В докладе рассматриваются достигнутые нашей научной группой результаты в направлении ассоциативной стеганографии и обсуждаются перспективы дальнейшего развития этого направления.

Состояние и перспективы развития ассоциативной стеганографии

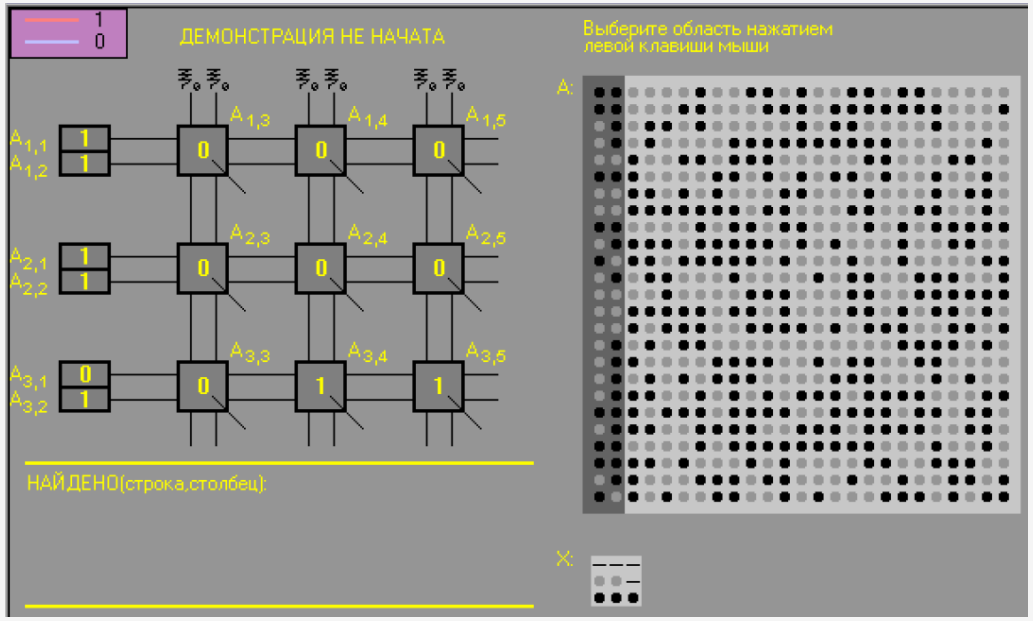
Р.Ф. Гибадуллин

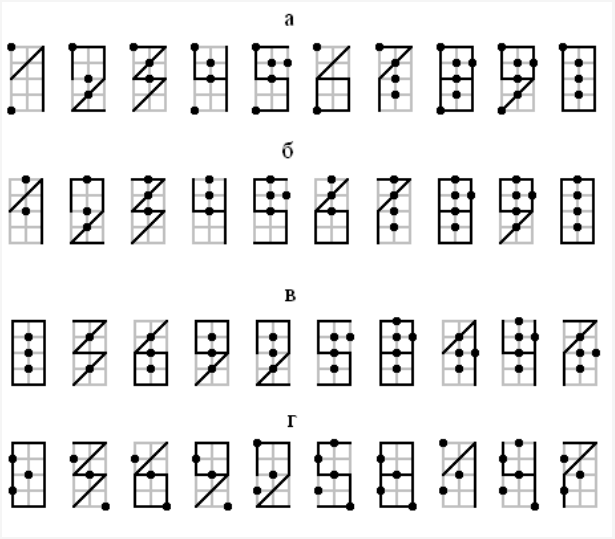
1. Введение

Вершинин И. С.

Моделирование двумерно-ассоциативных механизмов маскирования стилизованных бинарных изображений.

Диссертация на соискание ученой степени кандидата технических наук, 2004.





2. Система Security Map-Point Cluster

Гибадуллин Р. Ф.

Система баз данных картографии с ассоциативной защитой.

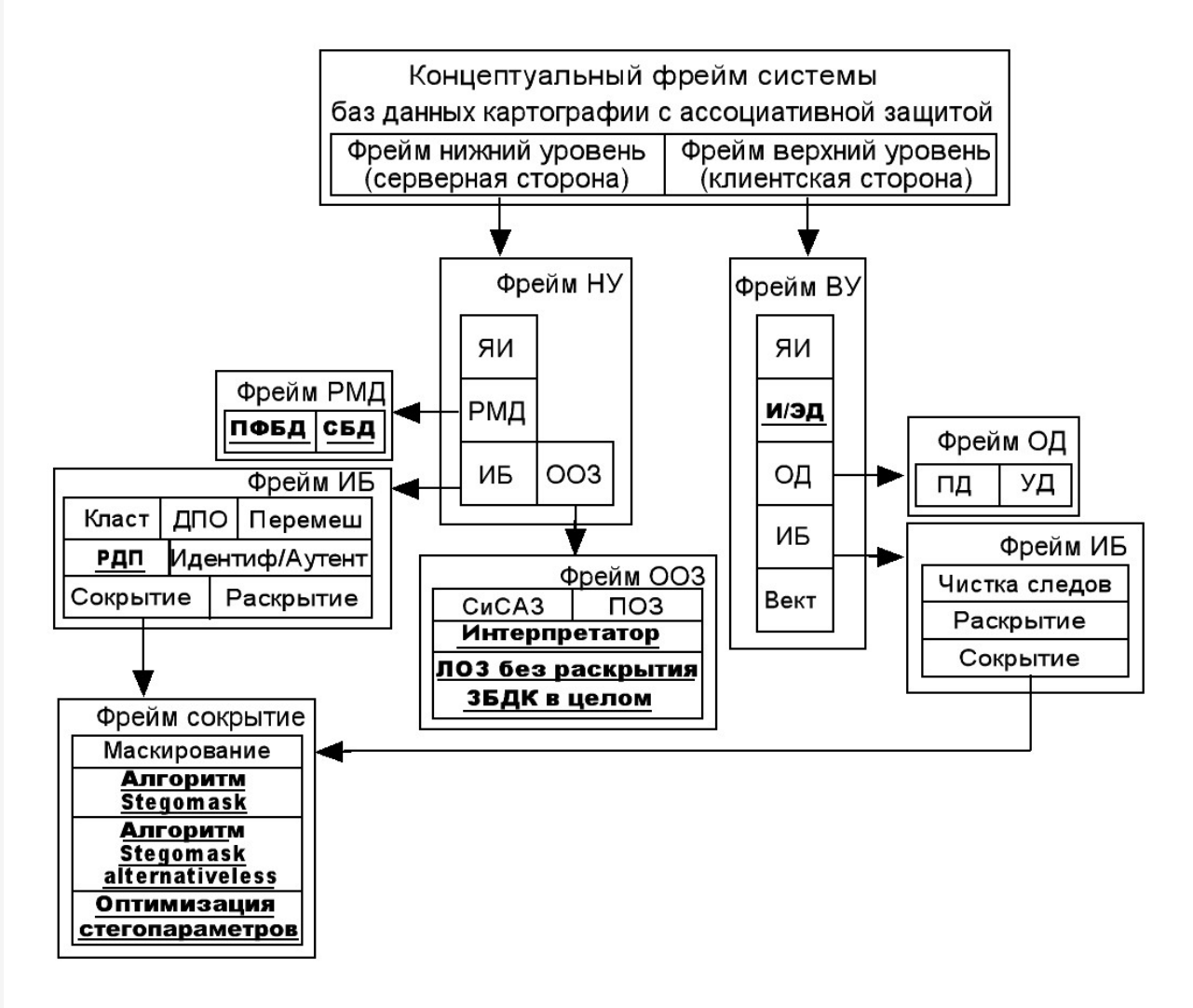
Диссертация на соискание ученой степени кандидата технических наук, 2011.

Результаты

1. ***Предложена двухуровневая модель системы баз данных картографии с ассоциативной защитой***, которая позволяет повысить эффективность управления защищенными БД картографии в сравнении с известными СУБД по критерию быстродействия.
2. Разработан алгоритм формирования стегоконтейнера, основанный на применении двумерно-ассоциативного механизма защиты. На его основе ***подтверждена гипотеза о принципиальной возможности достижения безусловной стойкости ассоциативного метода стегозащиты***.
3. Оптимизированы значения стегопараметров алгоритма формирования стегоконтейнера по критерию быстродействия. ***Установлено, что время формирования стегоконтейнера предложенным алгоритмом Stegomask минимально при 40 ≤ m ≤ 60 и 105 ≤ K ≤ 3×105. Показана предпочтительность использования алгоритма Stegomask в режиме безальтернативного выбора гаммы при m = 60.*** Выявлены положительные черты двумерно-ассоциативного механизма маскирования сравнительно с ГОСТ 28147-89.
4. ***Разработана схема защищенной БД картографии***, которая реализует ассоциативно-защищенное хранение данных картографии. ***Предложен эффективный метод локальной обработки запросов к защищенной БД картографии*** и на его основе разработаны алгоритмы интерпретации пользовательских запросов, отличающиеся от существующих тем, что позволяют обрабатывать запросы к защищенной БД картографии без ее полного раскрытия.
5. ***Разработан исследовательский прототип СУБД Security MapPointCluster***, на основе которого обоснованы практические рекомендации к построению системы баз данных картографии с ассоциативной защитой.

2.1. Система Security Map-Point Cluster

Предложена модель системы баз данных картографии с ассоциативной защитой.

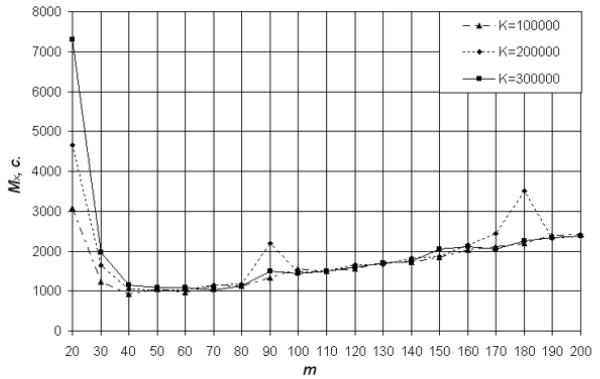


2.2. Система Security Map-Point Cluster

- Подтверждена гипотеза о принципиальной возможности достижения безусловной стойкости ассоциативного метода стегозащиты.
- Установлено, что время формирования стегоконтейнера предложенным алгоритмом Stegomask минимально при $40 \le m \le 60$ и $10^5 \le K \le 3 \times 10^5$.
- Показана предпочтительность использования алгоритма Stegomask в режиме безальтернативного выбора гаммы при m = 60.

Оптимизация значений стегопараметров

Оценка математического ожидания времени сокрытия (M_x) 100 кодов при различных значениях m и K

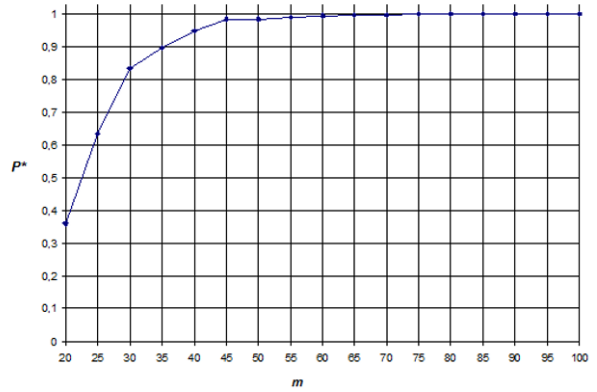


Утверждение 1. Формирование стегоконтейнера при $k = 3$ и $\gamma = 10$ при удовлетворении энтропийного критерия К.Шеннона в его логической трактовке занимает минимальное время при $40 \le m \le 60$ и $10^5 \le K \le 3 \times 10^5$.

m – параметр, определяющий размер стегоконтейнера по формуле $3 \times (9 \times m - 12)$;
K – максимальное число случайных выборок ключей из полного их множества;
k – разрядность кодового слова;
γ – основание исчисления.

Алгоритм *Stegomask* в режиме безальтернативного выбора контейнера

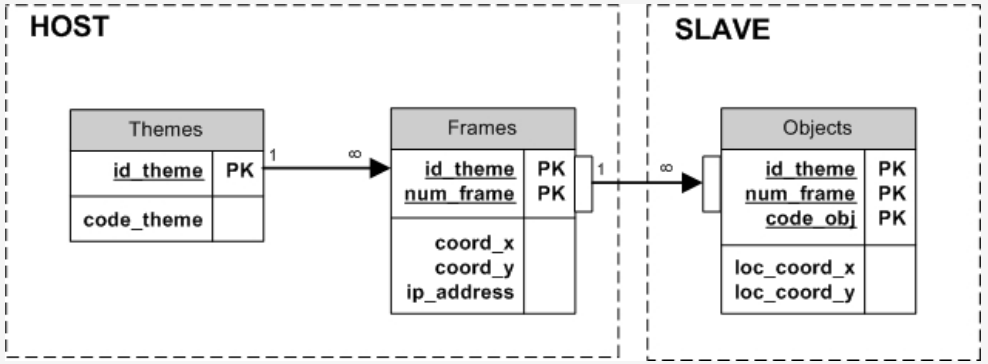
Оценка вероятности события (P^*), при котором первый попавший контейнер был успешным, для различных m



Утверждение 2. С увеличением значения m растет оценка вероятности того, что стегоконтейнер, полученный безальтернативным выбором гаммы, покроет полный словарь сообщений при ограниченном переборе ключей. В частности, при $m = 60$, $K = 2 \times 10^5$ значение $P^* = 0{,}999$.

2.3. Система Security Map-Point Cluster

- Разработана схема защищенной БД.
- Предложен эффективный метод локальной обработки запросов.



Функция инициализации

```
my_bool udf_decode_init
(UDF_INIT *initid, UDF_ARGS *args, char *message) {
initid->ptr=(char*) malloc(3000); //выделение памяти
read_key(&initid->ptr[0]); //чтение секретного ключа
read_etalons(&initid->ptr[1500]); //чтение эталонов
args->arg_type[0] = STRING_RESULT; //задание типа данных
                                    результата
return 0; }
```

Функция деинициализации

```
void udf_decode_deinit(    UDF_INIT *initid) {
free(initid->ptr); } //освобождает всю память, выделенную функцией
                      инициализации
```

Функция раскрытия

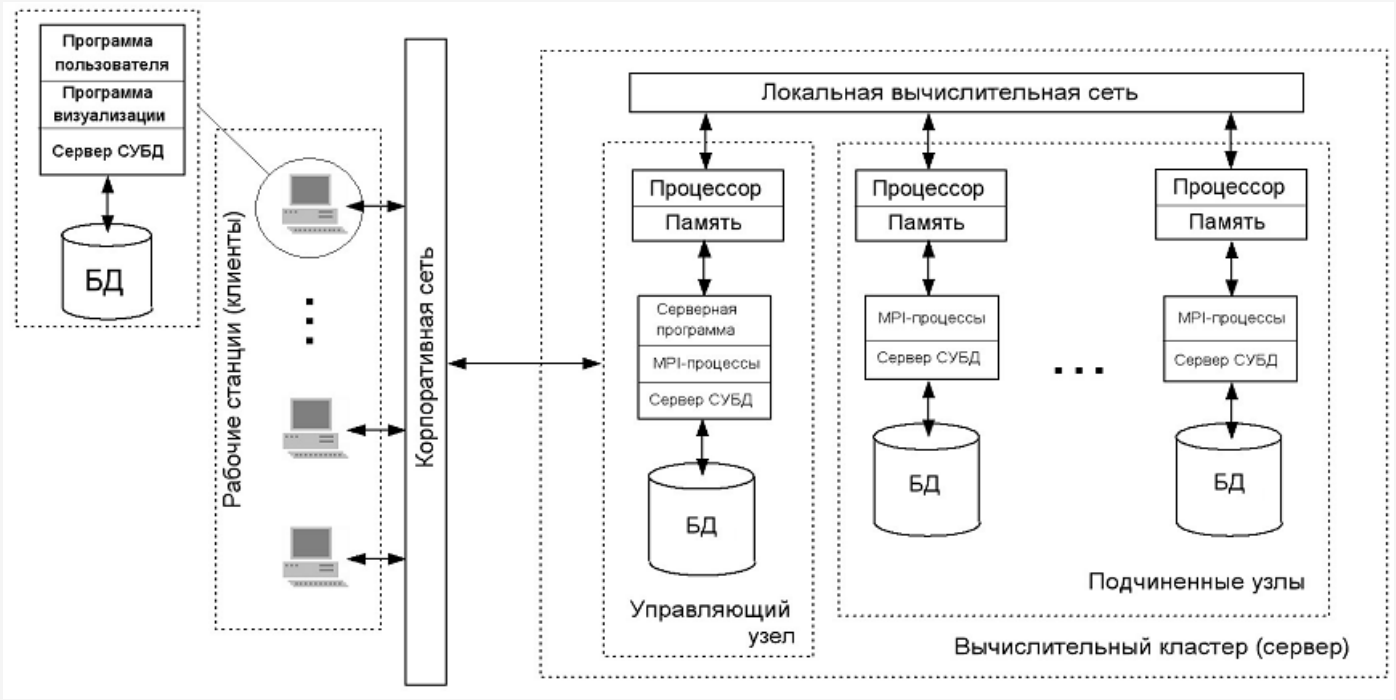
```
char* udf_decode(UDF_INIT *initid,    UDF_ARGS *args, char* result,
unsigned long *length, char *is_null, char *error){
//раскрытие стегоконтейнера и запись результата в result
sprintf(result,"%03d",decode(&initid->ptr[3000], &initid->ptr[0],
&args->args[0]));
*length=strlen(result); //определение размера возвращаемых данных
return result; }

CREATE FUNCTION udf_decode RETURNS STRING
SONAME 'udf_decode.dll';

SELECT * FROM Theme WHERE udf_decode(code_theme) > 1;
```

2.4. Система Security Map-Point Cluster

Разработан исследовательский прототип.



3. Система Security Map Cluster

Пыстогов С. В.

СУБД полнообъектных картографических сцен с ассоциативной защитой на кластерной платформе.

Диссертация на соискание ученой степени кандидата технических наук, 2019.

Результаты

1. ***Предложен метод организации (схема) БД ПКС с ассоциативной защитой (АЗ)***, основанный на разделении тематических слоев для разных типов объектов с выделением своего слоя для любого линейного и площадного объекта, что, в отличие от известного, позволяет снять ограничения на размеры протяженных объектов.
2. ***Предложен метод генерации тестовых БД ПКС с АЗ, основанный на выделении в сцене прямоугольной области для каждого запроса представительского теста***, что, в отличие от универсальных тестов TPC, позволяет провести анализ динамики СУБД ПКС при обработке пакетов запросов.
3. ***Предложен метод обработки селективных запросов к БД ПКС, основанный на неполной выборке узловых точек протяженных объектов***, что, в отличие от предложенного ранее подхода, позволяет провести обработку таких запросов по указанным объектам без «раскрытия» всей БД. На основе метода разработан программный комплекс (натурная модель, воспроизводящая реальные системные ситуации) серверной части ассоциативно-защищенной СУБД ПКС с ассоциативной защитой, который позволяет проводить исследования по ассоциативной стеганографии с использованием адекватного инструментального средства.
4. На разработанном программном комплексе ***проведен ряд экспериментальных исследований, что позволило получить сравнительные характеристики динамики процессов при обработке пакетов запросов для двух возможных архитектур системы*** и на их основе предложить практические рекомендации по применению архитектур системы и возможному улучшению производительности.
5. ***Предложен программный алгоритм клиентской части системы***, основанный на предварительной обработке запросов пользователя, что в отличие от существующих подходов позволяет пользователю выполнять запросы без знания структур БД ПКС. На основе алгоритма ***разработан программный прототип клиентской части системы***.

3.1. Система Security Map Cluster

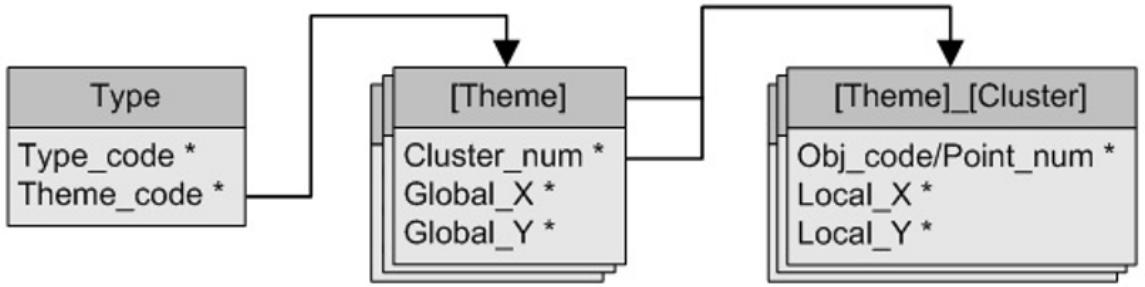
Предложен метод организации (схема) БД ПКС.

БАЗА ДАННЫХ ПОЛНООБЪЕКТНЫХ КАРТОГРАФИЧЕСКИХ СЦЕН

***Предлагаемая инфологическая схема* БД ПКС.**

– Схема предполагает единообразный формат хранения данных для всех типов объектов: точечных, линейных и площадных.

– Связи между отношениями определяются в процессе работы программы сервера.



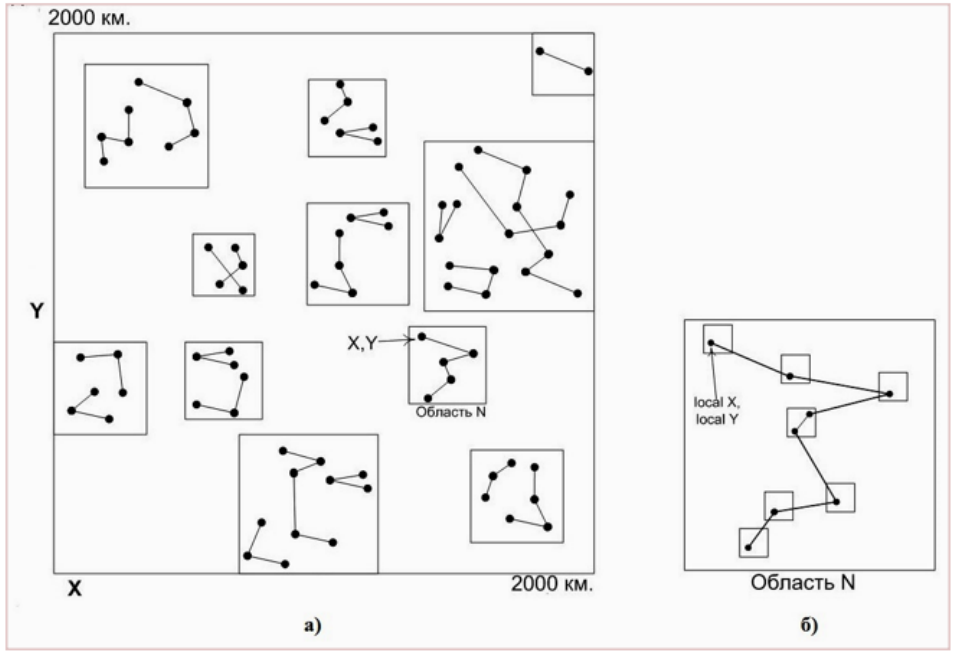
Type – содержит информацию о всех тематических слоях сцены, представленных парой сокрытых кодов: Код типа – Код слоя.

[Theme] – набор отношений, каждое из которых описывает отдельный тематический слой (фрагменты внутри слоя).

[Theme]_[Cluster] – набор отношений, каждое из которых описывает содержимое (объекты) одного фрагмента какого-либо тематического слоя.

3.2. Система Security Map Cluster

Предложен метод генерации тестовых БД ПКС.



Объемы полученных тестовых ПБД КС АЗ:
БД1 ≈ 80 Мб.
БД2 ≈ 150 Мб.
БД3 ≈ 300 Мб.

Пусть ***k*** – число точечных объектов (узловых точек), выбираемых в результате выполнения селективного запроса ***m*** из области N для БД1. Тогда число объектов, выбираемых из области N тем же запросом ***m*** для БД2 должно быть примерно $2k$. Для БД3 – $4k$.

3.3. Система Security Map Cluster

Предложен метод обработки селективных запросов к БД ПКС, основанный на неполной выборке узловых точек протяженных объектов.

Метод обработки запросов без раскрытия всей БД ПКС

На примере селективного запроса:

select * from kbd1.theme_name where X<20000 and Y>5000;

На основе параметров, указанных в этом запросе, формируется перечень подзапросов адаптированных к языку MySQL и схеме ПБД КС, выполняемых последовательно этой СУБД:

1 A. SELECT Code from Point_Themes where Name= ”theme_name”;
Получение кода тематического слоя, в рамках которого ведется поиск.

2 B. SELECT Cluster_num, Global_X, Global_Y from Theme_N;
Получение списка фрагментов (кластеров) слоя ***N*** с их глобальными координатами.

3 C. Множество подзапросов
SELECT Obj_code, local_X + Global_X*A, local_Y + Global_Y*A from Theme_N, Cluster_(i) where Cluster_num=i, (local_X + Global_X*A) < 20000 and (local_Y + Global_Y*A)> 5000);
Поиск объектов в каждом выбранном фрагменте.

3.4. Система Security Map Cluster

Сравнительные характеристики динамики процессов при обработке пакетов запросов для двух возможных архитектур системы.

Обсуждение результатов экспериментов

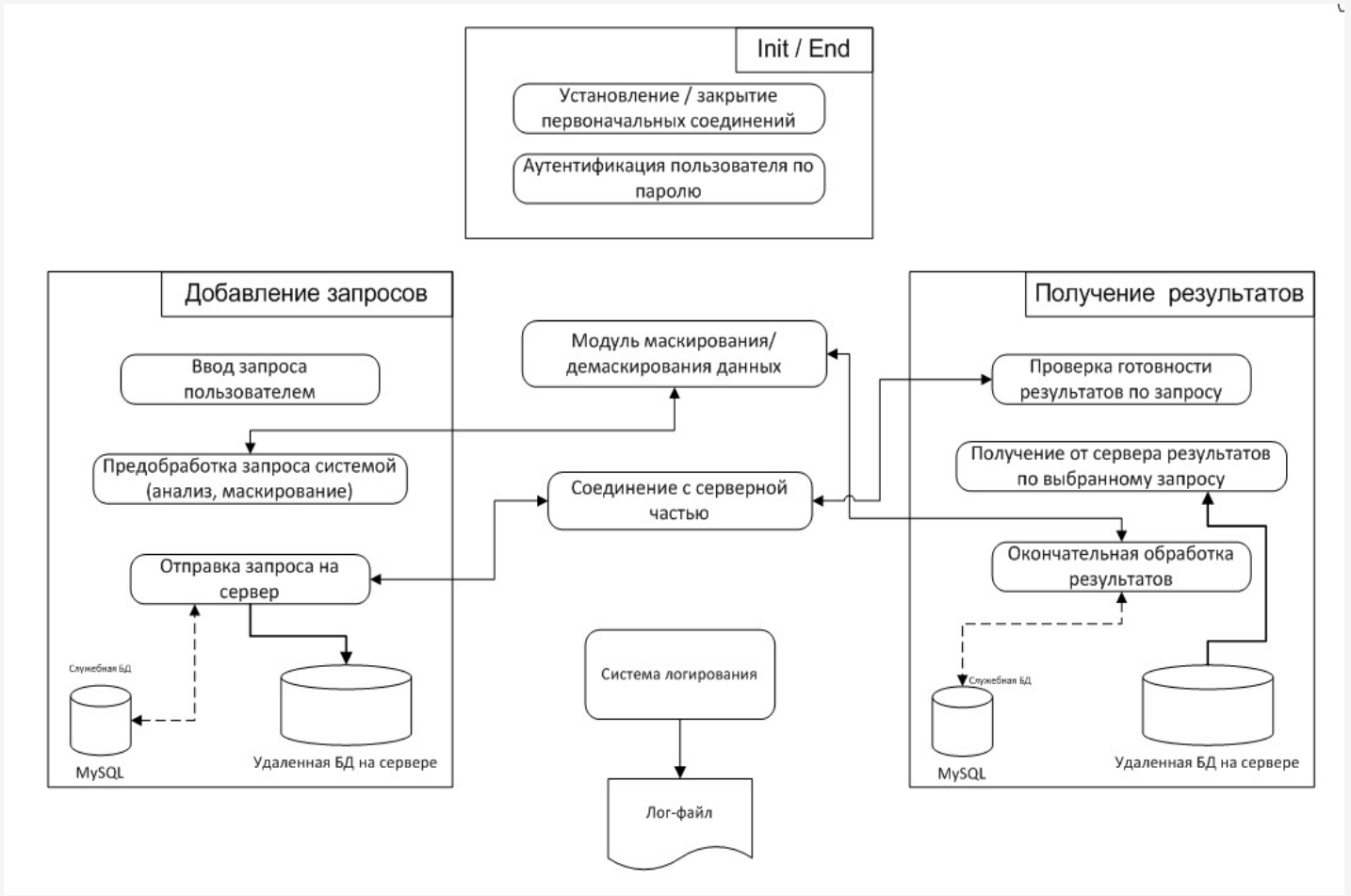
1. *Эксперименты 1 и 2* выявили преимущество монокластерной архитектуры по значениям параметров S и $N_{гр}$.
2. *Эксперимент 3* отдает предпочтение мультикластеру. Однако сценарий этого эксперимента видится маловероятным для небольшого числа пользователей.
3. *Мультикластерный подход проигрывает* при выполнении ***запросов изменения*** и при выполнении ***селективных запросов*** с выборкой *крупных областей со множеством объектов*.
4. *Выбор монокластера однозначен* при ***генерации новой БД ПКС*** или ***изменении защитного ключа*** в системе.

Таким образом,

архитектура монокластера предпочтительна для практического применения.

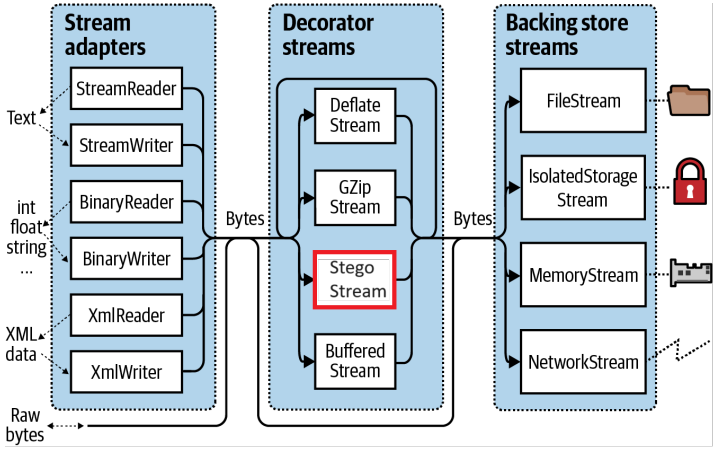
3.5. Система Security Map Cluster

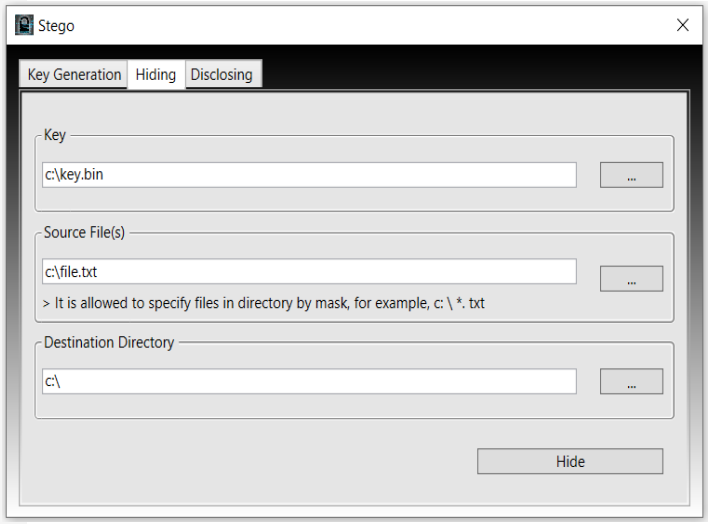
Разработан программный прототип клиентской части системы.

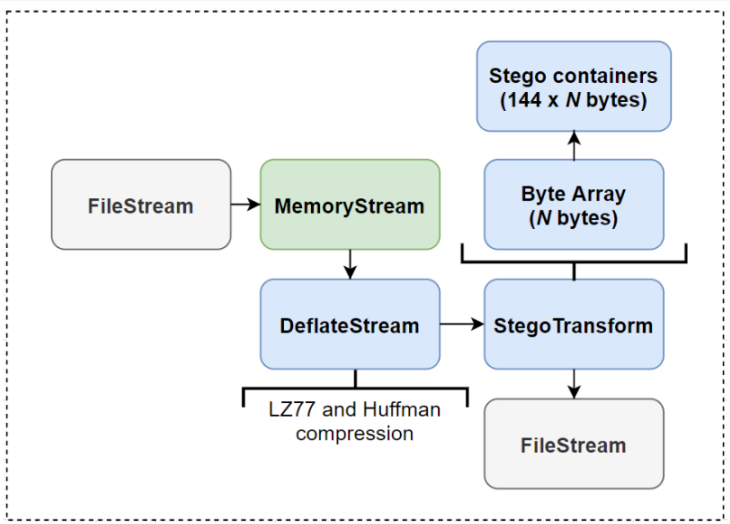


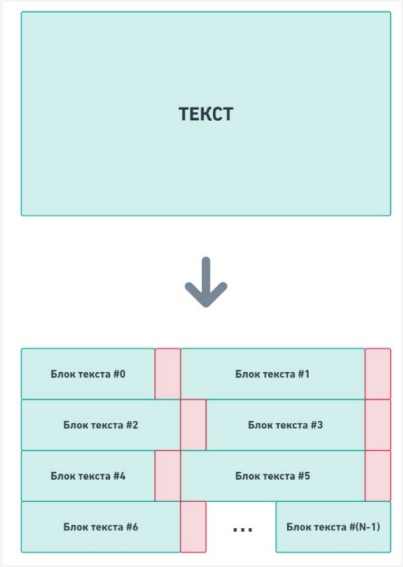
4. Защита текстовых сведений

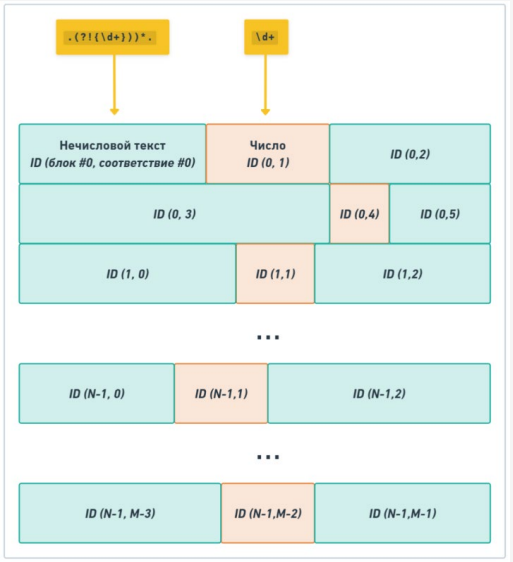
- Программный модуль Stego.
  - Декоратор StegoStream.

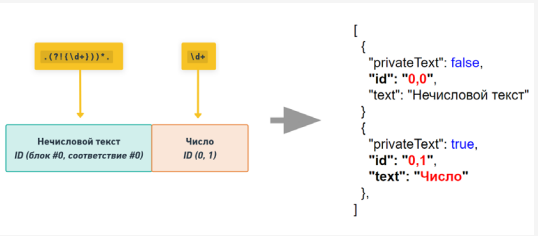












5. Помехо-устой-чивость

Случайным образом выбиралось 16 байтов для каждого стегоконтейнера. В любом из этих байтов случайно выбиралось n_i искажаемых (инвертируемых) бит. Стегоконтейнеры искаженного сообщения по-отдельности распознавались по всем Q ключам. Определялось количество неверных распознаваний и отказов от распознавания.

Таблица. Q = 7, искажение16 байт каждого из 10^3 стегоконтейнеров в %

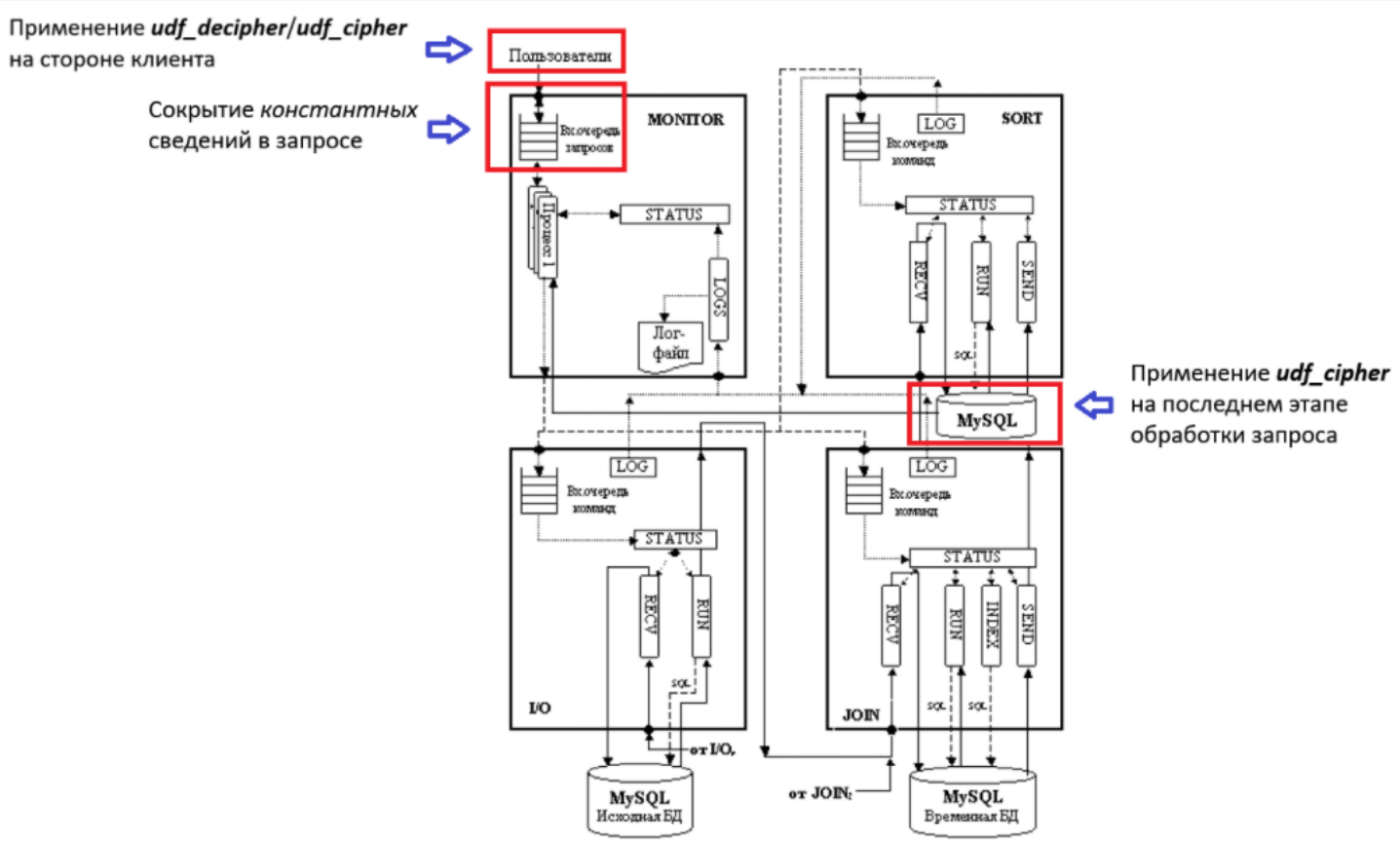
Число не-верных бит в 1 байте	n = 60			n = 40			n = 30		
	верно	*неверно*	*отказ**	*верно*	*неверно*	*отказ*	*верно*	*неверно*	*отказ*
1	**100**	**0**	**0**	**99,6**	**0**	**0,4**	**100**	**0**	**0**
2	**100**	**0**	**0**	**99,6**	**0**	**0,4**	**99,2**	**0**	**0,8**
3	**98,4**	**0**	**1,6**	**96**	**0**	**4**	**91,2**	**0**	**8,8**
4	**97,2**	**0**	**2,8**	84,8	0	15,2	72,8	0	27,2
5	**92,8**	**0**	**7,2**	73,6	0,8	25,6	54,8	0	45,2
6	88,8	0	11,2	62,4	0,8	36,8	38,8	0,4	60,8
7	81,2	0	18,8	48	1,2	50,8	25,2	0,4	74,4
8	74,4	0	25,6	36,4	2,4	61,2	15,2	0,4	84,4

* Отказ при не соблюдении условия: $r_i \geq](Q+1)/2[$.

Использование мажоритарного принципа обеспечивает более 90% правильных распознаваний и менее 10% отказов от распознавания при полном отсутствии неверных распознаваний, если для n = 60 искажены от одного до пяти бит в любых 16 байтах каждого стегоконтейнера, для n = 40 и 30 – до трех бит.

6.1. Перспективы

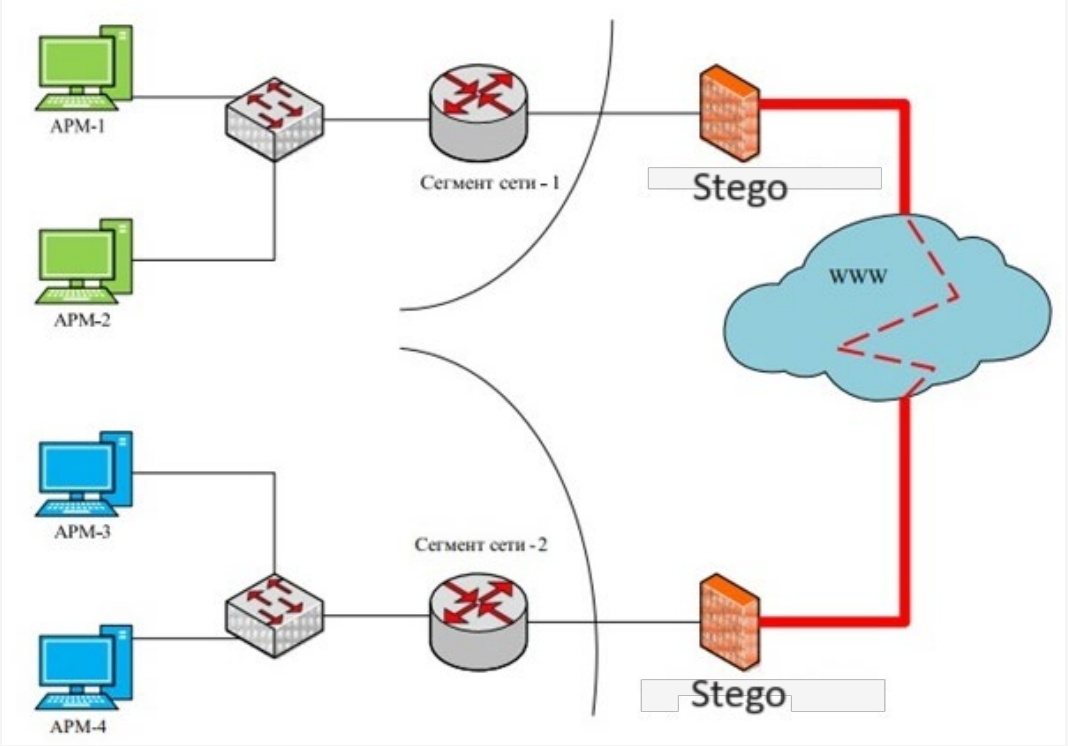
Параллельные СУБД.



6.2. Перспективы

Компьютерные сети.

Криптошлюз — это компонент выполняющий сквозное шифрование всего передаваемого трафика (как в локальной сети, так и при инициализации интернет-соединения). В качестве шлюза можно разработать программу, устанавливаемую на сервере.

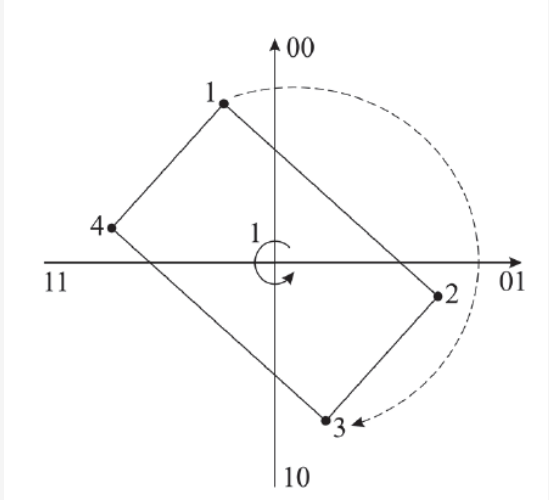


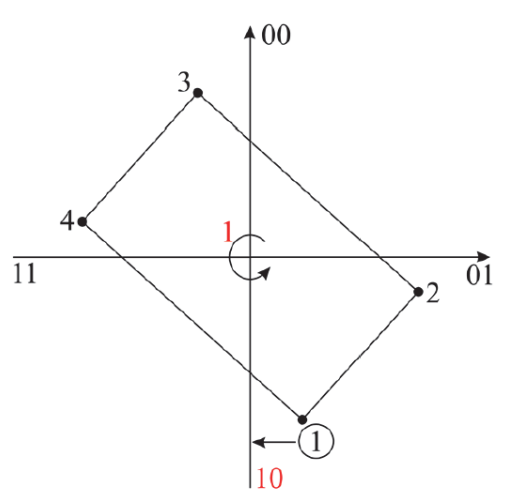
6.3. Перспективы

Выборнова, Ю. Д., Сергеев, В. В. (2021). Метод защиты авторских прав на векторные картографические данные. Информатика и автоматизация, 20(1), 181-212.

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. 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 предлагается использовать растровое изображение, наложенное на выбранный фрагмент векторного слоя путем разбиения карты на прямоугольные ячейки и отображения полученного разбиения на сетку пикселей растра.





Заключение

Использование разработанных функций ***udf_cipher*** и ***udf_decipher*** обеспечит защиту передаваемых результатов обработки запросов по сети. Также *возможен* вариант обеспечения прозрачного шифрования передаваемого трафика с применением программного стегошлюза.

В статье В.В. Сергеева и Ю.Д. Выборнова цифровые водяные знаки встраиваются в виде шумоподобных изображений. 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.