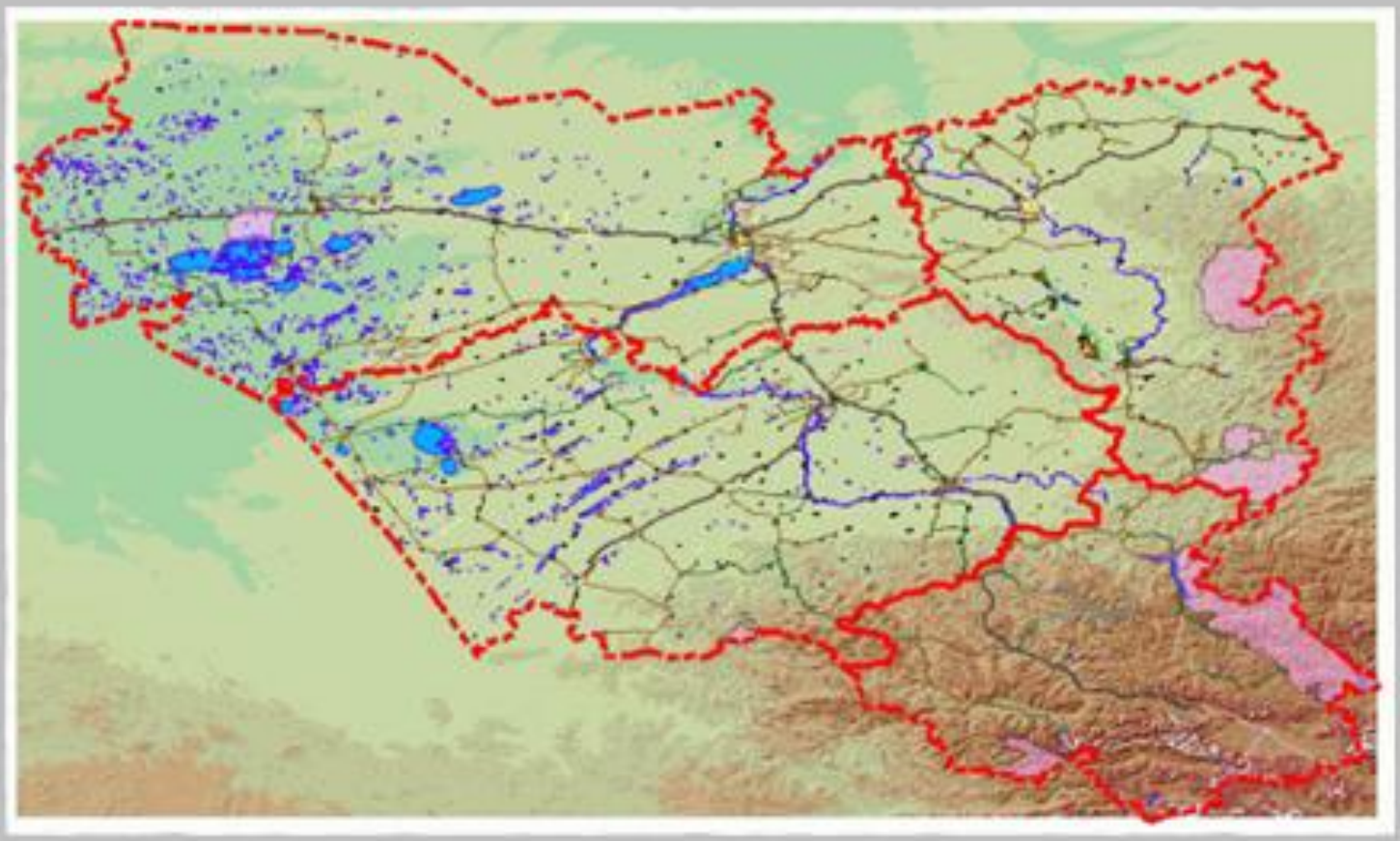


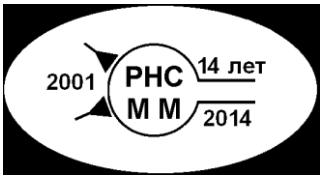
И.С. ВЕРШИНИН, Р.Ф. ГИБАДУЛЛИН
С.В. ПЫСТОГОВ, В.А. РАЙХЛИН

АССОЦИАТИВНАЯ СТЕГАНОГРАФИЯ

/ Приложение к анализу сцен /

Академия наук Республики Татарстан

Республиканский научный семинар
«МЕТОДЫ МОДЕЛИРОВАНИЯ»



И.С. ВЕРШИНИН, Р.Ф. ГИБАДУЛЛИН,
С.В. ПЫСТОГОВ, В.А. РАЙХЛИН

АССОЦИАТИВНАЯ СТЕГАНОГРАФИЯ

/Приложение к анализу сцен/

Под редакцией В.А. РАЙХЛИНА

КАЗАНЬ
2014

УДК 681.3
ББК 32
В18

Издание осуществлено по рекомендации Оргкомитета Республиканского научного семинара АН РТ «Методы моделирования»

Вершинин И.С., Гибадуллин Р.Ф., Пыстогов С.В., Райхлин В.А.
В 18 Ассоциативная стеганография (*Приложение к анализу сцен*) /Под ред. В.А. Райхлина. – Казань: Изд-во Казан. ун-та, 2014. – 132 с.

ISBN 978-5-00019-284-9

Вводится понятие ассоциативной стеганографии. Показаны корректность его названия, обоснованность принципов, высокая стего- и помехоустойчивость их реализации. Определена прикладная ниша ассоциативной стеганографии, ей адекватная. В этой нише выделяется направление ассоциативной защиты картографических данных. Оно развивается не только в теоретическом, но и в плане разработки параллельных СУБД защищенных картографических сцен. Развитие других практически важных приложений потребует создания специальных технических средств, немалых затрат ресурсов и творческой энергии.

Для научных работников, аспирантов и магистрантов, специализирующихся в области защиты информации и высокопроизводительных информационных систем.

Табл. 19. Ил. 86. Библиогр.: 72 назв.

УДК 681.3
ББК 32

ISBN 978-5-00019-284-9

ПРЕДИСЛОВИЕ РЕДАКТОРА

Ассоциативная стеганография – принципиально новое понятие, введенное авторами post factum. Оно сформировалось в итоге 1) многолетних исследований [1-5] по ассоциативной обработке информации вообще и стилизованных бинарных изображений, в частности, и 2) по получении позитивных результатов представленных в книге исследований по двумерно-ассоциативной защите геопространственных данных. Такая защита относится к области *стеганографии* (тайнописи, скрывающей сам факт передачи сообщения), а не *криптографии* (занимающейся формированием и обработкой шифрограмм). Двумерно-ассоциативное маскирование следует рассматривать как частный случай т.н. *трафаретного способа классической стеганографии* [6], когда скрываемое сообщение записывается по трафарету на чистый лист, после чего формируется осмысленный текст с такой вставкой. Вся разница в том, что в данном случае сообщение внедряется в шумовую картину. Но это – не принципиально. Главные вопросы в обоих случаях – алгоритмизация случайного формирования трафарета (ключа) и заполнения не занятых сообщением участков. Поэтому в книге, в коррективу терминологии, принятой на начальных этапах исследований, и в противовес «крипто-», используются принятые в стеганографии термины: *стегозащита*, *стегоключ* и т.д.

Определение понятия принято связываеть с заданием необходимых и достаточных условий, которым это понятие должно удовлетворять. В данном случае эти условия (принципы) таковы:

1. Рассматривается всегда не единичное, а фиксированное конечное множество сообщений. В том – принципиальное отличие рассматриваемого подхода от всех известных методов шифрования. Сообщения стилизуются в виде полагаемых заданными бинарных матриц-эталонов одинаковых размеров $m \times n$. Передача (хранение) любого из сообщений заданного множества считается априорно равновероятной. Принимаемое сообщение распознается (различается) путем сравнения на полном множестве эталонов.

2. Множество таких матриц подвергается маскированию. Для каждой матрицы создается своя матрица масок тех же размеров, которая сохраняет в эталоне биты, существенные для его дальнейшей идентификации.

При этом могут быть введены ограничения по исключению некоторых бит из числа существенных. Процесс генерации масок случаен. Сгенерированное множество масок является ключом. Допускается избыточное маскирование, когда несколько наборов инверсных масок дизъюнктивно объединяется поэталонно.

3. Целью маскирования является удовлетворение, во-первых (в теории), критерия совершенной секретности по К. Шеннону [7] (равенство априорной вероятности передачи и апостериорной вероятности раскрытия при приеме) в его логической трактовке (замене термина «равновероятно» на термин «равноправдоподобно») и, во-вторых, требования высокой помехоустойчивости передачи любого из сообщений заданного множества.

4. То и другое предполагает погружение каждой матрицы по ее маске в стегоконтейнер, первоначально заполненный отрезком бинарной псевдослучайной последовательности (ПСП) – ГАММЫ, длина которой всегда много больше числа сохраняемых бит. При этом размеры матриц и ГАММЫ выбираются из условия удовлетворения заданного множества сообщений указанному критерию.

Как показано в книге, сформулированные принципы адекватны в строгом смысле (соответствие плюс достаточность) различным приложениям, где требование «жесткой» стилизации объекта распознавания является определяющим и перечень объектов заведомо известен. К ним в полной мере можно отнести анализ защищенных картографических сцен. Сегодня во всем мире широко используются средства пространственного анализа данных органами власти и управления, исследовательскими институтами и др. Содержание цифровых карт далеко не всегда является информацией общего пользования. Требование защиты картографических данных стало особо актуальным с развитием сетевых технологий. Несомненный практический интерес представляет и защищенная идентификация (с целью выявления подделок) по фиксированному множеству фрагментов архивных документов, библиографических редкостей и произведений живописи. В будущем возможно развитие и таких приложений. Оно потребует разработки специальных технических средств бинаризации, немалых затрат ресурсов и творческой энергии на преодоление разного рода препятствий.

Рассматриваемый подход относится к классу вероятностных способов защиты данных [8], но принципиально отличается от известных методов. Так, в наиболее близких, достаточно криптостойких и быстрых, но трудно реализуемых потоковых системах выполняется защита *одиночных* сообщений. Биты открытого текста складываются по mod2 с

битами ГАММЫ, являющейся ключом. Текст восстанавливается путем повторного суммирования по mod2 ключа с полученной шифрограммой. В рассматриваемом же случае основой защиты является различение (противопоставление) сообщений заданного *неединичного* множества. Ключом является набор масок на полном множестве эталонов. Он оставляет истинным ограниченное подмножество бит в каждой бинарной матрице-эталоне со случайным распределением этого подмножества по ее битовой сетке. Размер ключа определяется числом эталонов, размерами матриц и не зависит от объема сообщения.Наличие ГАММЫ никак не сказывается на санкционированном распознавании, но создает непреодолимую преграду для несанкционированного.

При ассоциативной защите картографических сцен, рассматриваемой в этой книге, случайность вносится использованием специальных механизмов пространственной кластеризации объектов, маскирования их бинарных представлений и рандомизации. Предметом защиты в данном случае является набор тематических карт-кластеров как случайно формируемых по карте местности таблиц в терминах «коды объектов – коды координат». Имена и координаты объектов кодируются в цифровом виде. Секретный ключ – случайно сгенерированный набор масок на множестве бинаризованных цифр {0, 1, …, 9}. Кластер охватывает участок местности определенных размеров, выделяемый случайно выбранным объектом – «родителем кластера». Множество кластеров образует картографическую базу данных. Выполнение в «реальном времени» ресурсоемких процедур по ее защите и последующему управлению связывается с использованием вычислительных кластеров в симбиозе с построением соответствующих СУБД [9].

Маскирование – непременный атрибут ассоциативной обработки. В ассоциативных процессорах маски непрерывно формируются с целью выделения своего подмножества активных процессорных элементов для каждой очередной операции. Это определено особенностями ассоциативных алгоритмов [10,11]. При решении задач распознавания стилизованных бинарных изображений роль масок иная. Они могут быть использованы:

1. Для *нейтрализации противодействия санкционированному распознаванию*. Это противодействие является следствием несовершенства систем хранения, передачи или воспроизведения изображений. Но может быть и преднамеренным. Моделируется инверсией несвязанных подмножеств бит изображения, подлежащих маскированию.

2. Для *противодействия несанкционированному распознаванию.* В данном случае внесение случайных искажений в бинарное пред-

ставление объекта становится прерогативой самого пользователя. Здесь уже маскирование – первично, а действие помех – вторично.

Прежде всего, книга призвана ответить на вопрос: насколько ассоциативная стеганография отвечает обоим предназначениям? Оговоренная ранее совершенная секретность (безусловная стойкость) – это всего лишь полезная математическая абстракция, не учитывающая действия возможных атак. Применительно к картографии, логическая трактовка критерия К. Шеннона означает следующее: если число типов объектов по теме равно Т и на рассматриваемой местности с числом градаций координат Г сосредоточено М таких объектов, то в результате несанкционированного распознавания тип каждого из М объектов определится как «любой из Т», а координаты – как «любые из Г». Так что, в математическом плане, метод безусловно стоек независимо от вычислительной сложности полного перебора ключей.

Несмотря на свою абстрактную сущность, это – несомненное методологическое преимущество перед известными методами. На практике, возможные атаки с целью нарушения защиты – «лобовые» (путем полного перебора ключей при точном знании положения некоторых объектов либо характера местности) , «отсутствия» (того или иного объекта), манипулирования стегограммой известного фрагмента сцены, атака на ГАММУ – снижают уровень стойкости от безусловного к доказуемому (непреодолимой вычислительной сложностью). Установлено, что и помехоустойчивость, не в пример другим методам, достаточно высока.

Напомним, к числу наиболее известных методов защиты данных относятся блочные (симметричные и асимметричные) и ранее упомянутые потоковые шифры [12]. Доказуемая стойкость симметричных и потоковых шифров основана на недостижимости полного перебора ключей, асимметричных – на математической сложности обратных преобразований однонаправленных функций [13]. Использование блочных шифров требует выполнения большого числа раундов при шифровании каждого блока для получения нужной стойкости, что обуславливает их меньшее быстродействие в сравнении с потоковыми системами. Они критичны к искажению даже одиночного бита. Здесь уже несомненны преимущества ассоциативного подхода. По быстродействию он должен приближаться к потоковым системам. В частности, маскирование выполняется за один проход текста, последовательно по случайно формируемым кластерам, цифра за цифрой.

О формате книги. Она состоит из 5 разделов. В первых трех излагаются основы теории ассоциативной защиты объектов картографии.

Два последних представляют исследования по созданию систем управления защищенными картографическими базами данных.

Раздел 1 – базовый. В нем излагаются основные положения картографии и ГИС, необходимые для понимания дальнейшего материала. Конкретизируется принятая стратегия защиты. Рассматривается базовый алгоритм маскирования. Анализируются его свойства. Обсуждаются особенности его применения для анализа бинарных сцен.

В *разделе 2* исследуется достижимая стойкость защиты объектов картографии развиваемым методом при действии разного рода атак, связь размеров ключа со стойкостью и вычислительной сложностью метода.

В *разделе 3* анализируется влияние случайных и преднамеренных помех на эффективность правильного распознавания скрытых сообщений. Предлагаются различные методы ослабления этого влияния.

В разделе 4 рассматриваются общие вопросы построения баз данных картографических сцен с ассоциативной защитой (БД КС АЗ). Показывается возможность декомпозиции сложных запросов функционально полной системы на множестве запросов селективного типа. Предлагаются варианты схем точечно-объектных и полнообъектных (включающих точечные, линейные и площадные объекты) БД КС АЗ. Дается обоснование принятой архитектуры СУБД КС АЗ.

В разделе 5 представлены созданные исследовательские прототипы параллельных СУБД КС АЗ. Рассматриваются алгоритмы обработки типовых запросов к серверной части соответствующих СУБД. Показаны принципы организации клиентской части на примере точечных объектов. Дается сравнительная оценка эффективности моно- и мультикластерной организации серверной части полнообъектной СУБД КС АЗ.

В книге систематизированы результаты ранее опубликованных работ авторов. На них даются ссылки после заголовка каждого подраздела. Все они детально обсуждались на Республиканском научном семинаре АН РТ «Методы моделирования» в период с 2001 по 2014 г. (всего по тематике книги было заслушано 25 докладов) и получили положительную оценку. По итогам обсуждений семинар поддержал публикацию монографии. Даты, авторы и названия докладов указаны в приложении «Modelling’ 01-14».

Авторы признательны академику В.К. Левину за его благожелательное отношение к представленным в этой книге исследованиям на всех этапах их развития.

В.А. Райхлин

СОДЕРЖАНИЕ

ЛИТЕРАТУРА

1. Райхлин В.А., Медведев А.С., Мотягин В.Г. Вопросы разработки матричных компиляторов //Вычислительные системы.– Новосибирск: СОАН СССР. 1981. Вып.89. С.69-83.
2. Райхлин В.А. Операционные логико-запоминающие среды. Вопросы применения и синтеза //Автоматика и телемеханика. 1983. № 11. С.161-171.
3. Райхлин В.А., Медведев А.С., Мотягин В.Г., Ильин А.В., Шварцман М.И. К исследованию эффективности комплектования универсальных ЭВМ средней производительности матричными процессорами ассоциативного типа //Управляющие системы и машины. 1985. № 3. С.23-28.
4. Райхлин В.А. Об использовании аппарата двумерного ассоциативного поиска в процессе распознавания /Проблемно-ориентированные средства повышения эффективности вычислительных систем. – Казань: КАИ, 1991. С.38-54.
5. Райхлин В.А. Анализ производительности процессорных матриц при распознавании двоичных образов //Автометрия. 1996. №5. С.97 -103.
6. Стеганография. – http://dic.academic.ru/dic.nsf/ruwiki/30097
7. Shannon C.E. Communication Theory of Secrecy Systems //Bell System Technical Journal. V. 28. 1949. №4. P. 656-715.
8. Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В. Криптография. Скоростные шифры. – СПб: БХВ-Петербург, 2002. – 496 с.
9. Вершинин И.С., Гибадуллин Р.Ф., Пыстогов С.В. Использование кластерных технологий при решении задач защиты картографических данных //Тр. междунар. конф. НРС-2008. – Владимир: Изд. ВГУ, 2009. С. 68-72.
10. Райхлин В.А. Системы параллельной обработки данных. – Казань: Изд. «Фән» (наука), 2010. – 268 с.
11. Фостер К. Ассоциативные параллельные процессоры. – М.: Энергоиздат, 1981. – 240 с.
12. Schneier B. Applied Cryptography, 2nd Edition. – John Wiley & Sons., 1996. – 784 p.
13. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999. – 328 с.
14. Вершинин И.С. Двумерно-ассоциативный механизм защиты бинарных объектов картографии //Эволюционное моделирование /Под. ред. В.А. Райхлина. Тр. Казанского городского семинара «Методы моделирования». Вып.2. – Казань: Изд-во «Фән» («Наука»), 2004. С.73-88.

15. Основы геоинформатики и ГИС-технологий. – Интернет-адрес: http://cnit.pgu.serpukhov.su/win/SEMINAR/PREZ/Sld001.htm
16. Лебедев В.Б., Беркович Е.В. Анализ информационных ресурсов при проектировании ГИС //Новые информационные технологии и системы. Тр. V Междунар. научно-технич. конф. – Пенза, ПГУ, 2002. – С.62-71.
17. ДеМерс М.Н. Географические информационные системы. Основы. – М: Изд-во «Дата+», 1999. – 491 с.
18. Картография. Пособие. – Интернет-адрес: http://kartograff.h1.ru/polka/kniga/index.php
19. Каев А. Системы координат в картографии и геодезии. – Интернет-адрес: http://www.firststeps.ru/gis/geodez/r.php?3
20. Сережников С.В. Геоинформационные системы – что это? – М.: НТФ «Трисофт», 1997. – 327 с.
21. Дьяков Б.Н. Геодезия. Общий курс. – Интернет-адрес: http://www.ssga.ru/metodich/geodesy_ep/index.html
22. Райхлин В.А. Конструктивное моделирование систем. – Казань: Изд-во «Фән» («Наука»), 2005. – 304 с.
23. Райхлин В.А., Вершинин И.С., Гибадуллин Р.Ф. Конструктивное моделирование систем в приложении к защите данных картографии //Методы моделирования /Под. ред. В.А. Райхлина. Тр. Респ. научн. семинара АН РТ «Методы моделирования». Вып.4. – Казань: Изд-во «Фән» («Наука»), 2010. С.68-95.
24. Райхлин В.А., Вершинин И.С. Моделирование процессов двумерно-ассоциативного маскирования распределенных точечных объектов картографии //Нелинейный мир. 2010. Т. 8. № 5. С. 288-296.
25. Ростовцев А.Г., Михайлова Н.В. Методы криптоанализа классических шифров. – М.: Наука, 1995. – 208 с.
26. Райхлин В.А., Вершинин И.С., Глебов Е.Е. К решению задачи маскирования стилизованных двоичных изображений //Вестник КГТУ им. А.Н. Туполева. 2001. №1. С.42-47.
27. Райхлин В.А., Вершинин И.С. Элементы криптоанализа двумерного картографического шифра //Вестник КГТУ им. А.Н. Туполева. 2002. №4. С.48-54.
28. Raikhlin V. A., Vershinin I. S., Gibadullin R. F., and Pystogov S. V. Reliable Recognition of Masked Binary Matrices. Connection to Information Security in Map Systems //Lobachevskii Journal of Mathematics, 2013, Vol. 34, No. 4, pp. 319–325.
29. Райхлин В.А., Вершинин И.С. К оценке сложности двумерного картографического шифра //Вестник КГТУ им. А.Н. Туполева. 2003. №4. С.50-54
30. Дуда Р., Харт П. Распознавание образов и анализ сцен. – М.: Мир, 1976. – 511 с.
31. Ker D.A. A capacity result for batch steganography //IEEE Signal Processing Letters. 2007. V. 14(8). P. 525 -528.

32. What is Mersenne Twister (MT)? Интернет-адрес: http://www.math.sci. hiroshima-u.ac.jp/ ~m-mat/MT/ewhat-is-mt.html
33. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – М.: Государственный Стандарт Российской Федерации, 2001. – 16 с.
34. Вершинин И.С., Гибадуллин Р.Ф., Земцов П.Е. Параллельные алгоритмы защиты бинарных объектов картографии //Методы моделирования /Под ред. В.А. Райхлина. Тр. Респ. научн. семинара АН РТ. – Казань: КГТУ, 2007. Вып.3. С. 96–108.
35. Вершинин И.С. Верхняя оценка числа ключей двумерно-ассоциативной стегозащиты объектов картографии **//**Методы моделирования. /Под ред. В.А. Райхлина. Тр. Респ. научн. семинара АН РТ «Методы моделирования». Вып.4. – Казань: Изд-во «ФЭН» (Наука), 2010. С. 96-100.
36. Вершинин И.С. Стойкость ассоциативной защиты распределенных объектов картографии //Нелинейный мир, №12. Т.9, 2011. Изд-во «Радиотехника». С. 822-825.
37. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие, 2-е изд., испр. и доп. – М., Гелиос АРВ, 2002. – 480 с.
38. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – М.: Издательство ТРИУМФ, 2002. – 816 с.
39. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Госстандарт СССР, 1989. – 28 с.
40. Вершинин И.С. Стойкость ассоциативной защиты к атаке со знанием открытого текста //Вестник Казан. технол. ун-та. 2014. №11. С.218-220.
41. Вершинин И.С. Помехоустойчивость анализа ассоциативно-защищенных картографических сцен при действии случайных помех //Моделирование систем. /Под ред. В.А. Райхлина. Тр. Респ. научн. семинара АН РТ «Методы моделирования». Вып.5. – Казань: Изд-во «Фән» («Наука»), 2013. С.59-70.
42. Элементы теории передачи информации. Интернет-адрес: https://www.msfu.ru/studnet/tpi/lecture/index.htm
43. Р. Морелос-Сарагоса. Искусство помехоустойчивого кодирования – М.: Техносфера, 2006. – 320 с.
44. Семенов Ю.А. Алгоритмы телекоммуникационных сетей. В 3 частях. Часть 1. Алгоритмы и протоколы каналов и сетей передачи данных – М.: ИНТУИТ.РУ, Бином. Лаборатория знаний, 2012. – 620 с.
45. От бумажной карты к ГИС. Опыт векторизации топографических карт в среде Spotlight [Электронный ресурс]. URL: http://www.cadmaster.ru/ magazin/articles/cm_21_spotlight.html.

46. Иванников А.Д., Кулагин В.П., Тихонов А.Н., Цветков В.Я. Геоинформатика. – М.: МАКС Пресс, 2001. – 349 с.
47. Берлянт А.М. Геоинформационное картографирование. – М.: Изд-во Московского университета, 1997. – 64 с.
48. Взаимодействие картографии и геоинформатики /Под ред.А.М. Берлянта, О.Р. Мусина. – М.: Научный мир, 2000. – 192 с.
49. Сербенюк С.Н. Картография и геоинформатика – их взаимодействие /Под ред. В.А. Садовничего. – М.: Изд-во Моск. ун-та, 1990. – 159 с.
50. Цифровая модель местности и ее использование в современных геоинформационных системах [Электронный ресурс]. URL: http: //scbist.dyndns.org.
51. Защита информации в ГИС (с использованием ESRI SDE и Oracle Server) [Электронный ресурс]. Бюро Кадастра Таганрога © 2010. URL: http://www.cbt.ru/news/136-zashhita-informaczii-v-gis-s-ispolzovani -em-esri-sde-i-oracle-server.
52. ArcStorm [Электронный ресурс]. DATA + © 2010. URL: http://www.dataplus.ru/Soft/ESRI/AINFO_UN/ArcStorm.htm.
53. Бабаш А.В., Гольев Ю.И., Ларин Д.А., Шанкин Г.П. Криптография в XIX веке. – М.: «Первое сентября», 2004. С.17–23.
54. Черчхаус Р. Коды и шифры. Юлий Цезарь, «Энигма» и Интернет. /Пер. с англ. – М.: «ВЕСЬ МИР», 2005. – 320 с.
55. MapInfo Professional [Электронный ресурс]. Pitney Bowes Software Inc © 2014. URL: http://www.mapinfo.com.
56. Comparison of raster-to-vector conversion software [Электронный ресурс]. Wikimedia Foundation Inc © 2014. URL: http://en.wikipedia.org/ wiki/List_of_ raster_to_vector_conversion_software.
57. Общие сведения о ГИС Панорама [Электронный ресурс]. Panorama Group © 2014. URL: http://www.gisinfo.ru.
58. Воеводин В.В., Воеводин Вл.В. Параллельные вычисления. – СПб.: БХВ-Петербург, 2004. – 608 с.
59. Калиниченко Л.А., Рывкин В.М. Машины баз данных и знаний. – М.: Наука, 1990. – 296 с.
60. Гибадуллин Р.Ф. Система баз данных картографии с ассоциативной защитой /Автореф. дис. ... канд. техн. наук. Уфа, 2011. – 16 с.
61. Acronis Privacy Expert [Электронный ресурс]. Acronis Inc © 2011. URL: http://www.acronis.ru.
62. Geospatial and location standards [Электронный ресурс]. Open Geospatial Consortium © 2014. URL: http://www.opengeospatial.org.
63. Гибадуллин Р.Ф. Развитие единообразного формализма защиты точечных, линейных и площадных объектов картографии //Вестник КГТУ им. А.Н. Туполева. 2010. №2. С.102–107.

64. Пыстогов С.В. Моделирование процессов в файл-сервере СУБД полнообъектных картографических сцен с ассоциативной защитой //Моделирование систем /Под ред. В.А. Райхлина. Тр. Респ. научн. семинара АН РТ «Методы моделирования». − Казань: «ФЭН» (Наука), 2013. Вып.5. С.100-110.
65. Гибадуллин Р.Ф. Моделирование процессов управления кластерами защищенных картографических баз данных //Методы моделирования /Под ред. В.А. Райхлина. Тр. Респ. научн. семинара АН РТ. – Казань: «ФЭН» (Наука), 2010. Вып. 4. С.101–115.
66. Вершинин И.С., Гибадуллин Р.Ф., Прохоров А.Е. Распределенное управление защищенными картографическими базами данных //Высокопроизводительные параллельные вычисления на кластерных системах. Материалы 8-й Междунар. конф. HPC-2008 – Казань: КГТУ, 2008. С. 216–221.
67. Вершинин И.С., Гибадуллин Р.Ф., Пыстогов С.В. Параллельные СУБД с ассоциативной защитой картографических данных //Высокопроизводительные параллельные вычисления на кластерных системах. Материалы 11-й Междунар. конф. HPC-2011. – Н. Новгород: ННГУ, 2011, С.46-49.
68. Geosample: Открытый набор геоданных для различного ПО ГИС [Электронный ресурс]. GIS-Lab © 2011. URL: http://www.gis-lab.info/ qa/geosample. html.
69. Гибадуллин Р.Ф., Пыстогов С.В. Параллельная система управления полнообъектными защищенными базами данных картографических сцен //Высокопроизводительные параллельные вычисления на кластерных системах. Материалы 12-й Всерос. конф. HPC-2012 – Нижний Новгород: ННГУ, 2012. С. 91–95.
70. Шаши Шекхар, Санжей Чаула. Основы пространственных баз данных. – М.: КУДИЦ-ОБРАЗ, 2004. – 336 с.
71. Бабенко Л.К., Басан А.С., Журкин И.Г., Макаревич О.Б.. Защита данных геоинформационных систем. – М.: Гелиос АРВ, 2010. – 336 с.
72. Гибадуллин Р.Ф., Пыстогов С.В. Клиентская часть системы управления защищенными картографическими базами данных //Материалы 18-й Междунар. научн. конф. «Туполевские чтения» – Казань: КГТУ, 2010. Т.4. С. 97–99.

21.02.01.
В.А. Райхлин, И.С. Вершинин
МАСКИРОВАНИЕ БИНАРНЫХ ИЗОБРАЖЕНИЙ В УСЛОВИЯХ ПРОТИВОДЕЙСТВИЯ

06.02.02.
В.А. Райхлин, И.С. Вершинин
ЭЛЕМЕНТЫ КРИПТОАНАЛИЗА ДВУМЕРНОГО КАРТОГРАФИЧЕСКОГО ШИФРА

16.04. 03.
И.С. Вершинин
К ОЦЕНКЕ СЛОЖНОСТИ ШИФРА ЗАЩИТЫ ТЕМАТИЧЕСКИХ КАРТ GIS

30.10. 03.
И.С. Вершинин
ДВУМЕРНО-АССОЦИАТИВНЫЙ КАРТОГРАФИЧЕСКИЙ ШИФР И МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ЕГО СИНТЕЗА

28.10. 04.
И.С. Вершинин
МОДЕЛИРОВАНИЕ ДВУМЕРНО-АССОЦИАТИВНЫХ МЕХАНИЗМОВ МАСКИРОВАНИЯ СТИЛИЗОВАННЫХ БИНАРНЫХ ИЗОБРАЖЕНИЙ

23.05.07.
И.С.Вершинин, Р.Ф. Гибадуллин, П.Е.Земцов
ПАРАЛЛЕЛЬНЫЕ АЛГОРИТМЫ ЗАЩИТЫ БИНАРНЫХ ОБЪЕКТОВ КАРТОГРАФИИ И ИХ РЕАЛИЗАЦИЯ НА ВЫЧИСЛИТЕЛЬНОМ КЛАСТЕРЕ

26.02.08.
И.С. Вершинин, Р.Ф. Гибадуллин
ПАРАЛЛЕЛЬНАЯ РЕАЛИЗАЦИЯ ЗАЩИЩЕННОЙ ВЕКТОРНОЙ МОДЕЛИ ДАННЫХ ГИС

28.10.08.
Р.Ф. Гибадуллин
РАСПРЕДЕЛЕННОЕ УПРАВЛЕНИЕ ЗАЩИЩЕННЫМИ КАРТОГРАФИЧЕСКИМИ БАЗАМИ ДАННЫХ

10.06.09.
Р.Ф. Гибадуллин, А.Е. Прохоров
МОДЕЛИРОВАНИЕ ПРОЦЕССОВ УПРАВЛЕНИЯ КЛАСТЕРАМИ ЗАЩИЩЕННЫХ КАРТОГРАФИЧЕСКИХ БАЗ ДАННЫХ

25.11.09.
Гибадуллин Р.Ф. (КАИ)
РАЗВИТИЕ ЕДИНООБРАЗНОГО ФОРМАЛИЗМА ЗАЩИТЫ ТОЧЕЧНЫХ, ЛИНЕЙНЫХ И ПЛОЩАДНЫХ ОБЪЕКТОВ КАРТОГРАФИИ

03.03.10.
В.А. Райхлин, И.С. Вершинин, Р.Ф. Гибадуллин
КОНСТРУКТИВНОЕ МОДЕЛИРОВАНИЕ СИСТЕМ В ПРИЛОЖЕНИИ К ЗАЩИТЕ ДАННЫХ КАРТОГРАФИИ

09.06.10.
Р.Ф. Гибадуллин
МОДЕЛИРОВАНИЕ ПРОЦЕССОВ УПРАВЛЕНИЯ ЗАЩИЩЕННО-КАРТОГРАФИЧЕСКИМИ БАЗАМИ ДАННЫХ НА ПЛАТФОРМЕ ВЫЧИСЛИТЕЛЬНЫХ КЛАСТЕРОВ

29.09.10.
Гибадуллин Р.Ф.
МОДЕЛИ, АЛГОРИТМЫ И КОМПЛЕКС ПРОГРАММ ГЕНЕРАЦИИ И АНАЛИЗА ЗАМАСКИРОВАННЫХ СЦЕН КАРТОГРАФИИ

08.06.11.
И.С. Вершинин
СТОЙКОСТЬ АССОЦИАТИВНОЙ ЗАЩИТЫ. СЛУЧАЙ АТАКИ НА ГАММУ

14.12.11.
И.С. Вершинин
УСТОЙЧИВОСТЬ АССОЦИАТИВНОЙ СТЕГОЗАЩИТЫ ДАННЫХ КАРТОГРАФИИ К ПОМЕХАМ ДЕЗИНФОРМАЦИИ В КОРПОРАТИВНОЙ СЕТИ

29.02.12.
И.С. Вершинин
ИЗМЕНЕНИЕ РЕЗУЛЬТАТОВ РАСПОЗНАВАНИЯ НА МНОЖЕСТВЕ ЗАМАСКИРОВАННЫХ БИНАРНЫХ МАТРИЦ ПРИ ДЕЙСТВИИ АДДИТИВНЫХ ПОМЕХ

30.05.12.
С.В. Пыстогов, Р.Ф. Гибадуллин
ПРЕДСТАВЛЕНИЕ ЗАЩИЩЕННЫХ ДАННЫХ КАРТОГРАФИЧЕСКИХ СЦЕН С ПРИМЕНЕНИЕМ ВЫЧИСЛИТЕЛЬНЫХ КЛАСТЕРОВ

04.10.12.
И.С. Вершинин
ПОМЕХОУСТОЙЧИВОСТЬ РАСПОЗНАВАНИЯ СТИЛИЗОВАННЫХ БИ-

НАРНЫХ ИЗОБРАЖЕНИЙ ЗАДАННОГО МНОЖЕСТВА ПО ДИХОТОМАЛЬНЫМ ТРОИЧНЫМ ЭТАЛОНАМ. ***Часть 1***

27.12.12.

С.В. Пыстогов

ПРИНЦИПЫ ОРГАНИЗАЦИИ СЕРВЕРНОЙ ЧАСТИ УНИВЕРСАЛЬНОЙ СУБД КАРТОГРАФИЧЕСКИХ СЦЕН С АССОЦИАТИВНОЙ ЗАЩИТОЙ

16.05.13.

И.С. Вершинин

ПОМЕХОУСТОЙЧИВОСТЬ РАСПОЗНАВАНИЯ СТИЛИЗОВАННЫХ БИНАРНЫХ ИЗОБРАЖЕНИЙ ЗАДАННОГО МНОЖЕСТВА ПО ДИХОТОМАЛЬНЫМ ТРОИЧНЫМ ЭТАЛОНАМ. ***Часть 2***

30.05.13.

С.В. Пыстогов

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ В ФАЙЛ-СЕРВЕРЕ СУБД ПОЛНООБЪЕКТНЫХ КАРТОГРАФИЧЕСКИХ СЦЕН С АССОЦИАТИВНОЙ ЗАЩИТОЙ. *Часть 1*

06.11.13.

С.В. Пыстогов

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ В ФАЙЛ-СЕРВЕРЕ СУБД ПОЛНООБЪЕКТНЫХ КАРТОГРАФИЧЕСКИХ СЦЕН С АССОЦИАТИВНОЙ ЗАЩИТОЙ. *Часть 2*

20.11.13.

И.С. Вершинин

ИЗМЕНЕНИЕ УРОВНЯ СТОЙКОСТИ АССОЦИАТИВНОЙ ЗАЩИТЫ КАРТОГРАФИЧЕСКИХ СЦЕН ПРИ СНИЖЕНИИ КРИТИЧНОСТИ РАСПОЗНАВАНИЯ К ДЕЙСТВИЮ ПОМЕХ

23.04.2014.

С.В. Пыстогов

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ В ФАЙЛ-СЕРВЕРЕ СУБД ПОЛНООБЪЕКТНЫХ КАРТОГРАФИЧЕСКИХ СЦЕН С АССОЦИАТИВНОЙ ЗАЩИТОЙ. *Часть 3*

21.05.2014.

И.С. Вершинин

ПОМЕХОУСТОЙЧИВОСТЬ АНАЛИЗА АССОЦИАТИВНО-ЗАЩИЩЕННЫХ БИНАРНЫХ СЦЕН КАК ТАКОВЫХ

Научное издание

Игорь Сергеевич Вершинин, Руслан Фаршатович Гибадуллин,
Сергей Васильевич Пыстогов, Вадим Абрамович Райхлин

АССОЦИАТИВНАЯ СТЕГАНОГРАФИЯ
/Приложение к анализу сцен/

Под редакцией В.А. Райхлина

Подписано в печать 10.10.2014.
Формат 60 x 90 1/16. Бумага для офисной техники.
Печ.л. 8,25. Усл.печ.л. 7,7. Усл.кр.-отт. 7,7. Уч.-изд.л. 8.
Тираж 100.

Издательство Казанского университета
420008, г. Казань, ул. Профессора Нужина, 1/37
тел. (843) 233-73-59, 233-73-28

Отпечатано с готового оригинал-макета
в типографии ООО «Фолиантъ»
г. Казань, ул. Дементьева, 1А4

ISBN 978-5-00019-284-9