

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ/METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.60797/IRJ.2026.168.86 EDN: OMOLBD

АССОЦИАТИВНАЯ СТЕГАНОГРАФИЯ В КОНТЕКСТЕ СОВРЕМЕННЫХ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Обзор

Гибадуллин Р.Ф.[1, *]

[1] ORCID : 0000-0001-9359-911X;

[1] Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань, Российская Федерация

* Корреспондирующий автор (landwatersun[at]mail.ru)

Предложена: 06.03.2026; Принята: 24.04.2026; Опубликована: 17.06.2026

Аннотация

Ассоциативная стеганография объединяет принципы стеганографии и криптографии для обеспечения безопасности информации в процессе анализа сцен. В отличие от традиционных методов стеганографического преобразования, ассоциативный подход обеспечивает практически абсолютную стеганографическую стойкость, доказуемую криптостойкость и более высокую помехозащищенность при хранении и передаче информации по незащищенным каналам связи по сравнению с известными криптографическими методами. В статье рассматриваются достигнутые результаты в направлении ассоциативной стеганографии, включая разработку параллельных систем управления защищенными картографическими базами данных, механизмы формирования стегоконтейнеров и подходы к защите текстовых сведений. Особое внимание уделяется возможностям применения ассоциативного подхода в параллельных СУБД для защиты результатов обработки клиентских запросов, а также перспективам использования стегоконтейнеров в качестве альтернативы шумоподобным изображениям при встраивании цифровых водяных знаков. Обсуждаются направления дальнейшего развития ассоциативной стеганографии в условиях растущих требований к информационной безопасности.

Ключевые слова: ассоциативная стеганография, криптография, защита информации, криптостойкость, помехозащищенность, система управления базами данных, параллельная обработка.

ASSOCIATIVE STEGANOGRAPHY IN THE CONTEXT OF MODERN INFORMATION SECURITY CHALLENGES

Review article

Gibadullin R.F.[1, *]

[1] ORCID : 0000-0001-9359-911X;

[1] Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan, Russian Federation

* Corresponding author (landwatersun[at]mail.ru)

Suggested: 06.03.2026; Accepted: 24.04.2026; Published: 17.06.2026

Abstract

Associative steganography combines the principles of steganography and cryptography to ensure information security during scene analysis. Unlike traditional methods of steganographic transformation, the associative approach provides virtually absolute steganographic strength, provable cryptographic strength and greater jamming resistance during the storage and transmission of information over unsecured communication channels compared to known cryptographic methods. The article examines the results achieved in the field of associative steganography, including the development of parallel management systems for secure cartographic databases, mechanisms for generating stegocontainers, and approaches to protecting textual data. Particular attention is paid to the possibilities of applying the associative approach in parallel DBMSs to protect the results of client query processing, as well as the prospects for using stegocontainers as an alternative to noise-like images when embedding digital watermarks. Directions for the further development of associative steganography in the context of growing information security requirements are discussed.

Keywords: associative steganography, cryptography, information security, cryptographic strength, jamming resistance, database management system, parallel processing.

Введение

Стеганография, наука о скрытом внедрении информации в носители данных таким образом, чтобы сам факт внедрения оставался незаметным, в последние годы привлекает всё большее внимание специалистов в области защиты информации. Особенно актуален подход, известный как ассоциативная стеганография, который по своей природе фокусируется на анализе и обработке изображений сцен.

В современном мире данные являются одним из самых ценных активов как для индивидуальных пользователей, так и для организаций. С увеличением объемов данных и их значимости возрастает и потребность в их защите. Задача

обеспечения информационной безопасности цифровых сведений является критически важной для предотвращения несанкционированного доступа или кражи.

Среди традиционных методов защиты цифровых данных широко применяются симметричные алгоритмы шифрования (AES, ГОСТ 34.12-2018) [1], [2], которые делают содержимое нечитаемым без секретного ключа. Однако их существенным недостатком является неспособность самостоятельно корректировать ошибки, возникающие в процессе передачи или хранения зашифрованных данных. В случае появления таких ошибок зашифрованный текст может быть искажен, что после дешифрования приведет к получению поврежденных и нечитаемых данных.

Асимметричные алгоритмы шифрования (RSA, ECC) [3], [4] обеспечивают конфиденциальность информации путем использования пары ключей — открытого и закрытого. Помимо отсутствия встроенных механизмов коррекции ошибок, они характеризуются относительно низкой скоростью шифрования и расшифрования, что обусловлено более высокой вычислительной сложностью алгоритмов, использующих длинные ключи и сложные математические операции. Для обеспечения помехоустойчивости и улучшения производительности часто используются гибридные системы, сочетающие асимметричные и симметричные алгоритмы.

От указанных недостатков в некоторой степени свободны стеганографические подходы защиты цифровых данных. В настоящее время большое распространение получили алгоритмы Jsteg, Outguess и F5, которые используются для погружения скрытой информации в неподвижные изображения [5], [6]. Jsteg вкладывает информацию в наименьшие значащие биты (НЗБ) частотных коэффициентов цветных изображений в формате JPEG. Outguess также использует НЗБ частотных коэффициентов, однако для повышения стойкости к стегоанализу выполняет повторное вложение с целью приближения гистограммы покрывающих сообщений к гистограмме стегосистемы. F5 при вложении минимизирует количество изменяемых коэффициентов, что затрудняет использование простейших методов стегоанализа.

Существуют и более сложные стегосистемы, такие как "Model based" [7] и "Perturbed Stegosystem» [8], которые оказываются трудно обнаруживаемыми. Идея построения "Model based" состоит в том, что статистика НЗБ частотных коэффициентов изображения после вложения «подгоняется» под статистику этих же НЗБ покрывающих сообщений по аналитической модели. В случае "Perturbed Stegosystem" используется факт двойного квантования с ухудшением качества и вложение в определенные коэффициенты. Однако общим недостатком перечисленных стегосистем является их неустойчивость к так называемому «слепому» стегоанализу, когда не требуется точного знания алгоритмов погружения скрытой информации в покрывающее сообщение. Кроме того, при последовательном внедрении изменения могут скапливаться в начале файла, что увеличивает уязвимость к атакам, а полное использование всей стеганографической емкости делает методы более медленными.

В противовес указанным подходам, ассоциативная стеганография ориентируется на защиту данных, когда анализируется содержание изображений в терминах «объекты — координаты». Этот метод рассматривает изображения как наборы данных, структурированных в виде таблицы, где каждый объект и его координаты кодируются в определенный формат: используется k-разрядное десятичное кодирование почтовыми символами.

Теория и практика ассоциативной стеганографии подробно представлены в работе [9]. В ней изложены принципы создания стеганографических контейнеров, которые обеспечивают высокую степень стегостойкости и помехоустойчивости. Особое внимание в этих методах уделяется процессам генерации масок (процедурам маскирования), которые обеспечивают сохранение существенных битов данных для их последующей идентификации.

На базе ассоциативного подхода защиты были разработаны системы управления защищенными картографическими базами данных, о которых речь пойдет далее. Вполне закономерен вопрос — почему именно картографических? Дело в том, что из-за избыточного объема передаваемых стегосообщений применение предлагаемого способа к текстам значительных размеров технически затруднительно. Например, если для сокрытия 1 байта размер контейнера задать равным 936 бит, то объем исходных данных возрастет в 117 раз. В тематической картографии ситуация иная. Данные на таких картах не столь объемны, поэтому использование предлагаемого подхода не вызывает «подавляющих» технических трудностей. И тем не менее ассоциативный подход защиты применим в любой предметной области, такая адаптация стала еще более возможной благодаря разработанному декоратору StegoStream [10], который обеспечивает взаимодействие с адаптерами потоков и потоками с опорными хранилищами.

Несмотря на значительный объем накопленных результатов в направлении ассоциативной стеганографии, до настоящего времени в научной литературе отсутствует систематический обзор, который бы консолидировал достигнутые результаты, выявил взаимосвязи между отдельными разработками и определил перспективные направления дальнейших исследований. Имеющиеся публикации носят узкоспециализированный характер и посвящены отдельным аспектам метода: формированию стегоконтейнеров, распознаванию маскированных бинарных матриц, построению защищенных картографических баз данных. При этом целостное представление о текущем состоянии и потенциале ассоциативного подхода в контексте современных задач информационной безопасности не было сформировано.

Актуальность настоящего обзора обусловлена рядом факторов. Во-первых, в условиях постоянно усиливающихся киберугроз и роста объемов обрабатываемых данных возрастает потребность в методах защиты, сочетающих криптографическую стойкость с помехозащищенностью и стеганографической скрытностью. Во-вторых, развитие параллельных вычислительных архитектур и высокопроизводительных систем управления базами данных открывает новые возможности для практического применения ассоциативного подхода, которые ранее были ограничены избыточным объемом стегоконтейнеров. В-третьих, появление новых программных инструментов, таких как декоратор StegoStream [10], существенно расширяет область применения метода за пределы тематической картографии.

Основной целью данной статьи является обзор достигнутых результатов в направлении ассоциативной стеганографии и раскрытие перспектив её дальнейшего развития. В статье систематизированы ключевые разработки,

включая параллельные системы управления защищенными картографическими базами данных, механизмы формирования стегоконтейнеров и подходы к защите текстовых сведений, а также обозначены направления, представляющие наибольший интерес для дальнейших исследований.

Параллельная система управления защищенными картографическими базами данных точечных объектов

Security Map-Point Cluster — это параллельная система управления защищенными картографическими базами данных, ограниченная случаем защиты точечных картографических объектов [9]. Данная система обеспечивает формирование защищенной базы данных (кластеризация, генерация ключей, поиск подходящего контейнера и др.), обработку запросов к БД, распознавание бинарных изображений. Рассмотрим принцип формирования БД картографии на вычислительном кластере для защищенного хранения точечных объектов картографии.

В соответствии с принципами кластеризации строится база данных, состоящая из трех сущностей: Themes (Темы), Frames (Фрагменты), Objects (Объекты). Диаграмма «сущность-связь» этой базы данных дана на рисунке 1.

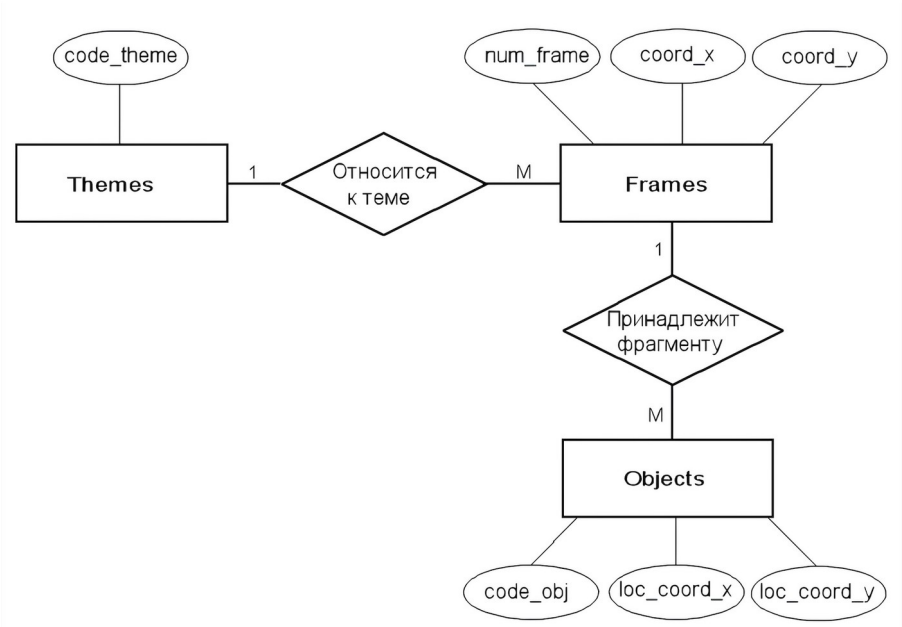

Рисунок 1 - Диаграмма «сущность-связь» картографической БД
DOI: https://doi.org/10.60797/IRJ.2026.168.86.1

Характеристики атрибутов таблиц даны ниже.

Themes [Темы слоев карт] (id_theme [Идентификатор темы]: integer, code_theme [Код темы]: text);

Frames [Фрагменты карт] (st [Счетчик-идентификатор]: integer, id_theme [Идентификатор темы]: integer, num_frame [Номер фрагмента]: integer, coord_x [Координата x фрагмента]: text, coord_y [Координата y фрагмента]: text);

Objects [Объекты] (st [Счетчик-идентификатор]: integer, id_theme [Идентификатор темы]: integer, num_frame [Номер фрагмента]: integer, code_obj [Код объекта]: text, loc_coord_x [Координата x объекта во фрагменте]: text, loc_coord_y [Координата y объекта во фрагменте]: text).

При сокрытии базы данных все значения в столбцах code_theme, coord_x, coord_y, code_obj, loc_coord_x, loc_coord_y заменяются соответствующими стегоконтейнерами.

Сокрытие картографической базы данных ведется параллельно на узлах вычислительного кластера. Для распараллеливания программ по узлам кластера применяется библиотека передачи сообщений MPICH-1.

Инфологическая схема базы данных полнообъектных картографических сцен

Существует множество проектов универсальных СУБД, способных хранить данные любого типа (в том числе и конфиденциальные). Специфика работы с данными полнообъектных картографических сцен, которые подвергаются маскированию, требует их хранения в базе данных специальной структуры. Для разрабатываемой специализированной системы управления Security Map Cluster [11] описание сущностей создаваемой базы данных и связей между ними может быть представлено инфологической ER-диаграммой (рис. 2).

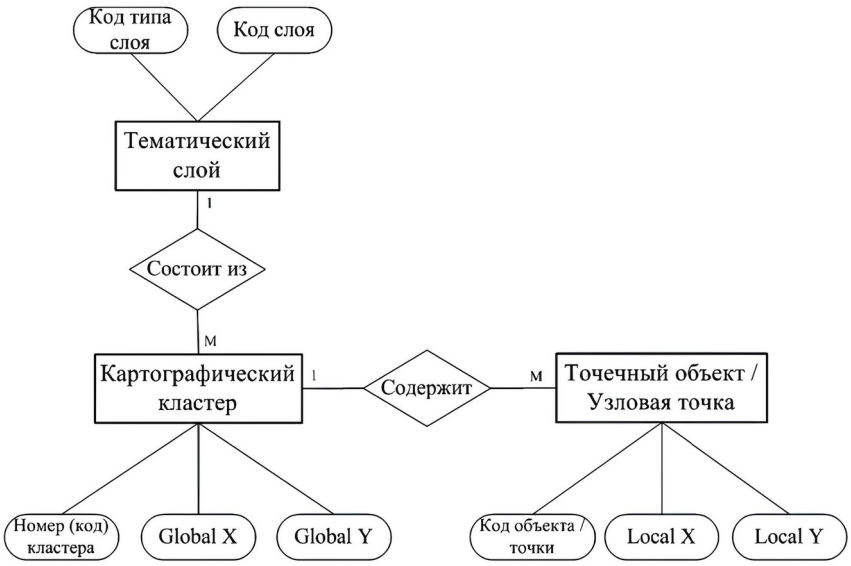

Рисунок 2 - ER-диаграмма базы данных
DOI: https://doi.org/10.60797/IRJ.2026.168.86.2

Однако особенности представления картографической сцены, единообразный формат хранения для всех типов объектов и необходимость хранения данных в сокрытом виде не позволяют сформировать схему базы данных как реляционную с наличием связей между отношениями по атрибутам. Хранение информации обо всех объектах картографической сцены в едином табличном отношении (вне зависимости от типа) приведет к необходимости поиска в этом отношении по двойному ключу (Код слоя — Код кластера). Такой поиск может повлечь большие временные задержки, так как все поля в базе данных маскируются. Поэтому предлагается следующая инфологическая схема базы данных полнообъектных картографических сцен БД ПКС (рис. 3).

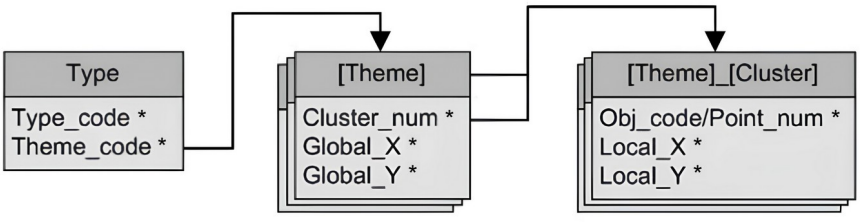

Рисунок 3 - Предлагаемая инфологическая схема БД ПКС
DOI: https://doi.org/10.60797/IRJ.2026.168.86.3

Здесь: Type — отношение, содержащее информацию обо всех тематических слоях сцены, представленных парой сокрытых кодов: Код типа — Код слоя. [Theme] – набор отношений, каждое из которых описывает отдельный тематический слой (кластеры-фрагменты внутри слоя). Название отношения есть открытый код этого слоя. [Theme]_[Cluster] — набор отношений, каждое из которых описывает содержимое (объекты) одного кластера (фрагмента) какого-либо тематического слоя. Название отношения составное, содержит открытый код слоя и код кластера. Связи между таблицами формируются по принципу «Атрибут М табл.А» –> «Табл.В». Например, необходимый для работы набор таблиц типа [Theme]_[Cluster] определяется на основе найденных в таблице [Theme] кодов, подходящих условию запроса фрагментов.

Перспективы применения ассоциативной стеганографии

Благодаря своей универсальности ассоциативная стеганография может применяться в различных прикладных областях. В свете современных вызовов в области информационной безопасности и растущего объема обрабатываемых данных, важность интеграции стеганографической защиты в программные продукты усиливается. Ассоциативный подход к защите данных отличается от традиционных (криптографических) методов, предлагая высокую стойкость к атакам и повышенную помехозащищенность при хранении и передаче информации по незащищенным каналам.

В работе [12] предложен подход к защите текстовых сведений, в котором основное внимание уделяется защите числовых фрагментов текста, выделяемых посредством регулярного выражения [13].

В качестве перспектив развития ассоциативной стеганографии целесообразно применение данного подхода в целях защиты данных в параллельных СУБД, при этом внимание акцентируется не на защите хранимой базы данных, а на результирующих отношениях (ответах на клиентские запросы), передаваемых конечным пользователям. Для защиты передаваемых результатов обработки запросов по сети предлагается использовать разработанные функции udf_cipher и udf_decipher [3] (рис. 4). Также возможен вариант обеспечения прозрачного шифрования передаваемого трафика с применением программного стегошлюза (рис. 5).

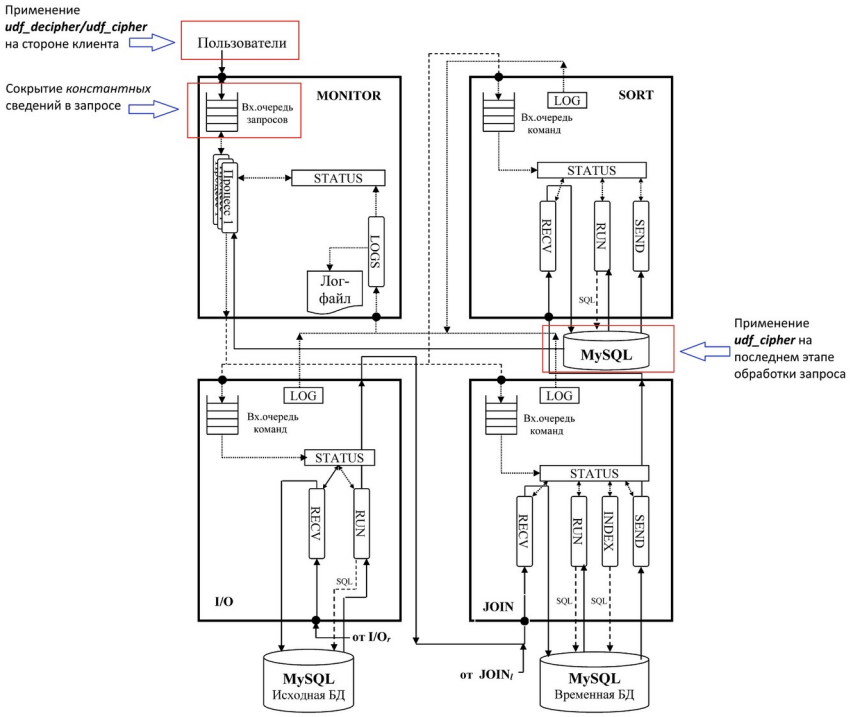

Рисунок 4 - Потенциальные участки воздействия механизма ассоциативной стеганографии на примере типовой архитектуры параллельной СУБД

DOI: https://doi.org/10.60797/IRJ.2026.168.86.4

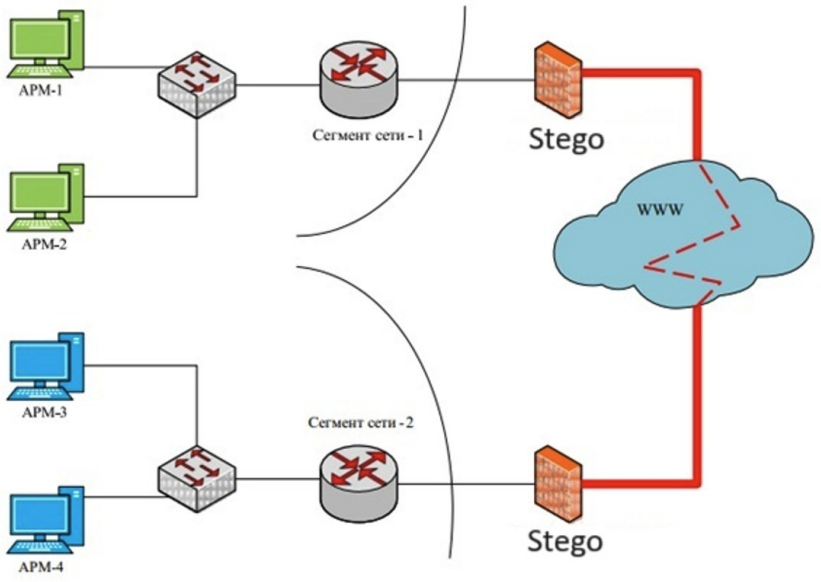

Рисунок 5 - Применение ассоциативного механизма защиты в качестве криптошлюза
DOI: https://doi.org/10.60797/IRJ.2026.168.86.5

В работе [14] цифровые водяные знаки (ЦВЗ) встраиваются в виде шумоподобных изображений. В качестве контейнера для встраивания ЦВЗ используется множество объектов полигонального типа. Каждый полигон представляет собой замкнутый объект (многоугольник), который может быть однозначно определен списком координат последовательно пронумерованных вершин (рис. 6). Таким образом, циклический сдвиг списка вершин полигона не повлияет на значения их координат. Эта идея есть суть предлагаемого подхода к встраиванию ЦВЗ без внесения искажений в координатную информацию. В качестве ЦВЗ используется растровое изображение, наложенное на выбранный фрагмент векторного слоя путем разбиения карты на прямоугольные ячейки и отображения полученного разбиения на сетку пикселей растра.

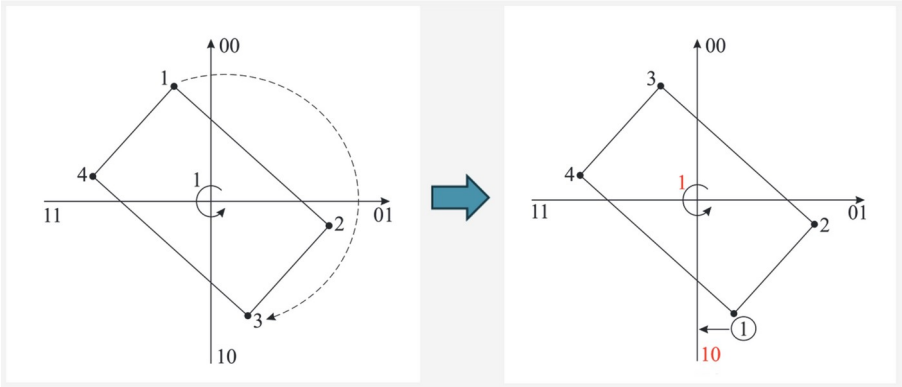

Рисунок 6 - Пример встраивания трех бит информации в полигональный объект
DOI: https://doi.org/10.60797/IRJ.2026.168.86.6

Примечание: источник [14]

Использование стегоконтейнеров вместо шумоподобных изображений:
– потенциально обеспечит дополнительный уровень защиты передаваемой информации;
– стегоконтейнеры могут быть адаптированы к изменениям в структуре векторных данных без потери встроенной информации.

Заключение

В настоящей статье представлен обзор достигнутых результатов и перспектив развития ассоциативной стеганографии — подхода, объединяющего принципы стеганографии и криптографии для обеспечения безопасности информации при анализе сцен.

Показано, что в отличие от традиционных криптографических методов (симметричных и асимметричных алгоритмов шифрования), а также известных стеганографических алгоритмов (Jsteg, Outguess, F5, Model based, Perturbed Stegosystem), ассоциативный подход обеспечивает практически абсолютную стеганографическую стойкость,

доказуемую криптостойкость и более высокую помехозащищенность при хранении и передаче информации по незащищенным каналам связи.

Рассмотрены две параллельные системы управления защищенными картографическими базами данных. Система Security Map-Point Cluster обеспечивает защищенное хранение точечных картографических объектов с использованием кластеризации и параллельной обработки на вычислительных узлах посредством библиотеки MPICH-1. Система Security Map Cluster расширяет данный подход на полнообъектные картографические сцены, для чего предложена инфологическая схема базы данных, позволяющая избежать поиска по двойному ключу в маскированных полях и обеспечивающая эффективную обработку запросов.

Обозначены ключевые перспективы дальнейшего развития ассоциативной стеганографии. Во-первых, применение ассоциативного подхода в параллельных СУБД для защиты не хранимых данных, а результирующих отношений (ответов на клиентские запросы), передаваемых конечным пользователям, с использованием разработанных функций udf_cipher и udf_decipher, а также программного стегошлюза для обеспечения прозрачного шифрования передаваемого трафика. Во-вторых, использование стегоконтейнеров в качестве альтернативы шумоподобным изображениям при встраивании цифровых водяных знаков в полигональные объекты векторных карт, что потенциально обеспечит дополнительный уровень защиты и адаптивность к изменениям в структуре данных. В-третьих, расширение области применения метода за пределы тематической картографии благодаря разработанному декоратору StegoStream.

Таким образом, дальнейшие исследования и разработки в области ассоциативной стеганографии остаются актуальными и многообещающими, потенциально позволяя значительно повысить уровень защиты информационных систем в условиях постоянно усиливающихся киберугроз и растущих требований к конфиденциальности, целостности и доступности данных.

Финансирование

Работа выполнена за счет гранта, предоставленного Академией наук Республики Татарстан образовательным организациям высшего образования, научным и иным организациям на поддержку планов развития кадрового потенциала в части стимулирования их научных и научно-педагогических работников к защите докторских диссертаций и выполнению научно-исследовательских работ (Соглашение №15/2025-ПД-КАИ от 22.12.2025).

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Funding

This work/publication was funded by a grant from the Academy of Sciences of the Republic of Tatarstan provided to higher education institutions, scientific and other organizations to support human resource development plans in terms of encouraging their research and academic staff to defend doctoral dissertations and conduct research activities (Agreement № 15/2025-PD-KAI dated December 22, 2025).

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Юсупов А.И. Эффективные методы шифрования для защиты данных в облачных хранилищах / А.И. Юсупов // Проблемы развития современного общества : сборник научных статей 10-й Всероссийской национальной научно-практической конференции— Курск : Университетская книга, 2025. — С. 442–445.

2. Шаханова М.В. Защита конфиденциальных сведений от несанкционированного доступа / М.В. Шаханова, Е.Е. Швец, Э.С. Шаханова // Международный журнал информационных технологий и энергоэффективности. — 2025. — Т. 10. — № 2 (52). — С. 166–171.

3. Семыкина Н.А. Защита графической информации от несанкционированного доступа / Н.А. Семыкина, А.В. Петрова // Безопасность. Управление. Искусственный интеллект. — 2025. — Т. 1. — № 1 (1). — С. 10–16.

4. Юсупова С.А. Основные аспекты шифрования информации / С.А. Юсупова, Р.Р. Шарипов, Р.Р. Халиулин // Цифровые системы и модели: теория и практика проектирования, разработки и использования : материалы международной научно-практической конференции. — Казань : Казанский государственный энергетический университет, 2025. — С. 2388–2390.

5. Сидоренко В.Г. Противодействие угрозам информационной безопасности, связанным с применением средств стеганографии / В.Г. Сидоренко, Я.Л. Грачев // Автоматика, связь, информатика. — 2025. — № 1. — С. 17–22. — DOI: 10.62994/AT.2025.1.1.004.

6. Белим С.В. Модель стеганографического встраивания в файлы с иерархической структурой / С.В. Белим, С.Н. Мунько, С.Ю. Белим // Прикладная информатика. — 2025. — Т. 20. — № 1 (115). — С. 125–139. — DOI: 10.37791/2687-0649-2025-20-1-125-139.

7. Самандаров Б.С. Анализ и моделирование уязвимостей безопасности информационных систем / Б.С. Самандаров, Г.А. Гулмирзаева, Д.Р. Жолдасбаев // Информатика. Экономика. Управление. — 2025. — Т. 4. — № 1. — С. 2019–2026. — DOI: 10.47813/2782-5280-2025-4-1-2019-2026.

8. Авсентьев О.С. Функциональная модель процесса реализации угроз безопасности информации с использованием скрытых стеганографических каналов внешним нарушителем / О.С. Авсентьев, В.В. Бутов, К.А.

Цыганов // Безопасность информационных технологий. — 2025. — Т. 32. — № 2. — С. 83–101. — DOI: 10.26583/bit.2025.2.07.

9. Райхлин В.А. Элементы содержательной теории ассоциативной стеганографии / В.А. Райхлин, И.С. Вершинин, Р.Ф. Гибадуллин // Вестник Московского университета. Серия 15: Вычислительная математика и кибернетика. — 2019. — № 1. — С. 41–47.

10. Гибадуллин Р.Ф. Разработка декоратора StegoStream для ассоциативной защиты байтового потока / Р.Ф. Гибадуллин, Д.А. Гашигуллин, И.С. Вершинин // Моделирование, оптимизация и информационные технологии. — 2023. — Т. 11. — № 2 (41). — С. 22–23.

11. Пыстогов С.В. СУБД полнообъектных картографических сцен с ассоциативной защитой на кластерной платформе : дис. … канд. техн. наук : 05.13.11 / С.В. Пыстогов. — 2019. — 144 с.

12. Гибадуллин Р.Ф. Ассоциативная защита числовых сведений в текстовых документах с применением библиотеки Parallel Framework платформы .NET / Р.Ф. Гибадуллин, И.С. Вершинин // Computational Nanotechnology. — 2023. — Т. 10. — № 3. — С. 121–129.

13. Abu Hawas F. Fast Regular Expression Matching in a Large Static Text / F. Abu Hawas, A.N. Arslan // 2016 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA. — 2016. — P. 1304–1309.

14. Выборнова Ю.Д. Метод защиты авторских прав на векторные картографические данные / Ю.Д. Выборнова, В.В. Сергеев // Информатика и автоматизация. — 2021. — Т. 20. — № 1. — С. 181–212.

Список литературы на английском языке / References in English

1. Yusupov A.I. Effektivnye metody shifrovaniya dlya zashchity dannykh v oblachnykh khranilishchakh [Effective encryption methods for data protection in cloud storage] / A.I. Yusupov // Problemy razvitiya sovremennogo obshchestva [Problems of development of modern society] : collection of scientific articles of the 10th All-Russian National Scientific and Practical Conference. — Kursk : University Book, 2025. — P. 442–445. [in Russian]

2. Shakhanova M.V. Zashchita konfidencial'nykh svedenij ot nesankcionirovannogo dostupa [Protecting confidential information from unauthorized access] / M.V. Shakhanova, E.E. Shvets, E.S. Shakhanova // Mezhdunarodnyj zhurnal informacionnykh tekhnologij i energoehffektivnosti [International Journal of Information Technologies and Energy Efficiency]. — 2025. — Vol. 10. — № 2 (52). — P. 166–171. [in Russian]

3. Semykina N.A. Zashchita graficheskoj informacii ot nesankcionirovannogo dostupa [Protection of graphic information from unauthorized access] / N.A. Semykina, A.V. Petrova // Bezopasnost'. Upravlenie. Iskusstvennyj intellekt [Security. Management. Artificial Intelligence]. — 2025. — Vol. 1. — № 1 (1). — P. 10–16. [in Russian]

4. Yusupova S.A. Osnovnye aspekty shifrovaniya informacii [The main aspects of information encryption] / S.A. Yusupova, R.R. Sharipov, R.R. Khaliulin // Cifrovye sistemy i modeli: teoriya i praktika proektirovaniya, razrabotki i ispol'zovaniya [Digital systems and models: theory and practice of design, development and use] : proceedings of the International Scientific and Practical Conference. — Kazan : Kazan State Power Engineering University, 2025. — P. 2388–2390. [in Russian]

5. Sidorenko V.G. Protivodejstvie ugrozam informacionnoj bezopasnosti, svyazannym s primeneniem sredstv steganografii [Countering information security threats associated with the use of steganography tools] / V.G. Sidorenko, Ya.L. Grachev // Avtomatika, svyaz', informatika [Automation, Communications, Informatics]. — 2025. — № 1. — P. 17–22. — DOI: 10.62994/AT.2025.1.1.004. [in Russian]

6. Belim S.V. Model' steganograficheskogo vstraivaniya v fajly s ierarkhicheskoj strukturoj [Steganographic embedding model in files with hierarchical structure] / S.V. Belim, S.N. Munko, S.Yu. Belim // Prikladnaya informatika [Journal of Applied Informatics]. — 2025. — Vol. 20. — № 1 (115). — P. 125–139. — DOI: 10.37791/2687-0649-2025-20-1-125-139. [in Russian]

7. Samandarov B.S. Analiz i modelirovanie uyazvimostej bezopasnosti informacionnykh sistem [Analysis and modeling of information system security vulnerabilities] / B.S. Samandarov, G.A. Gulmirzaeva, D.R. Zholdasbaev // Informatika. Ekonomika. Upravlenie [Informatics. Economics. Management]. — 2025. — Vol. 4. — № 1. — P. 2019–2026. — DOI: 10.47813/2782-5280-2025-4-1-2019-2026. [in Russian]

8. Avsentiev O.S. Funkcional'naya model' processa realizacii ugroz bezopasnosti informacii s ispol'zovaniem skrytykh steganograficheskikh kanalov vneshnim narushitelem [Functional model of the process of information security threats implementation using covert steganographic channels by an external intruder] / O.S. Avsentiev, V.V. Butov, K.A. Tsyganov // Bezopasnost' informacionnykh tekhnologij [IT Security]. — 2025. — Vol. 32. — № 2. — P. 83–101. — DOI: 10.26583/bit.2025.2.07. [in Russian]

9. Raihlin V.A. Elementy soderzhatel'noj teorii associativnoj steganografii [The elements of associative stegnanography theory] / V.A. Raihlin, I.S. Vershinin, R.F. Gibadullin // Vestnik Moskovskogo universiteta. Seriya 15: Vychislitel'naya matematika i kibernetika [Moscow University Bulletin. Series 15: Computational Mathematics and Cybernetics]. — 2019. — № 1. — P. 41–47. [in Russian]

10. Gibadullin R.F. Razrabotka dekoratora StegoStream dlya associativnoj zashchity bajtovogo potoka [Development of StegoStream decorator for associative protection of byte stream] / R.F. Gibadullin, D.A. Gashigullin, I.S. Vershinin // Modelirovanie, optimizaciya i informacionnye tekhnologii [Modeling, Optimization and Information Technologies]. — 2023. — Vol. 11. — № 2 (41). — P. 22–23. [in Russian]

11. Pystogov S.V. SUBD polnoob"ektnykh kartograficheskikh scen s associativnoj zashchitoj na klasternoj platforme [DBMS of full-object cartographic scenes with associative protection on a cluster platform] : dis. … of PhD in Engineering : 05.13.11 / S.V. Pystogov. — 2019. — 144 p. [in Russian]

12. Gibadullin R.F. Associativnaya zashchita chislovykh svedenij v tekstovykh dokumentakh s primeneniem biblioteki Parallel Framework platformy .NET [Associative Protection of Numerical Information in Text Documents Using the Parallel Framework Library on the .NET Platform] / R.F. Gibadullin, I.S. Vershinin // Computational Nanotechnology. — 2023. — Vol. 10. — № 3. — P. 121–129. [in Russian]

13. Abu Hawas F. Fast Regular Expression Matching in a Large Static Text / F. Abu Hawas, A.N. Arslan // 2016 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA. — 2016. — P. 1304–1309.

14. Vybornova Yu.D. Metod zashchity avtorskikh prav na vektornye kartograficheskie dannye [Method for Protection of Copyright on Vector Data] / Yu.D. Vybornova, V.V. Sergeev // Informatika i avtomatizaciya [Informatics and Automation]. — 2021. — Vol. 20. — № 1. — P. 181–212. [in Russian]