МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ

ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ
РАДИОЭЛЕКТРОНИКИ

ISSN 1563-0064

РАДИОЭЛЕКТРОНИКА И ИНФОРМАТИКА

Научно-технический журнал **Основан в 1997 г.**

№ 4(71), октябрь – декабрь 2015 **Выходит 4 раза в год**

Свидетельство о государственной регистрации КВ № 12097-968 ПР 14.12.2006

РИ, 2015, № 4

СОДЕРЖАНИЕ

УДК004:519.713

КВАНТОВЫЙ КОМПЬЮТИНГ ДЛЯ ПРОЕКТИРОВАНИЯ ЦИФРОВЫХ СИСТЕМ

ЛИТВИНОВА Е.И., ХАХАНОВ И.В.

Предлагается квантовый подход к проектированию цифровых устройств, который характеризуется использованием элементов памяти для реализации транзакционного взаимодействия всех компонентов операционного и управляющего автоматов, а также методами синтеза и анализа, основанными на суперпозиции кубит-векторных примитивов задания всех типов функциональностей, имплементируемых в элементы памяти, что дает возможность существенно (2-3 раза) повысить быстродействие средств моделирования.

1. Современное определение компьютинга

Цель исследования – существенное уменьшение времени проектирования, верификации цифровых систем и повышение их качества за счет повышения быстродействия интерпретативного моделирования путем использования квантового подхода к синтезу структур данных и процессоров, обеспечивающих инновационные решения. Задачи исследования: 1) Современное определение компьютинга. 2) Перспективы квантового компьютинга. 3) Квантовые структуры данных. 4) Квантовое моделирование цифровых систем. 5) Примеры анализа фрагментов цифровых устройств.

Наиболее значимые рыночно-ориентированные инновации ученые делают путем использования модели компьютинга для мониторинга и управления процессами и явлениями во всех областях деятельности человека и природы. Подтверждением сказанному могут служить модные глобальные технологии и бренды, масштабирующие модели компьютинга: 1) Cyber-Physical Systems. 2) Internet of Things and Everything. 3) Veb-, Cloud-, Mobile-, Service-, Network-, Automotive-, Big Data-, and Quantum- computing. 4) Smart Objects and Infrastructure: Enterprise, University, City, and Government. Компьютинг – замкнутая масштабируемая система мониторинга и управления процессами и явлениями для достижения поставленной цели. Развитие компьютинга имеет четыре выраженных фазы: 1) Сингулярный компьютинг. 2) Сетевой компьютинг. 3) Глобальный компьютинг. 4) Киберфизический компьютинг.

2. Перспективы квантового компьютинга

Компьютер – память, в которой реализуются адресные транзакции (считывание-запись) данных. Вселенная как компьютер: гравитационно-структурированная материя – память, на которой реализуются фотонные транзакции. Иначе, гравитационно-взаимодействующие материальные структуры способны принимать и испускать энергетические потоки квантов или фотонов. Электрон имеет квантовую неопределенность в практически одной точке физического и математического пространства. В этом его уникальное преимущество. Получив фотон или квант, он приобретает более высокую орбиту, которую можно интерпретировать как единицу. Отдав фотон, он опускается на уровень ниже, что можно отождествить со значением нуля. Трудно придумать более компактный компьютер, чем тот, который использует для кодирования двоичных состояний энергетический уровень электрона. Учитывая, что вся материя состоит из атомов, а значит – из электронов, человечество имеет возможность реализовать (квантовый) компьютер [1] в любой субстанции: жидкая, твердая, газообразная и плазменная. Плазменная реализация компьютера является более предпочтительной, поскольку здесь имеют место в чистом виде облака свободных электронов, отделенных от атомов, которые следует структурировать в пространственно-устойчивую вычислительную среду. Здесь бы пригодился базон Хиггса. Относительно трех других субстанций проблема заключается в том, чтобы научиться в реальном времени и достаточно быстро выращивать компьютеры из атомов, используя алгоритмы на основе безотходной технологии. Масштабируемость выращиваемых компьютеров предоставляет возможность изготавливать для рынка нано-компьютеры в размере клетки и супервычислители для массовых параллельных транзакций в киберпространстве больших данных. Это наше недалекое будущее. Однако уже сегодня можно и нужно использовать преимущества квантового компьютинга [2] в классических вычислителях. В этом случае неопределенность будет представлена двумя битами или двумя точками физического пространства. Идеальной демонстрацией изоморфизма "квантовых" структур данных и квантовых обозначений механики Дирака является алфавит и алгебра Кантора. В последней символы алфавита A = {0, 1, X = {0,1}, U} кодируются двоичными векторами (10, 01, 11, 00) соответственно. Свойство перепутывания отождествляется с неопределенностью состояния X, которое задает в математической точке пространства одновременное существование 0 и 1. Свойство суперпозиции связано с выполнением операции дизъюнкции над символами алфавита Кантора или его кодами. Свойство параллелизма основано на выполнении регистровых операций (И, ИЛИ, НЕ) над квантовыми структурами данных. Свойство осведомленности (телепортации) использует операцию отрицания или инверсии, когда каждое из двух состояний знает друг о друге все и на любом расстоянии. Существует изоморфизм между квантовой механикой Дирака и алгеброй Кантора, которая имеет символ двоичной неопределенности. Наряду с совершенствованием технологии исполнения квантового компьютера, необходимо параллельно разрабатывать новые квантовые подходы программирования затратных алгоритмов для решения оптимизационных задач.

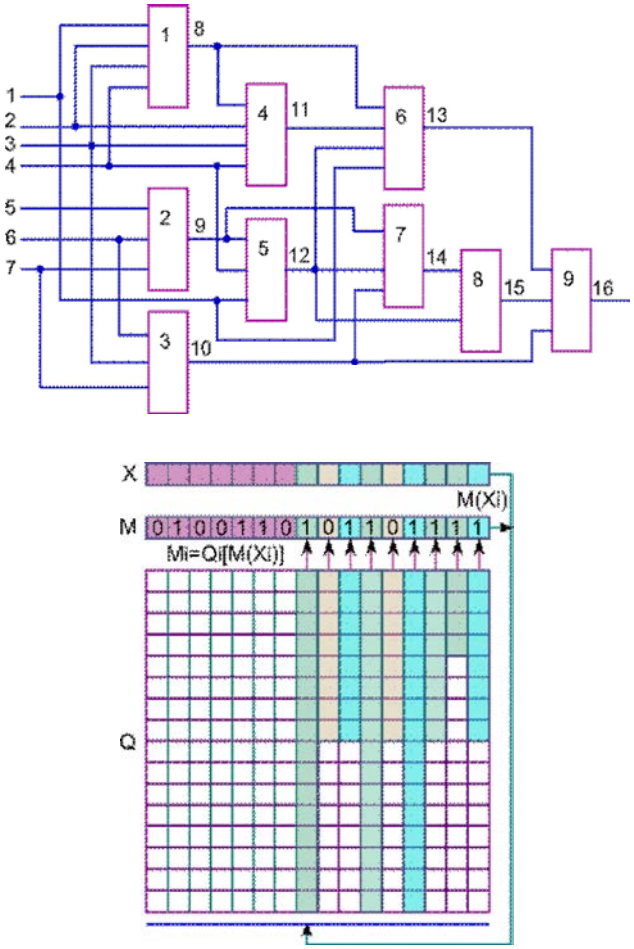
3. Квантовые структуры данных

Кубит (*n*-кубит) [3] это векторная форма унитарного кодирования универсума из *n* примитивов для задания

булеана состояний 2^{2^n} с помощью 2^n двоичных переменных. Например, если n=2, то 2-кубит задает 16 состояний с помощью четырех переменных. Если n=1, то кубит задает четыре состояния на универсуме из двух примитивов (10) и (01) с помощью двух двоичных переменных (00,01,10,11) [1,10]. При этом допускается суперпозиция (одновременное существование) в векторе 2^n состояний, обозначенных примитивами. Кубит (n-кубит) дает возможность использовать параллельные логические операции квантового процессора вместо поэлементных теоретико-множественных для существенного ускорения процессов анализа цифровых проектов. Квантовый процессор может быть любой конечной размерности: вектор, матрица, куб. Для структуры, содержащей два измерения, он представлен матрицей столбцов или Q-векторов, которые формируют соответствующие им ячейки M-вектора моделирования (рис. 1). Вектор M, совместно с X-вектором кортежей входных переменных примитивов создает структуру взаимных связей между столбцами-элементами. Адрес ячейки Q-покрытия, формирующей состояние невходного i-разряда M-вектора, определяется содержимым ячеек M-вектора, найденным по адресам, заданным i-кортежем вектора входных переменных. Каждый вектор Qi, равно как и кортеж Xi вектора номеров входных линий, имеет адресную связь с Mi-ячейкой вектора моделирования. Квантовый процессор может входить компонентом в состав более сложной системы. Квантовая модель процессора имеет следующую структуру.

В аналитической модели W (см. рис. 1) представлены [4]: 1) Упорядоченная адресно-доступная Q-совокупность квантовых примитивов, формирующих функциональность системы. 2) Вектор моделирования M, связывающий все примитивы в единую систему на основе идентификации эквипотенциальных линий, которые создают формат из существенных переменных: входных, внутренних и выходных. 3) Вектор X кортежей упорядоченных номеров входных переменных для каждого квантового примитива, которые формируют адреса доступа к ячейкам Q-векторов примитивов. Вектор количества входных переменных примитива $|X|$ формирует адресное пространство или длину каждого Q-покрытия.

Аксиомы квантового (only memory-based) процессора [5-7]: 1) В квантовом процессоре нет ничего, кроме адресуемой памяти. 2) Вычислительный процесс представлен единственной универсальной транзакцией между адресуемыми компонентами памяти Mi = Qi[M(Xi)]. 3) Транзакция есть универсальная процедура считывания-записи данных на непустом множестве адресуемых элементов памяти. 4) Все компоненты памяти являются online-repaired, благодаря их адресной связности. 5) Комбинационные логические элементы (reusable logic), равно как и последовательностные (sequential components), исполняются на элементах памяти. 6) Связывание всех компонентов в вычислительную систему осуществляется посредством (цифровой) идентификации псевдо-гальванических соединений вход-выходных переменных компонентов схемы, формирующих вектор моделирования, который хранит состояния всех существенных линий цифровой системы. 7) Все компоненты квантовой модели цифровой системы: W=<Q,M,X>, включая функциональные модули, вектор моделирования, вектор адресов входных переменных, являются online перепрограммируемыми, а значит – online ремонтопригодными. 8) Примитив цифровой системы имеет формат W=<Q,Y,X>, поскольку отдельный элемент не имеет связей и вектора M, создающих из отдельных компонентов систему.



$$W(\,(\,Q,M,X\,(,$$
$$Q\,(\,(Q_1,Q_2,\ldots,Q_i,\ldots,Q_n),$$
$$Q_i\,(\,(Q_{i1},Q_{i2},\ldots,Q_{ij},\ldots,Q_{ik_i});$$
$$M\,(\,(M_1,M_2,\ldots,M_i,\ldots,M_n);$$
$$X\,(\,(X_1,X_2,\ldots,X_i,\ldots,X_n),$$
$$X_i\,(\,(X_{i1},X_{i2},\ldots,X_{ij},\ldots,X_{im_i});$$
$$M_i\,(\,Q_i[M(X_i)];\ k_i\,(\,2^{m_i}.$$

Рис. 1. Схема, кубитные структуры данных и модель квантового процессора

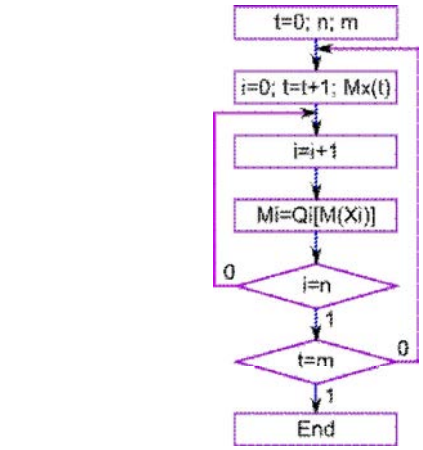
4. Квантовое моделирование цифровых систем

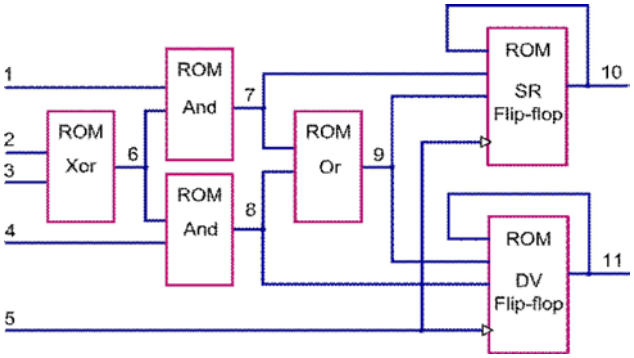
Использует memory-based only модели для адресного анализа цифровых систем в целях их верификации.

Реализация таких структур связана с ячейками памяти (LUT (Look Up Table) FPGA), которые способны хранить информацию в виде Q-вектора, где каждый бит или разряд имеет свой адрес, отождествляемый с входным словом. Программная реализация алгоритма моделирования таких структур становится конкурентоспособной по быстродействию на рынке проектирования цифровых систем на кристаллах за счет адресации функциональных примитивов. Одномерный Q-вектор описания функциональности можно привязать к выходной (внутренней) линии устройства, состояние которой формируется в процессе моделирования рассматриваемого Q-покрытия. Тогда регистровая реализация комбинационного устройства может быть представлена вектором моделирования M, невходные линии которого непосредственно связаны с выходами функциональных элементов. Упорядоченные значения входных переменных задают адрес бита Q-вектора, формирующего состояние рассматриваемой невходной линии. Если функциональности описываются одновыходовыми примитивами, то каждый из них можно отождествить с номером или координатой невходной линии, на которую нагружен данный элемент. Если функциональность многовыходовая, то Q-покрытие представляется матрицей с числом строк, равным числу выходов. Эффект от такого примитива заключается в параллелизме одновременного вычисления состояний нескольких выходов за одно обращение к матрице по текущему адресу. Данное обстоятельство является существенным аргументом в пользу синтеза обобщенных кубитов для фрагментов цифрового устройства или всей схемы в целях их параллельной обработки на одном временном такте. Модель функционирования цифровой структуры упрощается до вычисления двух адресов при формировании вектора моделирования $M_i = Q_i[M(X_i)]$ путем исключения сложного адреса выхода примитива в процессе записи состояний выходов в координаты M-вектора. Алгоритм моделирования квантовых примитивов цифровой схемы представлен на рис. 2 [8].

0) Инициирование начальных условий и параметров. 1) Задание очередного набора двоичных состояний на входных координатах вектора моделирования. 2) Определение i-номера очередного обрабатываемого примитива путем выполнения операции инкрементирования. 3) Выполнение процедуры конкатенации состояний битов M-вектора, соответствующих номерам вектора входных переменных Xi. Считывание соответствующего бита из кубит-покрытия Qi по двоичному вектор-адресу сконкатенированных битов M-вектора. Занесение считанного из кубита бита в вектор моделирования M по адресу i. (M-вектор может иметь координаты с символами X, что дает возможность выполнять троичное моделирование цифровых устройств для решения задач тестирования и верификации.) 4) Если не все примитивы обработаны i<n, выполняется переход к пункту 2 алгоритма. 5) Если не все входные наборы обработаны t<m, выполняется переход к пункту 1. 6) Конец моделирования.

На рис. 2 представлена схема с триггерами и комбинационной логикой, которая также описана в виде элементов памяти, куда занесены выходные состояния таблицы истинности каждого логического элемента. Структуры данных, необходимые для моделирования цифрового устройства, сведены в таблицу, где основными компонентами являются: M – вектор моделирования или состояния занумерованных линий, который в данном случае имеет 5 входных, 6 внутренних и выходных линий, состояния которых подлежат определению; X – вектор кортежей номеров входных линий примитивов, которые необходимы для формирования адреса в целях извлечения по нему состояния выхода элемента Qi, функциональность которого задается Q-вектором. Все примитивы схемы должны быть упорядочены по принципу: очередной элемент анализируется, если все предшественники для него были обработаны.





L	1	2	3	4	5	6	7	8	9	10	11
M	0	0	1	1	1	1	0	1	1	1	1
X	.	.	.	.	.	2	1	6	7	10	11
	.	.	.	.	.	3	6	4	8	7	9
	.	.	.	.	.	.	.	.	.	9	8
Q	.	.	.	.	.	0	0	0	0	1	0
	.	.	.	.	.	1	0	0	1	1	1
	.	.	.	.	.	1	0	0	1	1	0
	.	.	.	.	.	0	1	1	1	1	0
	.	.	.	.	.	.	.	.	.	0	0
	.	.	.	.	.	.	.	.	.	0	1
	.	.	.	.	.	.	.	.	.	0	1
	.	.	.	.	.	.	.	.	.	1	1

Рис. 2. Алгоритм моделирования и пример цифровой схемы с триггерами

В процессе моделирования адресно-извлеченное состояние ячейки текущего Q-покрытия заносится в разряд Mi вектора моделирования. Результаты после-

довательной обработки всех Q-векторов схемной структуры формируют состояния линий М-вектора для приведенного выше примера ячейки (6 – 11). Первоначальные состояния неопределенностей на псевдовходах функциональных примитивов доопределяются сигналами нуля или единицы в зависимости от внутренней технологической культуры компании, предоставляющей промышленные средства моделирования и верификации. Количество входных переменных примитива q связано с длиной Q-вектора соотношением: card(Q) (2^q. Правильность работы алгоритма моделирования была верифицирована на тестовых и реальных схемах с привлечением средств Active HDL 9.1 (Aldec Inc.). Особенность структурно-функционального задания цифровой системы заключается в представлении всех примитивов элементами памяти, куда записываются Q-векторы выходных состояний. Выводы: 1) Любые структурные компоненты вычислительных устройств, комбинационные и/или последовательностные, а также системы в целом можно описывать кубитными Q-векторами и реализовывать в элементах памяти FPGA, CPLD или VLSI. 2) Memory-based интерпретативное адресно-ориентированное моделирование комбинационных и последовательностных примитивов цифровых устройств становится соизмеримым по быстродействию с компилятивным анализом дискретных объектов.

5. Заключение

Предложен квантовый подход к проектированию цифровых устройств, который характеризуется: 1) Использованием элементов памяти для реализации транзакционного взаимодействия всех компонентов операционного и управляющего автоматов. 2) Методами синтеза и анализа, основанными на суперпозиции кубит-векторных примитивов задания всех типов функциональностей, имплементируемых в элементы памяти, что дает возможность существенно (в 2-3 раза) повысить быстродействие средств моделирования. Практическая значимость квантового синтеза и анализа цифровых систем: 1) Реализация процессора только на основе использования элементов памяти делает возможным ремонт в режиме online за счет применения на кристалле универсальных адресуемых spare-компонентов памяти. 2) Имплементация квантовых only memory-based моделей описания цифровых компонентов и систем непосредственно связана с увеличением выхода годной продукции, повышением надежности вычислительных изделий, снижением стоимости проектирования и изготовления, автономным online восстановлением работоспособности без участия человека [9,10].

Литература: 1. *Stenholm Stig, Kalle-Antti Suominen.* Quantum approach to informatics. John Wiley & Sons, Inc. 2005. 249p. **2.** *Литвинова Е.И., Хаханов И.В., Сергиенко В.* Синтез и анализ «квантовых» моделей цифровых систем // АСУ и приборы автоматики. 2015. Вып. 172. С. 56-70. **3.** *Hahanov V.I., Wajeb Gharibi, Litvinova E.I., Shkil A.S.* Qubit data structure of computing devices // Electronic modeling. № 1. 2015. P.76-99. **4.** *Hahanov V.I., Tamer Bani Amer, Chumachenko S.V., Litvinova E.I.* Qubit technology analysis and diagnosis of digital devices. “Electronic modeling.” Volume 37, № 3. 2015. P. 17-40. **5.***Vladimir Hahanov, Tamer Bani Amer, Ivan Hahanov*. MQT-model for Virtual Computer Design // Microtechnology and Thermal Problems in Electronics. 2015. P. 182-185. **6.** *Ivan Hahanov, Tamer, Irina Hahanova, Sergey Dementiev.* Automaton MQT-model for Virtual Computer Design. CADSM, Polyana, Ukraine. 2015. P.27-31. **7.** *Хаханов В.И., Обризан В.И., Зайченко С.А., Хаханов И.В*. MQT-автомат для анализа больших данных // АСУ и приборы автоматики. Вып. 168. 2014. С. 64-72. **8.***Хаханов В.И., Зайченко С.А., Мищенко А.С., Хаханов И.В.* Процессорные структуры для анализа Big Data // АСУ и приборы автоматики. Вып.169. 2014. С. 4-15. **9.***Wajeb Gharibi, Vladimir Hahanov, Eugenia Litvinova, Ivan Hahanov.* «Quantum» Structures for Digital Systems Synthesis // IEEE East-West Design & Test Symposium. Batumi. 2015. P. 115-122. **10.** *Vladimir Hahanov, Igor Yemelyanov, Volodymyr Obrizan, Ivan Hahanov.* “Quantum” Diagnosis and Simulation of SoC // XIth Intern. Conf. MEMSTECH-2015. P. 58-60.

Транслитерированный список литературы: 1. *Stenholm Stig, Kalle-Antti Suominen.* Quantum approach to informatics. John Wiley & Sons, Inc. 2005. 249p. **2.** *Litvinova E.I., Hahanov I.V., Sergienko V.* Sintez i analiz «kvantovyh» modelej cifrovyh sistem // ASU i pribory avtomatiki. Vyp. 172. 2015. S. 56-70. **3.** *Hahanov V.I., Wajeb Gharibi, Litvinova E.I., Shkil A.S.* Qubit data structure of computing devices // Electronic modeling. № 1. 2015. P.76-99. **4.** *Hahanov V.I., Tamer Bani Amer, Chumachenko S.V., Litvinova E.I.* Qubit technology analysis and diagnosis of digital devices. “Electronic modeling.” Vol. 37, № 3. 2015. P. 17-40. **5.***Vladimir Hahanov, Tamer Bani Amer, Ivan Hahanov*. MQT-model for Virtual Computer Design // Microtechnology and Thermal Problems in Electronics. 2015. P. 182-185. **6.** *Ivan Hahanov, Tamer Bani Amer, Irina Hahanova, Sergey Dementiev.* Automaton MQT-model for Virtual Computer Design. CADSM, Polyana, Ukraine. 2015. P.27-31. **7.** *Hahanov V.I., Obrizan V.I., Zajchenko S.A., Hahanov I.V.* MQT-avtomat dlja analiza bol'shih dannyh // ASU i pribory avtomatiki. Vyp. 168. 2014. S. 64-72. **8.***Hahanov V.I., Zajchenko S.A., Mishhenko A.S., Hahanov I.V.* Processornye struktury dlja analiza Big Data // ASU i pribory avtomatiki. №.169. 2014. S. 4-15. **9.***Wajeb Gharibi, Vladimir Hahanov, Eugenia Litvinova, Ivan Hahanov.* «Quantum» Structures for Digital Systems Synthesis // IEEE East-West Design & Test Symposium. Batumi. 2015. P. 115-122. **10.** *Vladimir Hahanov, Igor Yemelyanov, Volodymyr Obrizan, Ivan Hahanov.* “Quantum” Diagnosis and Simulation of SoC // XIth Intern. Conf. MEMSTECH-2015. P. 58-60.

Поступила в редколлегию 10.12.2015

Литвинова Евгения Ивановна, д-р техн. наук, профессор кафедры АПВТ ХНУРЭ. Научные интересы: техническая диагностика цифровых систем, сетей и программных продуктов. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. +380 57 70-21-326. E-mail: kiu@kture.kharkov.ua.

Хаханов Иван Владимирович, студент факультета компьютерной инженерии и управления ХНУРЭ. Научные интересы: техническая диагностика цифровых систем, программирование. Увлечения: горные лыжи, английский язык. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. +380 57 70-21-326.

РЕФЕРАТИ

УДК 621.396.933.21, 621.396.33:528.

Оцінка вологості повітря методом радіо акустичного зондування по загасанню акустичних хвиль / Ч. Лю, О.Ю. Панченко, Ю.М.Ульянов // Радіоелектроніка та інформатика. 2015. № 4. С. 3-8.

Проаналізовано дистанційні способи вимірювання вологості повітря. Як первинна інформація в них використано результати вимірювань покажчика заломлення для радіохвиль або загасання і дисперсії звукових хвиль. Розглянуто один з варіантів вимірювання загасання радіоакустичним методом з використанням подвійної звукової посилки. Показано його переваги, проведено попередній аналіз. Розглянуто питання практичної реалізації.

Іл. 3. Бібліогр.: 17 назв.

УДК 621.327:681.5

Метод криптосемантичного представлення зображень на основі плаваючої схеми в базисі по верхніх границях / В.В. Бараннік, І.М. Тупиця, С.О. Сідченко // Радіоелектроніка та інформатика. 2015. № 4. С. 9-12.

Розроблено метод криптосемантичного представлення зображень на основі плаваючої схеми системи поліадичного кодування в базисі по верхніх границях. Даний метод забезпечує: одночасне виконання процесів стиснення і шифрування (кодування) відеоданих; виключення надмірності одночасно без внесення похибки; зменшення кількості незначущих елементів (незначущих нульових біт) на початку кожної бітової послідовності кодів-номерів; формування кодограм рівномірної довжини на основі змінної (заздалегідь невизначеної) кількості елементів вихідного зображення; додаткове зниження початкового об'єму зображень.

Бібліогр.: 9 назв.

УДК 621.3

Модель оцінки цілісності динамічного відеоінформаційного ресурсу у випадку міжтрансформантної обробки / В.В.Бараннік, С.С.Шульгін // Радіоелектроніка та інформатика. 2015. № 4. С. 13-18.

Обґрунтована необхідність підвищення безпеки динамічних відеоінформаційних ресурсів. Показано напрямок для підвищення ефективності синтаксичного представлення послідовності Р-кадрів на основі міжтрансформантної обробки їх базових структурних одиниць – диференціально-описаних спектрограм. Розкрито напрямок додаткового зниження інтенсивності кодового представлення відеопотоку шляхом скорочення міжкадрової (тимчасової) психовизуальної надлишковості на рівні обробки диференціально-описаних спектрограм. Викладено етапи побудови моделі оцінки цілісності динамічного відеоінформаційного ресурсу шляхом знаходження нижньої межі пікового відношення сигнал-шум реконструйованих диференціально-описаних спектрограм відносно вихідних з урахуванням процесу інтерполяції.

Іл. 3. Бібліогр.: 5 назв.

ABSTRACTS

UDC 621.396.933.21; 621.396.33:528

For the estimation of air humidity with radio-acoustic sounding method by the attenuation of acoustic waves / Ch Liu, A.Yu. Panchenko, Y.N. Ulianov // Radioelektronika i informatika. 2015. N 4. P. 3-8.

The paper analyzes remote methods of measuring humidity. As the primary information they use the results of measuring the refractive index of radio waves or attenuation and dispersion of sound waves. One of the variants of radioacoustic method for measuring attenuation when using a double sound parsel is considered. It is showed its advantages and performed the preliminary analysis. Practical implementation questions are also examined.

Fig. 3. Ref.: 17 items.

UDC 621.327:681.5

The Method of Crypto-Semantic Presentation of Images Based on the Floating Scheme in the Basis of the Upper Boundaries / V.V. Barannik, I.M. Tupitsya, S.A. Sidchenko // Radioelektronika i informatika. 2015. N 4. P. 9-12.

Method of crypto-semantic images presentation based on a floating circuit system of polyadic coding in the upper boundaries basis is worked out. The developed method provides: concurrent compression execution and encryption (coding) of video data; redundancy elimination at the same time without making an error; reducing the amount of irrelevant elements (insignificant zero bits) at the beginning of each code-bit sequence of code numbers; a uniform length formation of the codegrams by variable (unspecified beforehand) original image number of elements; a further original image volume reduction.

Ref.: 9 items.

UDC 621.3

Model of the assessment of integrity of the dynamic video information resource in case of intertransformantal processing / V.V. Barannik, S.Shulgin // Radioelektronika i informatika. 2015. N 4. P. 13-18.

Need of dynamic video information resources increase in safety is justified. The direction for increase in syntactic representation efficiency of the P-frames sequence on the basis of intertransformantal processing of their basic structural units – the differential described spectrograms is shown. The additional direction lowering in intensity of a video stream code representation by interframe (temporal) psychovisual redundance reduction of differential described spectrograms reveals that is caused by limited sensitivity features of visual system concerning separate frequency components correction. Creation stages of a dynamic video information resource integrity assessment model by signal noise peak relation of the differential described spectrograms lower bound finding rather initial taking into account interpolation process are explaned.

Fig. 3. Ref.: 5 items.

УДК 681.3

Технологія формування кодової конструкції для селективного методу обробки відеоданих / Д.І. Комолов // Радіоелектроніка та інформатика. 2015. № 4. С.19-23.

Розглянуто селективний метод шифрування відеокадрів, заснований на закритті базового І-кадру. Розроблено технологію формування кодової конструкції для селективного методу обробки відеоданих. Описано технологію формування бітового коду в селективному методі шифрування відеоінформаційного ресурсу з урахуванням енергетично значущих структурних одиниць базового відеокадру.

Іл. 1. Бібліогр.: 4 назви.

УДК 519.713

Додатні розв'язки для еліптичного рівняння з двома параметрами/ В.С. Луханін // Радіоелектроніка та інформатика. 2015. № 4. С. 24-27.

Розглянуто питання існування, єдиності та побудови двосторонніх наближень до додатного розв'язку однієї лінійної еліптичної крайової задачі з двома параметрами. Отримано умови, яким мають задовольняти параметри, щоб можна було довести існування та єдиність додатного розв'язку, а також побудувати двосторонні наближення, які до нього збігаються. Обчислювальний експеримент проведено у крузі та півкрузі для різних значень параметрів, результати представлено у вигляді графіків поверхні наближення та ліній рівня, а також у вигляді таблиці.

Табл. 2. Іл. 4. Бібліогр.: 4 назви.

УДК 510.582

Використання машини Тьюринга для розв'язання криптографічної задачі поліноміальної складності / О.О. Петрова, Р.В. Бурменський// Радіоелектроніка та інформатика. 2015. № 4. С. 28-31.

Запропоновано модель процесу обчислення на детермінованій однострічковій машині Тьюринга для реалізації симетричного алгоритму шифрування з використанням полібіанського квадрату. Наведено етапи кодування даних та програма, що моделює роботу МТ для рішення задачі криптографії. Побудовано модель детермінованого алгоритму та програмне забезпечення, що надає можливість доведення існування або неіснування алгоритмів розв'язання задач.

Іл. 4. Бібліогр.: 9 назв.

UDC 681.3

Technology of forming of code construction for the selective method of treatment of videoinformation / D.I. Komolov // Radioelektronika i informatika. 2015. N 4. P. 19-23.

Under consideration is selective encryption method of video frames, which is based on the basic I-frame covering. This method is based on the processing of the frames group, with an accounting of the MPEG algorithm, which is implemented on the principle, which is forming an order, which has different types of video frames. On its foundation it has been developed a technology for a code structure forming for the selective method of processing video data. Also, it has been reached a development for the technology of the bit code, in the method of video information selective encryption resource, which is based on energy-relevant structural units of the basic video frame. It allows you to calculate the bandwidth of a secured video communication channel which is based on the encrypted bits' stream and open structural units' intensity.

Fig. 1. Ref.: 4 items.

UDC 519.713

On the construction of two-sided approximations of some linear elliptic boundary value problem / V.S. Lukhanin // Radioelektronika i informatika. 2015. N 4. P. 24-27.

In this paper the existence, uniqueness and possibility of constructing of two-sided approximations to the positive solution of the linear elliptic boundary problem with two parameters are considered. Conditions that the parameters must satisfy to prove the existence and uniqueness of the positive solution are obtained. The conditions guarantee that two-sided approximations converge to the solution of the problem. The computational experiment is performed in disk and halfdisk for different values of the parameters, the results of the experiment are presented as plots of approximate solution surface and level lines and also as a table.

Tab. 2. Fig. 4. Ref.: 4 items.

UDC 510.582

Using the Turing machine to solve cryptographic task polynomial complexity / E.A. Petrova, R.V. Burmensky /// Radioelektronika i informatika. 2015. N 4. P. 28-31.

A model of the process to calculate the deterministic tape Turing machine to implement a symmetric encryption algorithm using Polybius square. Here given the steps of encoding data and a program that simulates the MT work to solve cryptographic tasks. The constucted model of deterministic algorithm and software make it possible to proof the existence or nonexistence of algorithms for solving problems.

Fig. 4. Ref.: 9 items.

УДК 621.39

Метод локалізації втрати цілісності інформації на основі слот-технології / В.В. Бараннік, С.А. Підлісний, Д.В. Бараннік // Радіоелектроніка та інформатика. 2015. № 4. С. 32-41.

Показана проблематичність забезпечення інформаційної безпеки державного відеоінформаційного ресурсу. Розглянуто основні недоліки статистичного кодування при обробці відео в разі застосування кібератак. Обґрунтовано необхідність розробки технології розподілу кодів змінної довжини для відеопотоку. Сформовано механізм локалізації втрати цілісності інформації.

Іл. 14. Бібліогр.: 8 назв.

УДК 004:519.713

Квантовий комп'ютинг для проектування цифрових систем / Є.І. Литвинова, І.В. Хаханов // Радіоелектроніка та інформатика. 2015. № 4. С. 42-45.

Запропоновано квантовий підхід до проектування цифрових пристроїв, який характеризується використанням елементів пам'яті для реалізації транзакційної взаємодії всіх компонентів операційного і керуючого автоматів, а також методами синтезу та аналізу, заснованими на суперпозиції кубіт-векторних примітивів завдання всіх типів функціональностей, імплементованих в елементи пам'яті, що дає можливість істотно (в 2-3 рази) підвищити швидкодію засобів моделювання.

Іл. 2. Бібліогр.: 10 назв.

УДК 383.8:621.396.96:621.396.6

Оцінка глибини тріщини за її стереозображенням на основі ламбертівської моделі відбиття / Н.Р. Грабовська, Б.П. Русин, В.Г. Іванюк // Радіоелектроніка та інформатика. 2015. № 4. С. 46-53.

Розглянуто проблему тривимірної реконструкції поверхні за двомірними зображеннями з метою застосування результатів її розв'язку до задачі аналізу зображень матеріалів з тріщинами. Запропоновано метод визначення глибини тріщини на основі аналізу пари зображень з використанням Ламбертівської моделі відбиття світла. Розроблено та описано програму аналізу характеристик поверхневої тріщини за її зображеннями. Зокрема показано, що, в результаті застосування запропонованих методів, можна отримати таку інформацію про тріщину, як її профіль з більшою точністю.

Іл. 3.. Бібліогр. 13 назв.

УДК 681.3.06

Формалізоване представлення та аналіз агентно-орієнтованих задач / В.О. Філатов, Д.Ю. Узлов // Радіоелектроніка та інформатика. 2015. № 4. С. 54-60.

Розглянуто клас мультиагентних систем управління інформаційними ресурсами. Наведено класифікацію типів задач, найбільш характерних для інформаційних систем. Запропоновано специфікацію агентно-орієнтованого підходу. Обґрунтовано вибір математичного апарату на основі мереж Петрі для моделювання та аналізу розглянутого класу задач. Досліджено варіанти мереж Петрі, їх особливості при моделюванні потоків агентно-орієнтованих задач. Наведено приклад рішення агентно-орієнтованої задачі.

Іл. 2. Бібліогр.: 5 назв.

UDC 621.39

Method of location loss of integrity of information based on slot-technologies / V.V. Barannik, S.A. Podlesny, D.V. Barannik // Radioelektronika i informatika. 2015. N 4. P. 32-41.

It is shown that it is problematically to maintain an information security for state's video information. Also, in this work has been examined main disadvantages of the entropy coding, when it is using in a during cyber-attacks. It is proving that it is important to develop a technology for an allocation codes for the video streams, which has a variable length. In a result of what, there is a loss of data in a localization mechanism.

Fig. 14. Ref.: 8 items.

UDC 004:519.713

Quantum computing for digital systems design // Ye. Litvinova, I. Hahanov // Radioelektronika i informatika. 2015. N 4. P. 42-45.

A quantum approach to the design of digital devices is proposed, which is characterized by the use of memory elements for the implementation of transactional interaction of all components of operational and control automaton, and also methods for the synthesis and analysis based on the superposition of qubit-vector primitives specifying all types of functionalities implemented in memory elements, which allow significantly increasing the speed of modeling tools (in 2-3 times).

Fig. 2. Ref.: 10 items.

UDC 383.8:621.396.96:621.396.6

Crack depth estimation using two images based on Lambert reflectance model / Hrabovcska N.R., Rusyn B.P., Ivanyuk V.H. // Radioelektronika i informatika. 2015. N 4. P. 46-53.

The problem of three dimensional surface reconstruction based on its two dimensional images is considered. Results of solving the reconstruction problem are used for analyzing images of materials with cracks. Crack depth estimation method based on Lambertian reflection model is proposed. The paper contains descriptions of proposed program of cracks characteristics determination. Especially it is shown that such information as crack's profile can be determinate using proposed methods.

Fig.3: . Ref.: 13 items.

UDC 681.3.06

Formalized representation and analysis of agent-oriented problems / V. Filatov, D. Uzlov // Radioelektronika i informatika. 2015. N 4. P. 54-60.

In given paper the class of multi-agent systems information resources management is considered. The classification of problems specific to information systems is proposed. A specification of the agent-oriented approach is substantiated. The choice of a mathematical apparatus based on Petri nets for modeling and analysis of the considered class of problems is justified. Different variants of Petri nets, especially in their simulation of agent-oriented problems are investigated. An example of solution the agent-oriented problem is given.

Fig. 2. Ref.: 5 items.

УДК 519.7

Модель різнорідних розподілених знань / Л.Г. Петрова / / Радіоелектроніка та інформатика. 2015. № 4. С. 61-63.

Розглянута проблема формування розподіленого представлення знань, що охоплює як загальні закономірності предметної області, так і індивідуальні знання про її фрагменти. Запропоновано модель розподіленого представлення знань на основі структури Кріпке. Інтеграція різнорідних знань в моделі здійснена на основі врахування станів предметної області, а також допустимих відносин між цими станами.

Бібліогр.: 8 назв.

УДК 004.421.2:519.71

Використання методу секвенційного аналізу для дослідження структури фрактальних об'єктів/ Н.С. Кравець. / / Радіоелектроніка та інформатика. 2015. № 4. С. 64–66.

Показана можливість використання алгоритму пошуку асоціативних правил, що враховує фактор часу та взаємозв'язок подій, для відновлення параметрів моделі детермінованої L-системи з послідовності символів.

Табл. 2. Іл. 1. Бібліогр.: 2 назв.

UDC 519.7

Model of distributed heterogeneous knowledge / L.G. Petrova // Radioelektronika i informatika. 2015. N 4. P. 61-63.

The problem of the distributed knowledge representation, covering both the general laws of the subject area and individual knowledge of its fragments is considered. The model of distributed knowledge representation based on Kripke structure is proposed. States of domain and relationship between these states are used for sntegration of diverse knowledge in the model.

Ref.: 8 items.

UDC 004.421.2:519.71

The use ofsequentialanalysisforstudying the structure offractal objects/ N. Kravets // Radioelektronika i informatika. 2015. N 4. P. 64–66.

It is shownthe possibility of usingthe algorithmmining association rules, taking into accountthe time factorand the relationshipof eventsto restore theparameters of the modelL-deterministic systemsequence of characters.

Tab. 2. Fig. 1. Ref.: 2 items.