

Организация системы управления картографическими базами данных с ассоциативной защитой

И.С. Вершинин

*Казанский национальный исследовательский технический университет
им. А.Н. Туполева–КАИ, Казань, Россия*

Аннотация: Приводится введенное ранее и необходимое для дальнейшего рассмотрения понятие двумерно-ассоциативного механизма маскирования, используемого для защиты данных сцен картографии, реализованных в виде точечных, линейных или площадных объектов. Механизм маскирования положен в основу ассоциативной стеганографии. При этом объекты и координаты сцены представляются кодовыми словами в алфавите почтовых символов и подвергаются маскированию с дальнейшим формированием стегоконтейнеров. Набор масок является секретным ключом, используемым далее для распознавания сцены, представленной в защищенном виде совокупностью стегоконтейнеров. В статье рассматриваются вопросы организации специализированных СУБД для защиты данных картографических сцен с введением двух уровней таких СУБД – серверного и клиентского. Для серверной части СУБД предлагаются моно- и мультикластерная организация обработки запросов. Даются практические рекомендации по применению моно- и мультикластеров.

Ключевые слова: ассоциативная стеганография, маскирование, стегосообщение, картографические базы данных, параллельная СУБД, моно- и мультикластер, анализ сцен, криптография, стегостойкость, информационная безопасность.

Введение

Идея двумерно-ассоциативного картографического шифра является итогом исследований двумерно-ассоциативных механизмов, применяемых для маскирования стилизованных бинарных изображений при действии помех [1, 2]. Установлено, что найденный шифр доказуемо криптостоек, безусловно стегостоек и обладает сравнительно высокой помехоустойчивостью.

Предлагаемый шифр относится к классу вероятностных шифров. Для анализа сцен [3] картографии (сокрытия данных) случайность внедряется путем проведения кластеризации объектов сцен (их отнесение к тому или иному ранее сформированному кластеру либо формирование нового кластера с отнесением объекта-родителя к этому новому кластеру), при этом объект, а также его координаты (x, y) преобразуются в бинарный вид в алфавите

почтовых индексов. Далее к ним применяется процедура маскирования и последующая рандомизация.

После проведения над кодовыми представлениями объектов/координат процедуры маскирования генерируется случайный набор масок, выступающий в роли секретного ключа. Защите подлежит набор кластеров как табличная информация, представленная в виде «коды объектов – коды координат». Кластер «покрывает» участок карты определенных размеров, определяемых по заранее заданным условиям (в том числе погрешностью преобразования координат из глобальных по карте в локальные – в пределах кластера).

Цель статьи – рассмотрение вопросов построения специализированных СУБД сцен картографии с применением ассоциативной защиты на основе вычислительных кластеров. Решаемые задачи – разработка архитектур моно- и мультикластеров и сравнительная оценка их быстродействия с выработкой соответствующих практических рекомендаций.

Принципы построения СУБД

Как известно, в геоинформационных системах [4, 5] слои могут быть представлены тремя типами объектов. К ним относятся точечные (например, условные знаки), линейные (дороги) и площадные (лес, озеро) объекты.

Для формирования БД картографических сцен (КС) с ассоциативной защитой (АЗ) в процессе кластеризации необходимым является выполнение условия о нахождении линейного/площадного объекта в одном кластере. Перед проведением процедуры кластеризации объекты (либо их узловые точки) должны быть соотнесены с узлами координатной сетки. Это необходимо влечет за собой проведение процедуры векторизации с возможным применением специализированного ПО, например [6].

Организация процедур создания баз данных ассоциативных сцен и проведение в них процесса поиска информации в приемлемое время

приводит к необходимости использования параллельных СУБД и вычислительных кластеров.

Далее рассматривается принцип построения указанных параллельных СУБД на платформе вычислительных кластеров. Объемы таких баз данных могут быть значительны [7], что и обуславливает необходимость использования для их обработки вычислительных кластеров.

Рассматриваемая СУБД состоит из двух уровней – серверной и клиентской стороны. На серверном уровне проводится формирование БД и выдача информации (части БД) клиенту, на клиентском уровне – обработка пространственных запросов к полученной информации. Работа системы сводится к генерации запросов клиентом, получение от сервера результата обработки запроса и анализ результатов обработки.

Рассмотрим более подробно организацию серверной части СУБД (как наиболее значимую). Серверная часть представляет собой вычислительный кластер, к которому организуется подключение клиентов. Вычислительный кластер содержит один управляющий узел (УУ) и множество вычислительных узлов (ВУ). В ответ на запрос, клиенту отправляется файл с ответом – набор записей, описывающих точечные объекты или узловые точки (для линейных/площадных объектов), которые удовлетворяют условиям запроса. Дополнительная обработка собранной информации (например, пространственные запросы) выполняется клиентом.

Возможна моно- и мультикластерная организация обработки запросов. В первом режиме обработка запроса осуществляется сразу всеми вычислительными узлами кластера, во втором – только одним из этих узлов.

Отличительная особенность функционирования системы в режиме «мультикластер» заключается в том, что запросы после предобработки и синтаксического анализа на хосте-сервере распределяются по вычислительным узлам кластера согласно схеме «один узел – один запрос».

После обработки запроса на одном из рабочих узлов ответ передается на управляющий узел и далее – клиенту. В рабочий узел из управляющего поступает первоочередной запрос.

Формирование БД происходит в режиме «монокластер» (процессом управляет администратор) и включает в себя:

- Считывание информации об объектах;
- Создание в управляющем узле структуры базы данных;
- Заполнение базы данных на основе параллельной обработки информации об объектах;
- Распределение сгенерированной БД по вычислительным узлам кластера. При этом информация в базе данных подвергается процедуре маскирования. Таким образом получается зашифрованная БД.

Углубленная блок-схема программного модуля создания базы данных приведена на рис. 1.

Закономерным является вопрос, какая архитектура кластера более предпочтительна? Ответ на этот вопрос был дан по результатам проведения соответствующих экспериментальных исследований. Как известно, производительность вычислительного кластера в значительной мере определяется количеством вычислительных узлов. Однако эффективность рассмотренной СУБД на основе вычислительного кластера зависит не только от количества ВУ, но также определяется и архитектурой кластера.

Эксперимент заключался в выполнении совокупности селективных запросов к сформированной базе данных с оценкой среднего времени задержки выполнения одного запроса и общего времени выполнения всей совокупности запросов. По результатам экспериментов было установлено, что при одинаковом количестве вычислительных узлов моно- и мультикластера оба рассмотренных выше параметра примерно на треть

меньше для архитектуры монокластера по сравнению с архитектурой мультикластера.

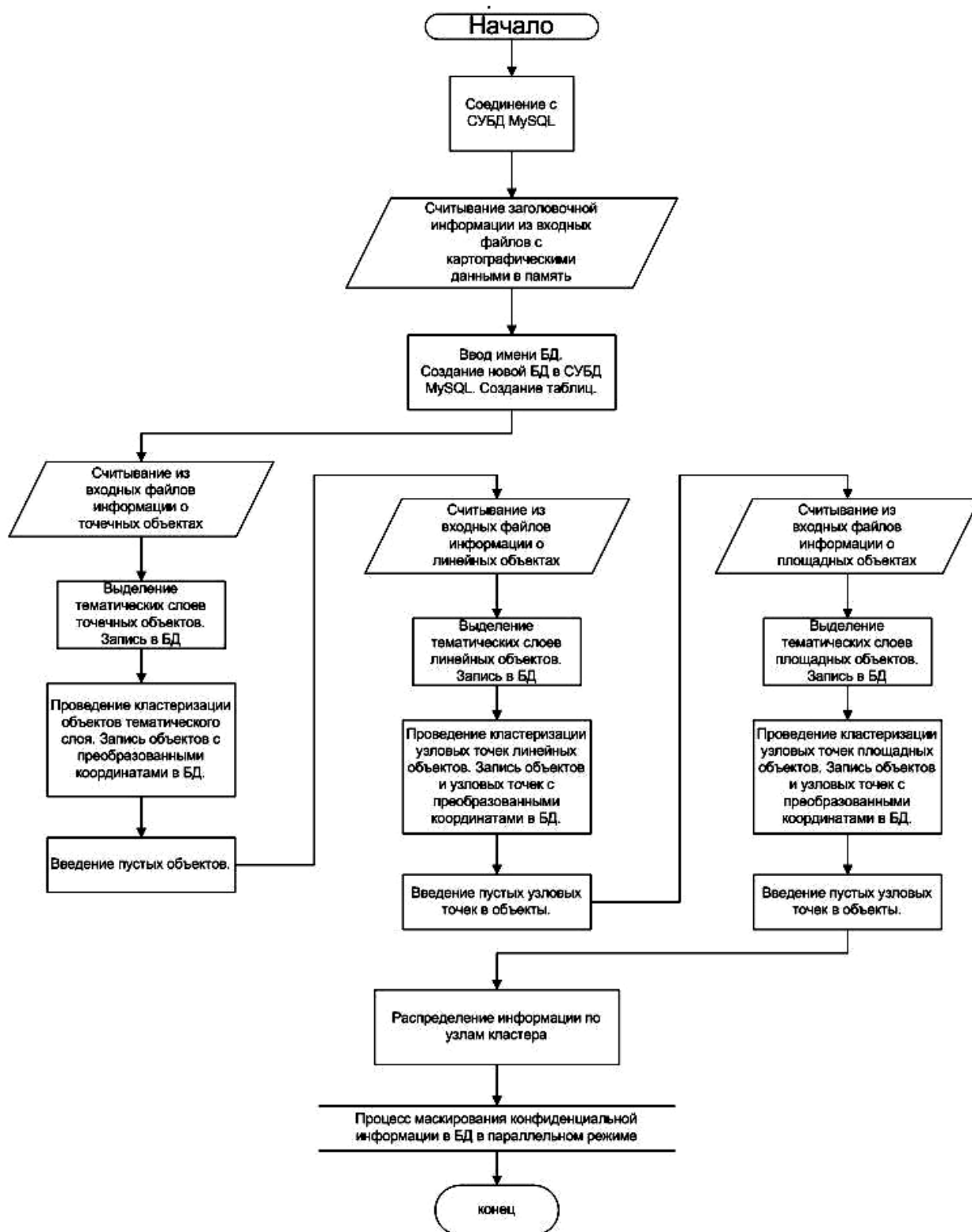


Рис. 1. – Укрупненная блок-схема программного модуля создания БД

Заключение

Полученные по итогам проведенных исследований результаты позволяют дать *однозначную* рекомендацию о необходимости использования на практике именно архитектуры монокластера.

Проведенное выше рассмотрение относилось к созданию СУБД-сцен картографии с применением метода ассоциативной защиты. Однако мыслимы и другие практические приложения. Так, в работе [8] рассматриваются вопросы защиты текстовых данных. Помимо защиты картографических и текстовых данных, актуальным видится применение ассоциативного стеганографического механизма защиты данных в и области защиты интеллектуальной собственности: защита авторских прав, мониторинг нарушений, защита конфиденциальных документов, обеспечение анонимности и т.п. Мыслимо использование метода и для выявления различного рода атак и противодействия им [9, 10].

Использование ассоциативного стеганографического механизма защиты данных в защите интеллектуальной собственности открывает новые горизонты для обеспечения конфиденциальности, сохранности и контроля над распространением произведений интеллектуальной собственности.

Литература

1. Raikhlin V.A., Vershinin I.S., Gibadullin R.F., Pystogov S.V. Reliable Recognition of Masked Binary Matrices. Connection to Information Security in Map Systems // Lobachevskii Journal of Mathematics, 2013. V. 34, №4. pp. 319-325.
2. Raikhlin V.A., Vershinin I.S., Gibadullin R.F. The Elements of Associative Steganography Theory // Moscow University Computational Mathematics and Cybernetics, 2019. V. 43, №1. pp. 40-46.
3. Duda R.O., Hart P.E., Stork D.G. Pattern classification and scene analysis. New York: Wiley, 1973. №3. pp. 731–739.

4. Сяо Н. Алгоритмы ГИС. М: ДМК Пресс, 2021. 328 с.
5. Бабенко Л.К., Басан А.С., Журкин И.Г., Макаревич О.Б. Защита данных геоинформационных систем. М.: Гелиос АРВ, 2010. 336 с.
6. WinTopo Raster to Vector Converter. URL: softsoft.net/wintopo/index.htm
7. Шаши Шекхар, Санжей Чаула. Основы пространственных баз данных / Пер. с англ. – М.: КУДИЦ-ОБРАЗ, 2004. 336 с.
8. Гибадуллин Р.Ф., Вершинин И.С., Глебов Е.Е. Разработка приложения для ассоциативной защиты файлов // Инженерный вестник Дона, 2023, №6. URL: ivdon.ru/ru/magazine/archive/n6y2023/8462/
9. Молдовян Н.А., Молдовян А.А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритмов. СПб.: БХВ-Петербург, 2004. 448 с.
10. Афанасьева Н.С., Елизаров Д.А., Мызникова Т.А. Классификация фишинговых атак и меры противодействия им // Инженерный вестник Дона, 2022, №5. URL: ivdon.ru/ru/magazine/archive/n5y2022/7641/

References

1. Raikhlin V.A., Vershinin I.S., Gibadullin R.F., Pystogov S.V. Lobachevskii Journal of Mathematics, 2013. V. 34, №4. pp. 319-325.
 2. Raikhlin V.A., Vershinin I.S., Gibadullin R.F. Moscow University Computational Mathematics and Cybernetics, 2019. V. 43, №1. pp. 40-46.
 3. Duda R.O., Hart P.E., Stork D.G. Pattern classification and scene analysis. New York: Wiley, 1973. №3. pp. 731–739.
 4. Xiao N. Algoritmy GIS [GIS algorithms]. Moskva: DMK Press, 2021. 328 p.
 5. Babenko L.K., Basan A.S., ZHurkin I.G., Makarevich O.B. Zashchita dannyh geoinformacionnyh sistem [Data protection of geoinformation systems]. Moskva: Gelios ARV, 2010. 336 p.
 6. WinTopo Raster to Vector Converter. URL: softsoft.net/wintopo/index.htm
-

7. Shashi Shekhar, Sanzhej Chaula. Osnovy prostranstvennykh baz dannykh [Fundamentals of spatial databases]. Moscow: KUDICZ-OBRAZ, 2004. 336 p.

8. Gibadullin R.F., Vershinin I.S., Glebov E.E. Inzhenernyj vestnik Dona, 2023, №6. URL: ivdon.ru/ru/magazine/archive/n6y2023/8462/

9. Moldovyan N.A., Moldovyan A.A., Eremeev M.A. Kriptografiya: ot primitivov k sintezu algoritmov [Cryptography: from Primitives to Algorithm Synthesis]. Sankt-Peterburg: BHV-Peterburg. 2004. 448 p.

10. Afanasyeva N.S., Elizarov D.A., Myznikova T.A. Inzhenernyj vestnik Dona, 2022, №5. URL: ivdon.ru/ru/magazine/archive/n5y2022/7641/