Параллелизация решения систем уравнений как инструмент в схеме разделения секрета

Д.А. Волков, Р.Т. Файзуллин

Омский Государственный Технический Университет

- Консолидация обработки и хранения больших массивов информации в центрах обработки данных – одно из самых перспективных направлений совершенствования корпоративных систем. Применение и внедрение ЦОД позволяет наиболее эффективно использовать коллективные вычислительные ресурсы, уменьшает общее число оборудования, снижает расходы на их поддержку.
- Необходимым элементом ЦОД является гарантированная защита информации. Основными направлениями защиты информации являются: защита от вирусных атак, обеспечение безопасности процесса взаимодействия информационных систем ЦОД с внешними источниками информации и, что наиболее важно, защита информации от несанкционированного доступа. Несмотря на все усилия у пользователей имеется определенная и обоснованная степень недоверия к уровню защиты ЦОД и к облачным вычислениям, основанная на угрозе мафиозной атаки. Даже наличие криптографических средств защиты информации и различных лицензий не убеждают в достаточной защищенности процессов хранения и обработки информации.

- Представляется возможным предложить решение данной проблемы с помощью различных схем разделения секрета, причем таких схем, что малая, но определяющая информативность часть секрета хранится или обрабатывается у клиента . Данный подход позволяет добиться того, что в ЦОД хранятся данные, но не сама информация и в каждом случае можно привести прозрачное для клиента доказательство того, что по большему массиву данных нельзя в принципе восстановить значимую информацию.

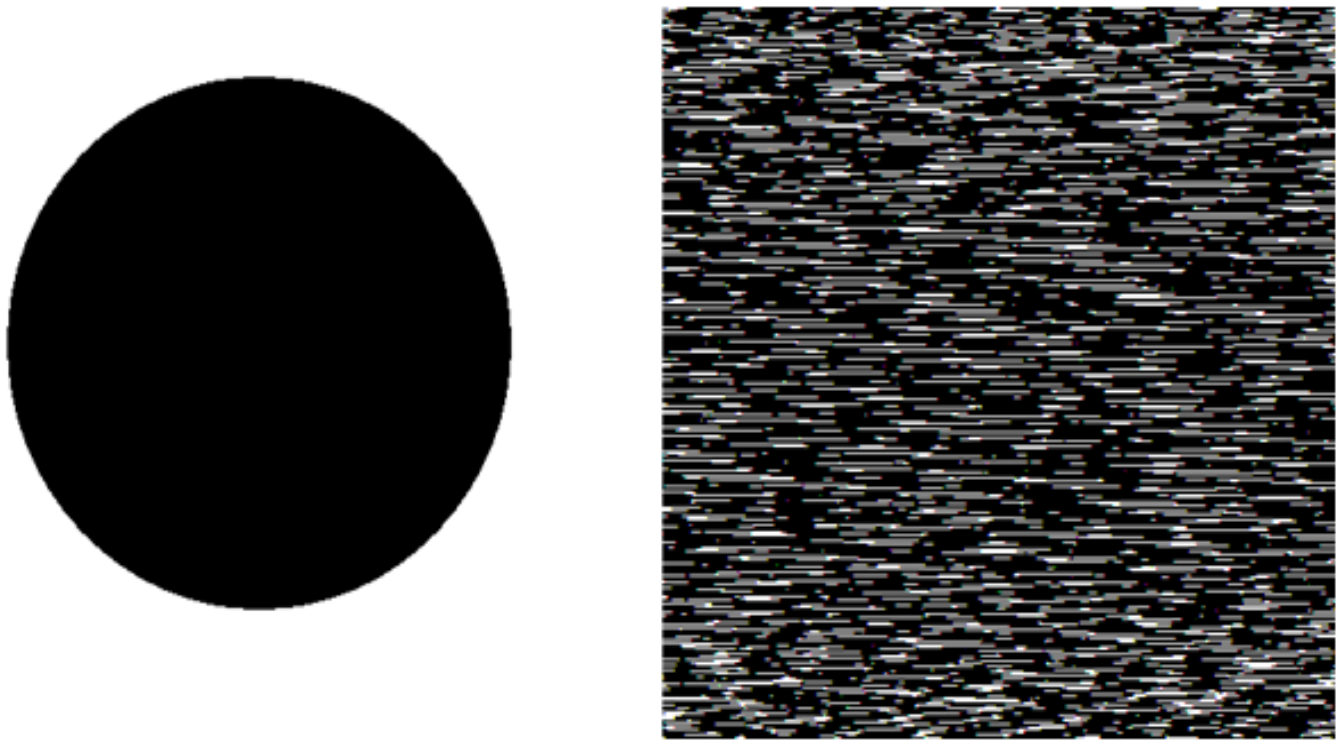
- Две задачи: разделение данных и разделение операций.
- Сборка информации на компьютере владельца.
- Доказуемая стойкость к атаке восстановления информации по их большей части данных.

а) б)

Рис. 1. а) – исходное изображение; б) – изображение, полученное атакующим, при попытке восстановить изображение из имеющейся у него последовательности бит.

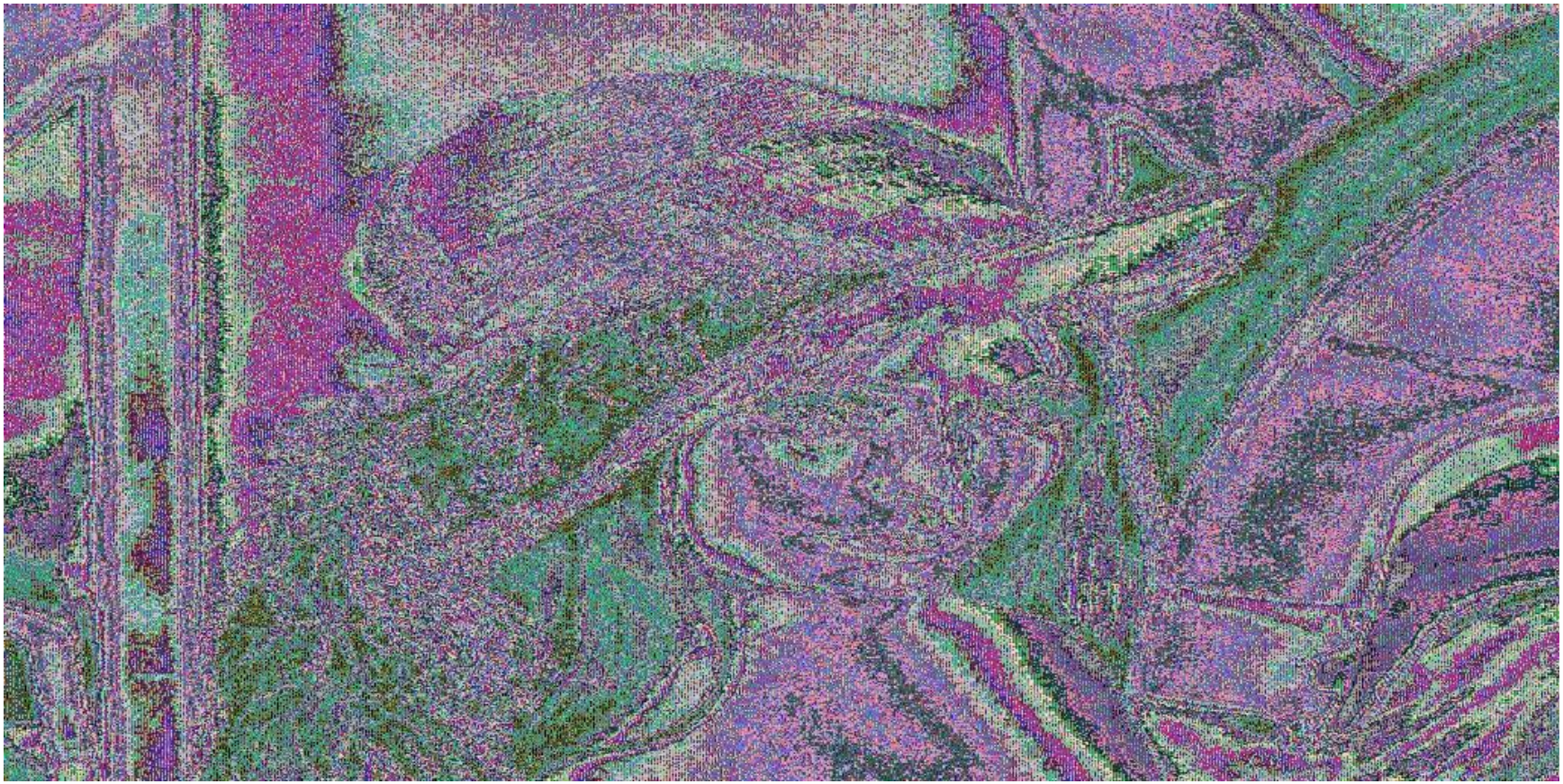
а) б)

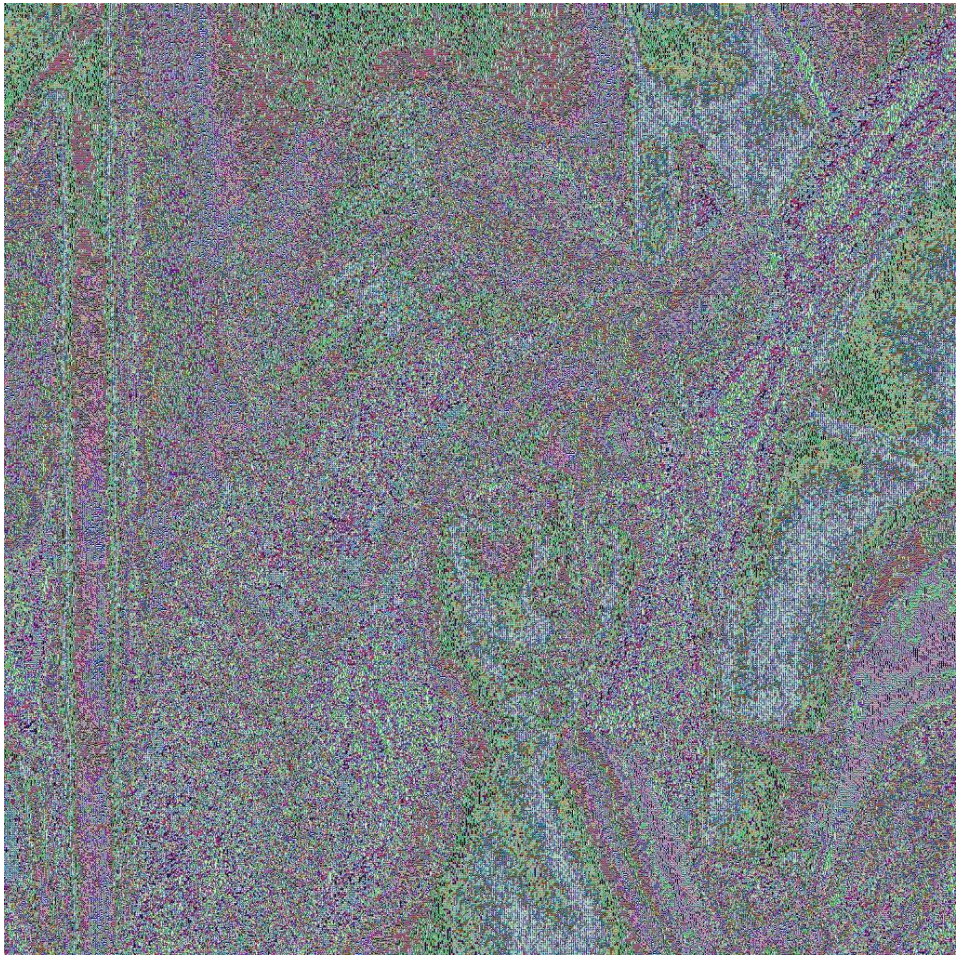
Рис. 2. а) – исходное изображение; б) – изображение, полученное атакующим, при попытке восстановить изображение из имеющейся у него последовательности бит.



а) б)

Рис. 3. а) – исходное изображение; б) – изображение, полученное атакующим, при попытке восстановить изображение из имеющейся у него последовательности бит.





Метод Гаусса

$$\begin{pmatrix} A, B \\ C, D \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = \begin{pmatrix} F_1 \\ F_2 \end{pmatrix}$$

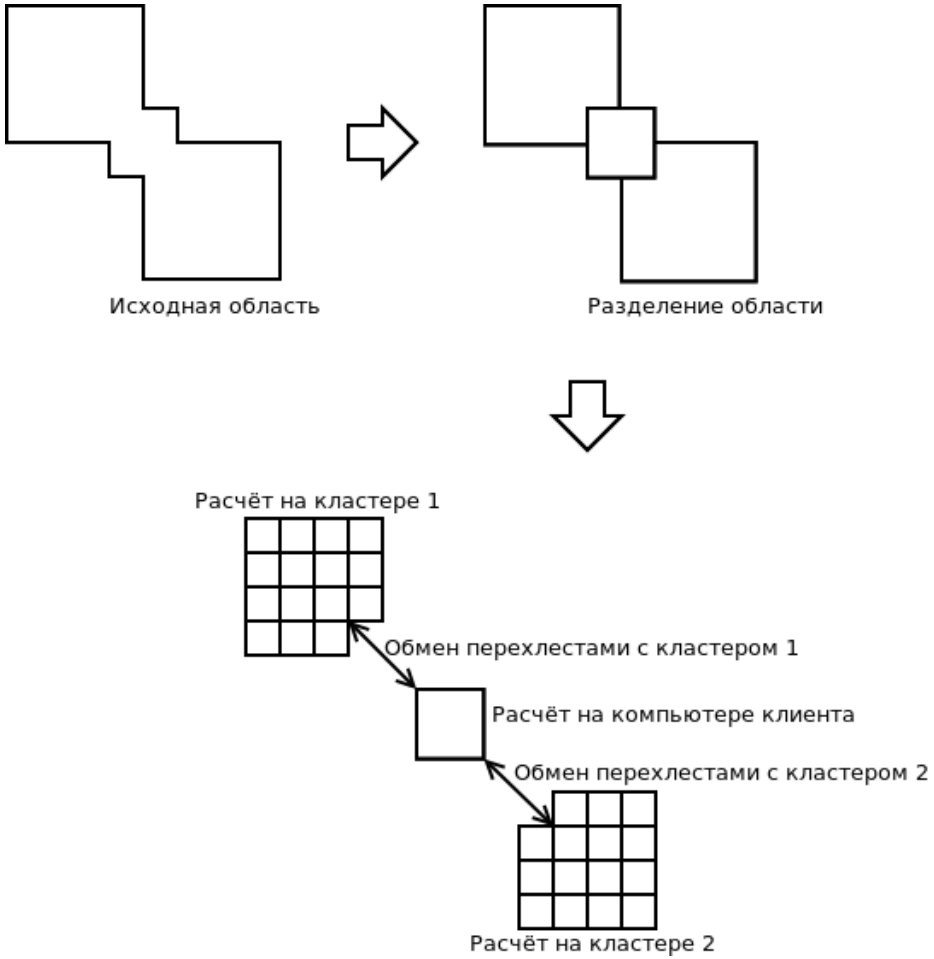
$$\begin{pmatrix} A, & B \\ 0, D - CA^{-1}B \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = \begin{pmatrix} F_1 \\ F_2 - CA^{-1}F_1 \end{pmatrix}.$$

Формула Фробениуса вычисления обратной матрицы

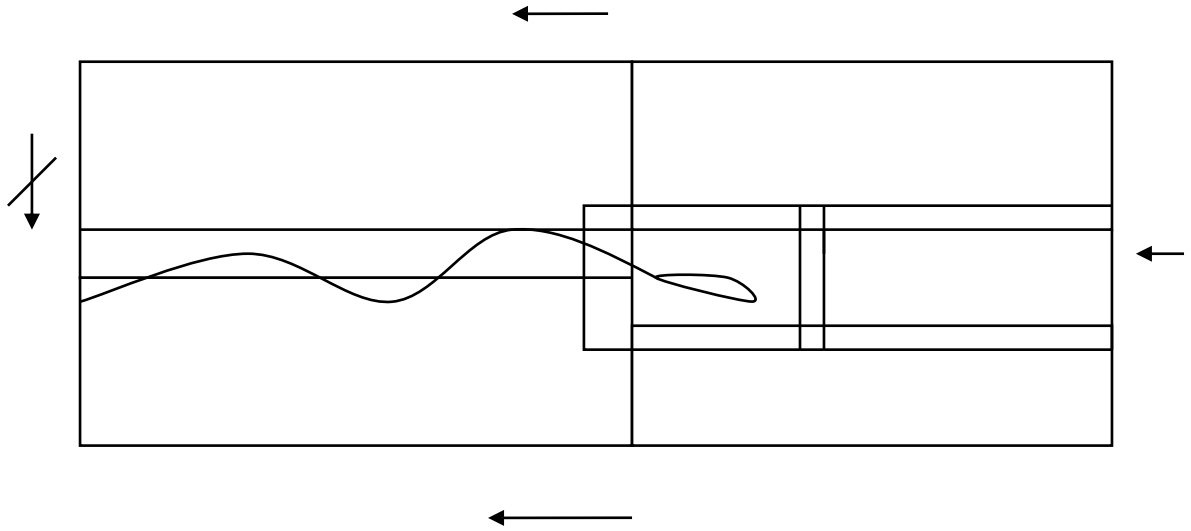
$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}^{-1} = \begin{pmatrix} A^{-1} + A^{-1}BH^{-1}CA^{-1}, & -A^{-1}BH^{-1} \\ -H^{-1}CA^{-1} & H^{-1} \end{pmatrix},$$

$$H = D - CA^{-1}B$$

Разбиение областей при решении эллиптической задачи

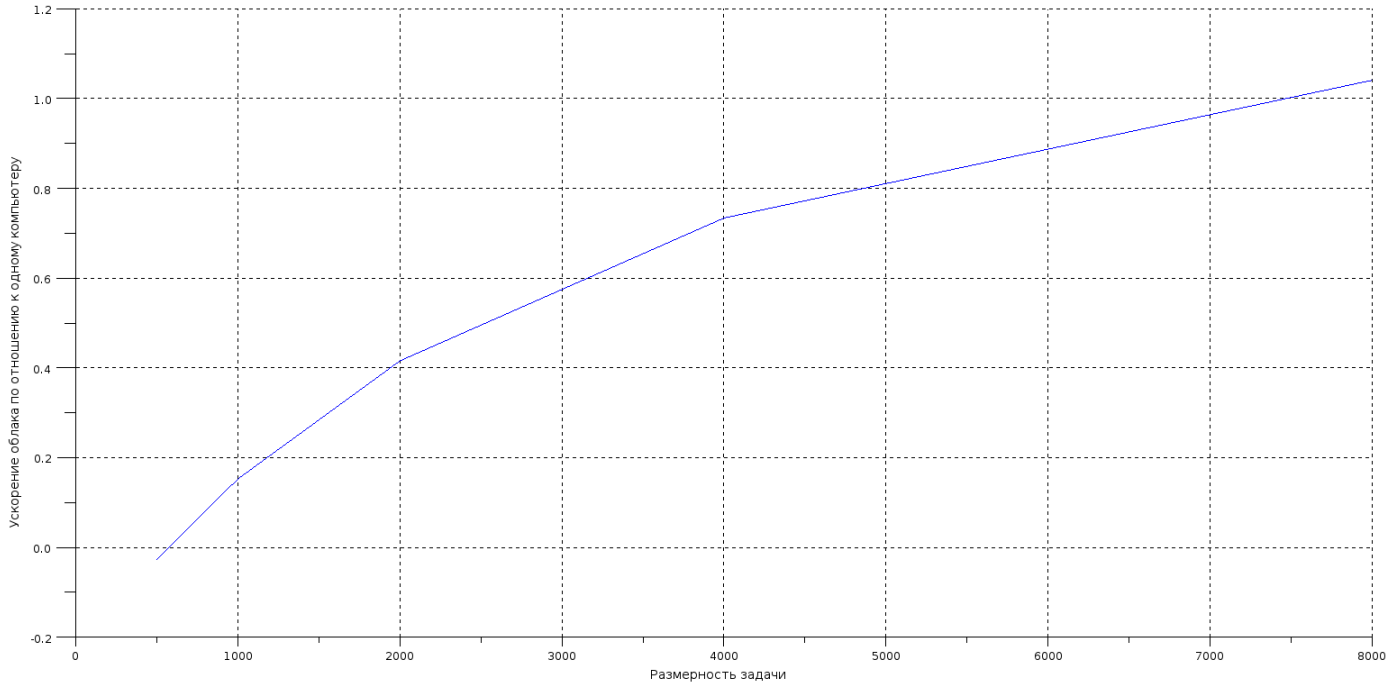


Разбиение области для задачи обтекания



Возможная схема разделения операций

Рост эффективности облака при росте размерности задачи, обмен файлами.



Применение к задачам дискретной математики

– Аналогичный подход можно реализовать не только для численного решения краевых задач математической физики, но и для задач дискретной математики. Например, очевидная параллелизация задач о кратчайшем пути или о максимальной клике позволяет разделить секрет о структуре графа.

Литература

- Файзуллин Р.Т., Сагайдак Д.А. Приложение алгоритма префиксного кодирования массива данных в схеме разделения секрета// Доклады Томского государственного университета систем управления и радиоэлектроники. -1(25), -часть 2, -2012, С. 136-140.
- Р.Т. Файзуллин, И.Р. Файзуллин, О.Т. Данилова Алгоритмы разделения секрета с использованием принципиально малой части в качестве ключа// Вестник Тюменского государственного университета. - Тюмень: ГОУ ВПО ТюмГУ, 2011. -вып. 7. - С.175 -179.
- Р. Т. Файзуллин, “О решении нелинейных алгебраических систем гидравлики”, Сиб. журн. индустр. матем., 2:2, 1999.
- К. В. Логинов, А. М. Мызников, Р. Т. Файзуллин,“Расчет, оптимизация и управление режимами работы больших гидравлических сетей”, Матем. моделирование, 18:9 (2006).