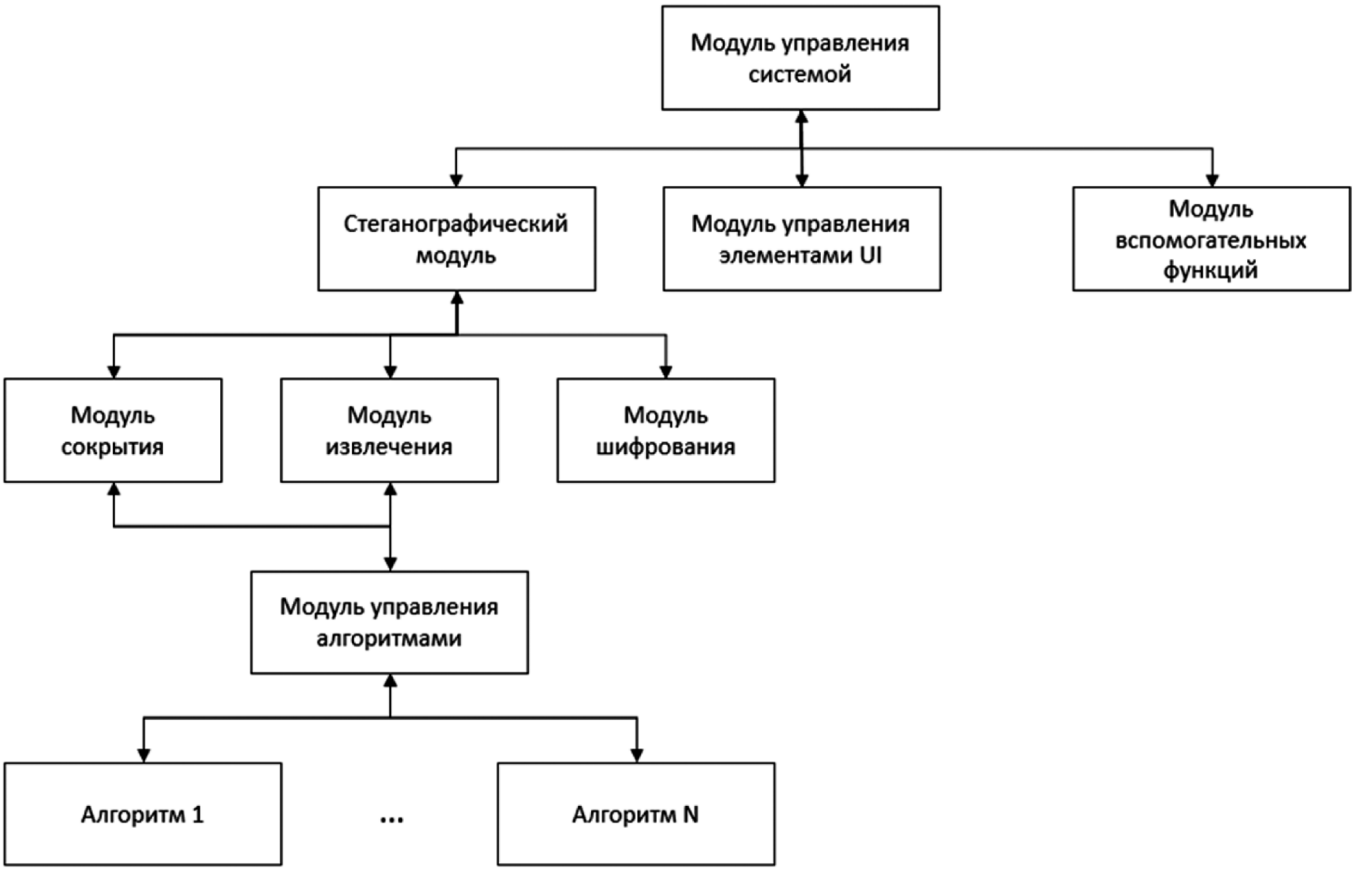

Рис. 1. Блок-схема архитектуры программного комплекса

рования до анализа извлечённых данных. На рисунке 1 представлена блок-схема архитектуры программного комплекса, отражающая взаимодействие модулей между собой.

2. *Задачи программного комплекса*

Автором были поставлены основные задачи, которые должен решать программный комплекс, предназначенный для изучения и тестирования стеганографических систем и моделей шифрования с использованием хаотических преобразований.

Первая задача заключается в обеспечении эффективного анализа алгоритмов сокрытия информации в цифровых изображениях. Это включает в себя как оценку их незаметности для стороннего наблюдателя, так и проверку устойчивости к атакам, что позволяет исследовать слабые места системы и усиливать ее защиту.

Вторая задача связана с реализацией методов шифрования данных, основанных на хаотических преобразованиях. Такие методы характеризуются высокой чувствительностью к начальным параметрам и сложной структурой выходных данных, что делает их особенно эффективными для защиты информации. Комплекс предоставляет возможность тонкой настройки параметров преобразований, адаптируя их под конкретные задачи.

Третья задача включает интеграцию всех компонентов стеганографической системы в единую архитектуру, что позволяет моделировать их взаимодействие и оценивать влияние различных комбинаций алгоритмов на общую производительность. Благодаря продуманной системе визуализации пользователи могут наблюдать изменения, происходящие на этапах сокрытия, шифрования и извлечения информации, что способствует глубокому пониманию принципов работы системы.

Четвертая задача направлена на решение образовательных и исследовательских потребностей. Комплекс должен быть полезен как для профессионалов, так и для студентов, позволяя не только использовать готовые алгоритмы, но и внедрять новые. Таким образом, он обеспечивает широкие возможности для экспериментов и дальнейших разработок в области стеганографии и защиты информации.

3. *Используемые хаотические преобразования*

В рамках программного комплекса для изучения и тестирования стеганографических систем используются следующие хаотические преобразования:

Карта Кота Арнольда

Карта Кота Арнольда позволяет перемешивать пиксели изображения таким образом, что результат визуально напоминает случайный шум. Однако, применяя обратное преобразование, можно восстановить исходное изображение. Основная задача, решаемая с использованием этой карты, — анализ устойчивости стеганографических систем к нарушителям, которые пытаются обнаружить скрытые данные за счет пространственных изменений.

Математическое описание:

$$p' = (2p + q) \bmod 1,\ q' = (p + q) \bmod 1. \quad (1)$$

В матричной форме эти соотношения имеют следующий вид как представлено в уравнении 2:

$$\begin{vmatrix} p' \\ q' \end{vmatrix} = \begin{vmatrix} 2 & 1 \\ 1 & 1 \end{vmatrix} \begin{vmatrix} p \\ q \end{vmatrix} \bmod 1 = \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix} \begin{vmatrix} p \\ p \end{vmatrix} \bmod 1. \quad (2)$$

Где p, q — это координаты пикселя.

Карта Бейкера

Карта Бейкера используется для создания высокой степени перемешивания данных в контейнере. Она особенно эффективна при работе с изображениями, обладающими регулярной структурой.

Математическое описание выглядит следующим образом:

$$(p', q') = \begin{cases} (2p, q / 2) \text{ если } 0 \le p < 1 / 2 \\ (2 - 2p, 1 - q / 2) \text{ если } 1 / 2 \le p < 1. \end{cases} \quad (3)$$

ДНК-преобразования

ДНК-преобразования представляют собой инновационный подход, основанный на использовании биоинформатических принципов. В данном случае данные кодируются в виде последовательностей, аналогичных ДНК. Это позволяет повысить скрытность и сложность обнаружения.

Пример: для представления данных используются правила дополнения Уотсона-Крика (A ↔ T, C ↔ G), а преобразования выполняются в соответствии с выбранной последовательностью.

С точки зрения стеганографических методов, эти нуклеотиды можно закодировать двоичными числами, например:

$$A \to 00, T \to 11, G \to 01, C \to 10.$$

Таким образом, пары A & T и G & C также становятся взаимодополняющими. При этом существуют 24 различных типа правил кодирования ДНК, из которых только восемь соответствуют принципу дополнения Уотсона-

Крика. В нашем исследовании используются именно эти восемь правил для шифрования каждого пикселя изображения в процессе кодирования ДНК.

Таблица 1.

Правила кодирования ДНК [1]

Правило	1	2	3	4	5	6	7	8
00	A	A	T	T	G	G	C	C
01	C	G	C	G	A	T	A	T
10	G	C	G	C	T	A	T	A
11	T	T	A	A	C	C	G	G

ДНК-преобразования применяются для усиления скрытности данных, так как сложные взаимосвязи между закодированными последовательностями усложняют обнаружение скрытой информации и увеличивают устойчивость к попыткам взлома. Подробно применение данного метода было разобрано в отдельной статье [2].

Синусоидальные карты

Эти карты основаны на использовании тригонометрических функций для создания хаотической последовательности. Синусоидальные преобразования применяются для случайного перемешивания пикселей, сохраняя их первоначальные значения.

Пример уравнения:

$$p_{n+1} = \alpha \sin(\pi p_n). \quad (4)$$

где α — коэффициент усиления хаотического эффекта, а x_n — текущее значение пикселя.

Эти хаотические преобразования позволяют программному комплексу выполнять задачи анализа устойчивости, оценки хаотичности преобразований и разработки алгоритмов, устойчивых к различным видам атак.

4. *Методы оценки стегосистем*

Методы оценки эффективности и надежности стегосистем базируются на ряде ключевых метрик, которые позволяют анализировать устойчивость, скрытность и хаотичность системы. Среди наиболее значимых показателей выделяются NPCR, UACI, корреляция соседних пикселей и энтропия.

NPCR (Number of Pixels Change Rate) — это метрика, которая измеряет процент изменившихся пикселей в изображении после внесения скрытого сообщения. Она отражает способность стегосистемы изменять структуру изображения при минимальном визуальном воздействии. Формула для вычисления NPCR выглядит следующим образом:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100, \quad (5)$$

где D (i, j) — функция, принимающая значение 1, если пиксели на позиции (i, j) различаются в двух изображениях, и 0 — в противном случае; W и H — ширина и высота изображения.

UACI (Unified Average Changing Intensity) — это метрика, оценивающая среднее изменение интенсивности пикселей между исходным и измененным изображениями. Она вычисляется по формуле:

$$UACI = \frac{1}{W \times H} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100 \quad (6)$$

где $C_1(i, j)$ и $C_2(i, j)$ — значения интенсивности пикселей в исходном и измененном изображении соответственно.

Корреляция соседних пикселей — важный показатель, демонстрирующий степень схожести между значениями соседних пикселей в изображении. Чем ниже корреляция, тем выше хаотичность системы. Коэффициент корреляции

r вычисляется по следующей формуле:

$$r = \frac{\sum_{i=1}^{N}(x_i - \mu_x)(y_i - \mu_y)}{\sqrt{\sum_{i=1}^{N}(x_i - \mu_x)^2 \cdot \sum_{i=1}^{N}(y_i - \mu_y)^2}}, \quad (7)$$

где x_i и y_i — значения интенсивности двух соседних пикселей, а μ_x и μ_y — их средние значения.

Энтропия — метрика, отражающая уровень неопределенности в распределении значений пикселей. Высокое значение энтропии говорит о большей сложности и хаотичности стегосистемы. Энтропия вычисляется по следующей формуле:

$$H = -\sum_{i=0}^{255} p_j \log(p_j). \quad (8)$$

Где p_i — вероятность появления каждого значения интенсивности i в изображении.

5. *Программный интерфейс*

Интерфейс разработанного программного обеспечения предназначен для обеспечения подробного учебного взаимодействия пользователя с функционалом стеганографической системы. Дизайн интерфейса основывается на принципах интуитивности и максимизации наглядности действий, необходимых для выполнения операций по кодированию и декодированию сообщений. На рисунке 2 представлен разработанный пользовательский интерфейс программного комплекса.

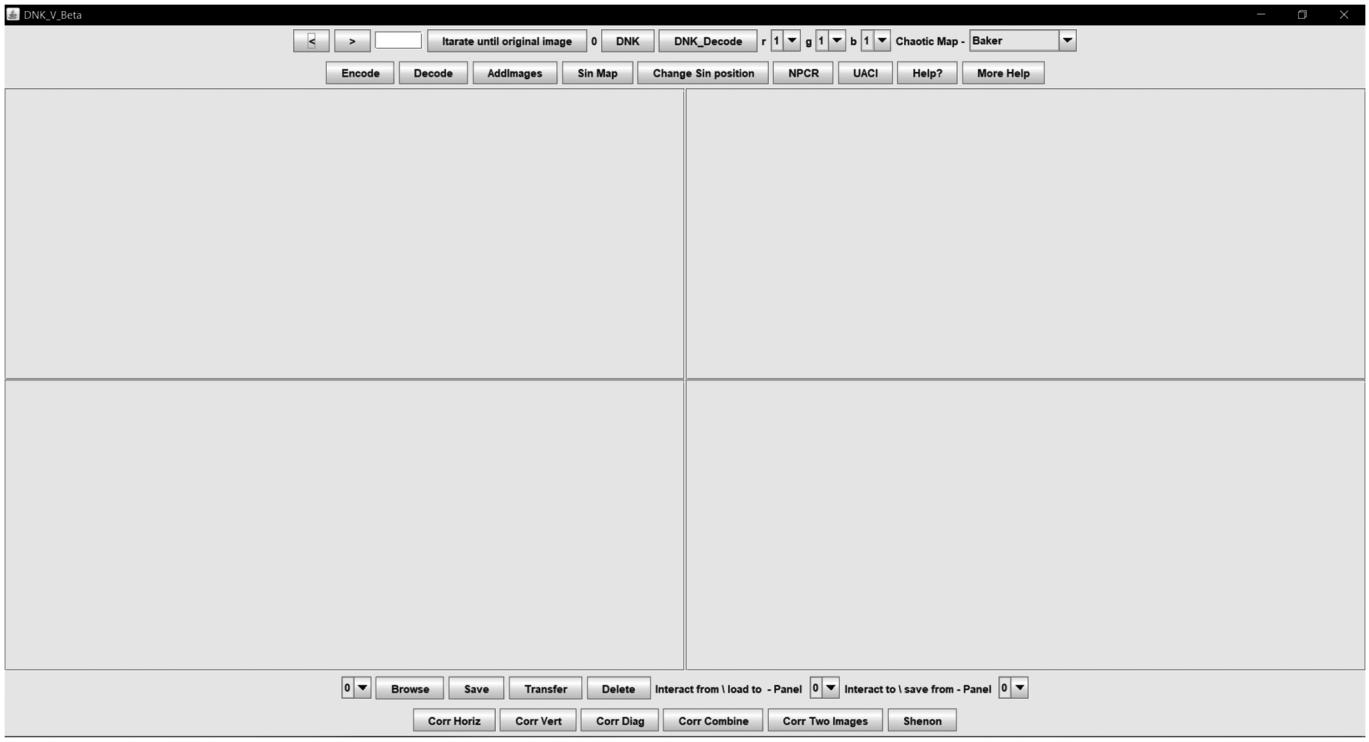

Рис. 2. Пользовательский интерфейс программного комплекса

В основе взаимодействия лежат 4 панели для работы с изображениями в центре. На них можно загрузить изображения с помощью основных кнопок управления внизу экрана, которые включают в себя кнопки:

- Browse — позволяет открыть проводник для выбора изображения, которое пользователь хочет загрузить в программу;
- Save — позволяет открыть проводник для выбора места, куда пользователь хочет сохранить изображение из программы;
- Transfer — позволяет переместить изображение из одной панели в другую;
- Delete — удаляет изображение, очищает панель до изначального состояния;
- Interact from \ load to — Panel — данное поле задает выбор панели для взаимодействия, например, в какую из панелей загрузить изображение, или из какой панели выполнять то или иное действие при хаотических преобразованиях и стеганографии;
- Interact to \ save from — Panel — данное поле задает выбор панели для результатов взаимодействия при хаотических преобразованиях, и стеганографии, а также поле из которого сохраняется на компьютер изображение;
- Corr Horiz, Corr Vert, Corr Diag — рассчитывает горизонтальную, вертикальную, и диагональную корреляцию одного изображения из поля interact from и выводит результат на экран;
- Corr Combine — рассчитывает среднее математическое из трех выше перечисленных значений корреляции изображения;
- Corr Two Images — рассчитывает корреляцию между двумя изображениями;
- Shenon — расчитывает коэффициент энтропии изображения.

Как видно из перечисления выше, нижняя панель изображения состоит из основных элементов управления изображениями, и из основных элементов для расчёта показателей для оценки хаотичности получившихся результатов.

Так же в нижней части есть элемент управления, который не приведен в списке сверху, это переключатель, состоящий из трех полей — 0, 1, 2 значение этого поля регулирует верхнюю панель. Для экономии места, и исключения нагромождения верхней панели по управлению параметрами хаотических преобразований и стеганографических преобразований, верхняя панель разделена на три раздела, которые и переключаются с помощью этого поля. Ниже, на рисунках 3, 4, 5 представлены существующие разделы верхней панели, они разделяются по задачам:

0. Данный раздел состоит из элементов управления для реализации хаотических преобразований Кота Арнольда, Бейкера, Синусной карты, шифрования ДНК, а также вычисления параметров NPCR и UACI изображения. С помощью этого раздела были проведены первые исследования, и написана статья [3]

1. Раздел под цифрой 1 посвящен реализации двух генераторов ключей Хаотической системы скрытого ат-

Рис. 3. Раздел 0 — Хаотические преобразования

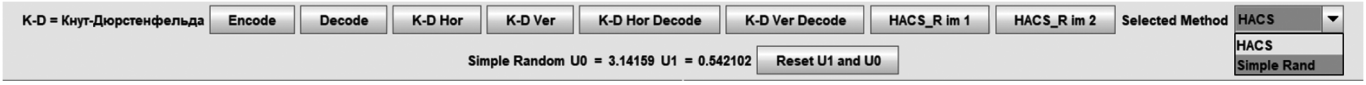

Рис. 4. Раздел 1 — генераторы ключей HACS, Simple Rand и алгоритм перестановки KD

Рис. 5. Раздел 2 — стеганографические методы

трактора (HACS), Simple Rand, а также реализации системы шифрования изображения на их основе с использованием алгоритма перестановки Кнута-Дюрстенфельда, подробнее они описаны в статье [4].

2. Раздел 2 реализует три стеганографических алгоритма: HUGO, HUGO +— 1, и LSB, также реализован выбор цвета пикселя r, g, b для встраивания, и количество битов от байта, использующихся для встраивания. Данный раздел был использован в статьях [5, 6].

Выводы

В результате проведенного исследования был разработан программный комплекс, предназначенный для решения актуальных задач в области стеганографии и хаотических преобразований. Основное внимание уделено созданию гибкого и удобного инструмента для работы с хаотическими картами, которые обладают высокой эффективностью при построении стегосистем. Реализованные алгоритмы включают такие преобразования, как Карта Арнольда, Карта Бейкера, ДНК-преобразования и синусоидальные карты, что позволяет комплексно подойти к процессу кодирования, декодирования и анализа скрытых данных.

Особенностью данного комплекса является интуитивно понятный пользовательский интерфейс, который предоставляет возможность как начинающим исследователям, так и опытным специалистам эффективно работать с различными методами хаотических преобразований. Гибкость интерфейса позволяет адаптировать программу под конкретные исследовательские задачи, включая подбор параметров преобразований, настройку метрик и тестирование моделей стегосистем.

Кроме того, в программный комплекс интегрированы инструменты для оценки характеристик стегосистем на основе таких метрик, как NPCR, UACI, корреляция соседних пикселей и энтропия. Эти метрики предоставляют возможность детального анализа устойчивости и качества скрытых данных, что является важным аспектом при разработке современных стеганографических методов.

Практическая значимость данного исследования заключается в том, что разработанный программный комплекс может использоваться как для научных исследований, так и для образовательных целей. Программа предоставляет исследователям инструмент для углубленного изучения процессов скрытой передачи данных, а также платформу для тестирования новых идей и алгоритмов.

В дальнейшем возможна доработка программного комплекса за счет расширения функционала. Например, интеграция дополнительных хаотических карт, улучшение визуализации результатов анализа, а также добавление новых метрик, направленных на оценку устойчивости к различным видам атак. Это позволит значительно увеличить потенциал комплекса и расширить его сферу применения.

Таким образом, предложенный программный комплекс является ценным вкладом в развитие методов скрытой передачи данных, предоставляя исследователям мощный инструмент для анализа, разработки и тестирования стеганографических систем на основе хаотических преобразований.

ЛИТЕРАТУРА

1. Ван Х., Ван Ю., Чжу Х., Ло С.: Новый хаотический алгоритм шифрования изображений с использованием одноразового ввода, основанный на уровне пикселей и уровне днк. Оптика и лазеры в технике 125, 105851 (2020). https://doi.org/10.1016/j.optlaseng.2019.105851 (10)
2. Головков Е.В. Арнольд, Бейкер, ДНК и хаотический синус — идеальный квартет для шифрования данных в 5G приложениях Интернета вещей / Е.В. Головков, А.И. Грохотов, В.Н. Кустов // Анализ и синтез в современной науке: сборник статей международной научной конференции, Кингисепп, 20 сентября 2023 года. — Санкт-Петербург: Частное научно-образовательное учреждение дополнительного профессионального образования Гуманитарный национальный исследовательский институт «НАЦРАЗВИТИЕ», 2023. — С. 34–50. — DOI 10.37539/230920.2023.23.40.003. — EDN NSYLQM.
3. Кустов В.Н. Программная модель маскировки скрытого сообщения в задачах стеганографии / В.Н. Кустов, А.И. Грохотов, Е.В. Головков // Интеллектуальные технологии на транспорте. — 2022. — № 1(29). — С. 45–57. — DOI 10.24412/2413–2527-2022-129-45-57. — EDN NAVAQO.
4. Головков Е.В. Гиперхаос HACS, Кнут и Дюрстенфельд обеспечивают гиперстойкость шифрования цветных изображений / Е.В. Головков, А.И. Грохотов, В.Н. Кустов // Анализ и синтез в современной науке: сборник статей международной научной конференции, Кингисепп, 20 сентября 2023 года. — Санкт-Петербург: Частное научно-образовательное учреждение дополнительного профессионального образования Гуманитарный национальный исследовательский институт «НАЦРАЗВИТИЕ», 2023. — С. 51–62. — DOI 10.37539/230920.2023.31.72.004. — EDN LLYLDM.
5. Кустов В.Н. Имитационная программная модель ⊕HUGO стегосистемы / В.Н. Кустов, А.И. Грохотов, Е.В. Головков // Интеллектуальные технологии на транспорте. — 2021. — № 4(28). — С. 46–56. — DOI 10.24412/2413–2527-2021-428-46-56. — EDN REUUZA.
6. Kustov V.N. A Simulation Software Model of the ⊕HUGO Stegosystem / V.N. Kustov, A.I. Grokhotov, E.V. Golovkov // Интеллектуальные технологии на транспорте. — 2022. — No. 3(31). — P. 25–36. — DOI 10.24412/2413–2527-2022-331-25-36. — EDN WUWLPL.

Журнал «Современная наука: актуальные проблемы теории и практики»