

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

© Харьковский национальный
университет радиоэлектроники, 2015

Свидетельство о государственной регистрации КВ № 12097-968 ПР 14.12.2006

РИ, 2015, № 4

СОДЕРЖАНИЕ

РАДИОТЕХНИКА

ЛЮ ЧАН, ПАНЧЕНКО А.Ю., УЛЬЯНОВ Ю.Н. ОЦЕНКА ВЛАЖНОСТИ ВОЗДУХА МЕТОДОМ РАДИОАКУСТИЧЕСКОГО ЗОНДИРОВАНИЯ ПО ЗАТУХАНИЮ АКУСТИЧЕСКИХ ВОЛН.....	3
--	---

ТЕЛЕКОММУНИКАЦИИ

БАРАННИК В.В., ТУПИЦА И.М., СИДЧЕНКО С.А. МЕТОД КРИПТОСЕМАНТИЧЕСКОГО ПРЕДСТАВЛЕНИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ПЛАВАЮЩЕЙ СХЕМЫ В БАЗИСЕ ПО ВЕРХНИМ ГРАНИЦАМ.....	9
БАРАННИК В.В., ШУЛЬГИН С.С. МОДЕЛЬ ОЦЕНКИ ЦЕЛОСТНОСТИ ДИНАМИЧЕСКОГО ВИДЕОИНФОРМАЦИОННОГО РЕСУРСА В СЛУЧАЕ МЕЖТРАНСФОРМАНТНОЙ ОБРАБОТКИ.....	13
КОМОЛОВ Д.И. ТЕХНОЛОГИЯ ФОРМИРОВАНИЯ КОДОВОЙ КОНСТРУКЦИИ ДЛЯ СЕЛЕКТИВНОГО МЕТОДА ОБРАБОТКИ ВИДЕОДАННЫХ.....	19

СИСТЕМЫ И ПРОЦЕССЫ УПРАВЛЕНИЯ

ЛУХАНИН В.С. ДОДАТНІ РОЗВ'ЯЗКИ ДЛЯ ЕЛІПТИЧНОГО РІВНЯННЯ З ДВОМА ПАРАМЕТРАМИ.....	24
--	----

КОМПЬЮТЕРНЫЕ НАУКИ

ПЕТРОВА О.О., БУРМЕНСЬКИЙ Р.В. ВИКОРИСТАННЯ МАШИНИ ТЬЮРИНГА ДЛЯ РОЗВ'ЯЗАННЯ КРИПТОГРАФІЧНОЇ ЗАДАЧІ ПОЛІНОМІАЛЬНОЇ СКЛАДНОСТІ.....	28
---	----

КОМПЬЮТЕРНАЯ ИНЖЕНЕРИЯ И ТЕХНИЧЕСКАЯ ДИАГНОСТИКА

БАРАННИК В.В., ПОДЛЕСНЫЙ С.А., БАРАННИК Д.В. МЕТОД ЛОКАЛИЗАЦИИ ПОТЕРИ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ НА ОСНОВЕ СЛОТ-ТЕХНОЛОГИИ.....	32
ЛИТВИНОВА Е.И., ХАХАНОВ И.В. КВАНТОВЫЙ КОМПЬЮТИНГ ДЛЯ ПРОЕКТИРОВАНИЯ ЦИФРОВЫХ СИСТЕМ.....	42

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

ГРАБОВСЬКА Н.Р., РУСИН Б.П., ІВАНЮК В.Г. ОЦІНКА ГЛИБИНИ ТРІЩИНИ ЗА ЇЇ СТЕРЕОЗОБРАЖЕННЯМ НА ОСНОВІ ЛАМБЕРТІВСЬКОЇ МОДЕЛІ ВІДБИТТЯ.....	46
ФИЛАТОВ В.А., УЗЛОВ Д.Ю. ФОРМАЛИЗОВАННОЕ ПРЕДСТАВЛЕНИЕ И АНАЛИЗ АГЕНТНО-ОРИЕНТИРОВАННЫХ ЗАДАЧ.....	54
ПЕТРОВА Л.Г. МОДЕЛЬ РАЗНОРОДНЫХ РАСПРЕДЕЛЕННЫХ ЗНАНИЙ.....	61
КРАВЕЦ Н.С. ИСПОЛЬЗОВАНИЕ МЕТОДА СЕКВЕНЦИАЛЬНОГО АНАЛИЗА ДЛЯ МОДЕЛИРОВАНИЯ ОБЪЕКТА С ФРАКТАЛЬНОЙ СТРУКТУРОЙ.....	64
РЕФЕРАТИ.....	67



ОЦЕНКА ВЛАЖНОСТИ ВОЗДУХА МЕТОДОМ РАДИОАКУСТИЧЕСКОГО ЗОНДИРОВАНИЯ ПО ЗАТУХАНИЮ АКУСТИЧЕСКИХ ВОЛН

ЛЮ ЧАН, ПАНЧЕНКО А.Ю., УЛЬЯНОВ Ю.Н.

При разработке методик радиоакустического зондирования атмосферы в качестве первичной информации используются параметры сигнала, наиболее сильно и независимо реагирующие на конкретный метеопараметр. Одним из таких параметров является затухание звуковых волн. Анализируются способы измерения затухания звука, а также способы измерения влажности воздуха. Представляется анализ одного из вариантов измерения затухания с использованием двойной звуковой посылки и особенностей его реализации.

Ключевые слова: системы радиоакустического зондирования, условие Брэгга, фаза сигнала, доплеровский сдвиг частоты.

Key words: radioacoustic sounding system, Bragg's condition, signals phase, Doppler frequency shift.

Введение

Потенциальные возможности радиоакустического зондирования (РАЗ) как дистанционного, неконтактного средства определения метеорологических параметров в настоящее время реализованы далеко не полностью. Акустические волны чувствительны к изменениям состояния воздушной массы, электромагнитные могут без потерь переносить информацию о состоянии зондирующего пакета акустических волн к месту расположения системы [1]. Но связь метеопараметров с параметрами акустической посылки и далее с параметрами принимаемого сигнала весьма сложная. На практике стараются выделить наиболее значимые связи. В настоящее время использование изменения скорости распространения акустических волн связано с измерением температуры воздуха, а при определенной геометрии антенного устройства – с определением скорости ветра [2,3]. Амплитудные параметры принимаемого радиосигнала связаны с пространственным положением акустического пакета, поэтому они с успехом применяются в ветровых измерениях [4]. Дисперсия скорости звука и затухание звуковых волн, которые связаны с влажностью воздуха, измерить существенно сложнее. Тем не менее, влажность воздуха при решении ряда метеорологических задач является определяющим фактором. Поэтому иногда приходится использовать весьма сложный путь косвенных измерений.

Цель данной работы – определение перспективных путей развития методик измерения затухания акустических волн методом радиоакустического зондирования, ориентированных на последующую оценку влажности воздуха. Задачей является анализ предложенных в настоящее время методик измерения непосредственно влажности воздуха с помощью систем РАЗ (RadioAcoustic Sounding System – RASS), а также затухания звука в воздухе.

1. Анализ текущего состояния вопроса

Прямой массометрический метод измерения влажности может быть реализован только в лабораторных условиях [5]. Рабочие средства определения влажности, основанные на явлениях сорбции, измерении температуры точки росы, использовании психрометрических методов [5-7], требуют контакта с исследуемым объемом. Но и они не всегда удобны при практическом применении. Поэтому в некоторых случаях используют весьма сложные косвенные методы.

Один из косвенных путей оценки влажности воздуха состоит в измерении диэлектрической проницаемости воздуха (ϵ) с помощью рефрактометра. Индекс преломления вычисляется по формуле [8]:

$$N = (n - 1) \cdot 10^6 = \frac{\epsilon - 1}{2} \cdot 10^6, \quad (1)$$

где n – показатель преломления.

Как известно [9], индекс преломления связан с температурой T (К), полным атмосферным давлением p (мбар) и парциальным давлением водяного пара e (мбар) соотношением:

$$N = K_1 p / T + K_2 e / T^2, \quad (2)$$

где $K_1 = 77.6$ К/мбар; $K_2 = 3.73 \cdot 10^5$ К²/мбар.

Суммарная относительная ошибка рефрактометра для наиболее часто употребляемого предела измерений в 50 N-единиц составляет 2% [8].

Согласно метрологическому анализу радиометеорологических данных [10] при погрешности не более ± 1 N-ед. и следующих допустимых значениях погрешностей измерения: $\Delta T = 0.788$ К, $\Delta p = 3.7$ мбар парциальное давление водяного пара будет вычислено с погрешностью не более $\Delta e = 0.22$ мбар. При этом относительная влажность будет определена с погрешностью не хуже $\Delta e = 0.33\%$ при температуре 35°C или $\Delta e = 3.0\%$ при 0.

Перечисленные способы являются контактными и имеют общие недостатки:

- 1 – не обеспечивают пространственного осреднения данных;
- 2 – невозможно получить оперативные данные о влажности над произвольно заданной территорией;

3 – способы нельзя применить для мониторинга в реальном времени;

4 – реализующие эти способы устройства не пригодны для использования в районе аэропортов ввиду создания помех воздушному движению.

Для исключения перечисленных недостатков необходимо применять неконтактные способы всепогодного зондирования атмосферы с поверхности Земли.

Известен способ, основанный на применении радиометра с рабочей длиной волны $\lambda = 2.1$ см и с антенной, имеющей главный луч шириной около 1° и низкий уровень боковых лепестков: параболический рефлектор диаметром 2.5 м, облучатель в виде рупора [11]. Сканирование антенны проводится около зенитных углов $\Theta = 85^\circ \dots 95^\circ$. При вертикальной поляризации антенны обнаружен всплеск радиояркостной температуры под углом $\Theta \approx 90^\circ$. Способ используется для нахождения волновода испарения над морской поверхностью.

Известен способ оценки ослабления и рефракции радиоволн над морской поверхностью с помощью двухчастотного радиолокационного зондирования ($\lambda = 3$ и 10 см) под малыми углами места [11]. Приемопередающие антенны кругового обзора имели ширину диаграмм направленности $\Theta_g = 0.75^\circ$ и 2.5° в горизонтальной плоскости, $\Theta_v = 20^\circ$ в вертикальной плоскости и располагались на высоте 25...26 м. Длительность импульса посылки 0.4...0.8 мкс. Способ основан на приеме обратного рассеяния радиоволн взволнованной морской поверхностью в результате резонансного брэгговского рассеяния.

Недостатком радиолокационного способа зондирования атмосферы является его ограниченное применение: он не может быть использован при распространении радиоволн над сушей и при больших углах места.

Над сушей применим способ определения показателя преломления радиоволн в пограничном слое атмосферы, основанный на теоретической модели [12]. Для применения модели требуется измерение с помощью акустического локатора высотных профилей температуры и скорости ветра, а также уточнение характера атмосферных неоднородностей. Недостатком способа является ограничение его применения только при некоторых погодных условиях, так как наличие слоев в приземном слое ограничивает применимость модели.

Общим недостатком способов акустического и радиолокационного зондирования атмосферы является использование естественных отражателей акустических или электромагнитных волн. Возникновение таких отражателей обусловлено локальной турбулентностью атмосферы, которая может отсутство-

вать на разных высотах при определенных погодных условиях.

Среди наиболее удачных, по совокупности признаков, является способ радиоакустического зондирования атмосферы [13]. Акустическая зондирующая посылка в виде пакета синусоидальных колебаний сопровождается излучением доплеровского локатора, который затем принимает сигнал, отраженный от возмущенного объема воздуха. По доплеровскому сдвигу принятых эхо-сигналов при изменении наклона антенного устройства определяют высотные профили температуры и ветра, по затуханию эхо-сигналов находят высотный профиль влажности.

Альтернативой оценке влажности на основании измеренного коэффициента затухания является радиоакустический способ, в котором используют акустический пакет, состоящий из импульсов длительностью τ_{s0} , частота повторения F_{s0} , длительность пакета τ_s [14]. Облучают пакет посылками электромагнитных импульсов (ЭМИ) длительностью τ_e , частота повторения F_{e0} , которая выбирается из условия выполнения соотношения Брэгга: $\lambda_s = \lambda_e / 2$, где $\lambda_e = C_e / F_{e0}$; C_e - скорость света; $\lambda_s = C_s / F_{s0}$; C_s - скорость звука в воздухе. В спектре ЭМИ имеются частоты mF_{e0} , где $m = 1, 2, \dots, M$. Максимальная частота $M F_{e0}$ выбирается по энергетическому критерию из условия $M = (F_{s0} \tau_{s0})^{-1}$. В принимаемом сигнале на частотах, близких к каждой mF_{e0} , измеряют значения частот доплеровских смещений $F_{D1}, F_{D2}, \dots, F_{DM}$ и разность фаз сигналов на этих доплеровских частотах $\Delta\phi_1, \Delta\phi_2, \dots, \Delta\phi_M$.

Положительный эффект в этом способе основан на различном изменении скоростей распространения звуковых волн различной частоты при изменении влажности h . В частности, согласно [1, 15] при нормальном давлении $p_0 = 1013$ мбар:

$$c_s = c_{s0} \sqrt{1 + 64 \cdot 10^{-5} \frac{(f/f_r)^2}{1 + (f/f_r)^2}}, \quad (3)$$

$$\text{где } f_r = \left(\frac{p}{p_0} \right) \left(24 + 4.41 \cdot 10^4 h \frac{0.05 + h}{0.391 + h} \right).$$

Частота релаксации лежит в области десятков кГц, поэтому согласно (3) изменение скорости весьма мало. В связи с этим в данном способе выбран фазометрический метод выделения первичной информации.

Указанный способ также имеет недостатки. С ростом частоты затухание звука резко увеличивается. Совместно с другими факторами, вызывающими снижение уровня принимаемого сигнала, это ограничи-

вает возможности способа. Кроме того, определенные технические сложности вызывает требование формирования излучаемых сигналов с широким спектром.

Тем не менее, к принципиальным отличиям данного способа следует отнести использование зондирующих сигналов со сравнительно сложным спектром. Предшествующие варианты построения систем РАЗ применяли, как правило, простые гармонические сигналы, ограниченные по времени. Использование сложных зондирующих сигналов увеличивает число вариантов построения РАСС и их возможности.

2. Зондирование двойной акустической посылкой

Малая величина коэффициента отражения электромагнитных волн от неоднородностей диэлектрической проницаемости воздуха, вызванных прохождением акустических волн, и линейные свойства отраженного поля позволяют построить систему, непосредственно формирующую сигнал, пропорциональный затуханию акустических волн в воздухе. Для этого необходимо сформировать двойную акустическую посылку, составляющие части которой отражают электромагнитные волны так, что они приходят к приемному устройству РАСС в противофазе.

На рис. 1. представлена геометрическая схема формирования принимаемого сигнала.

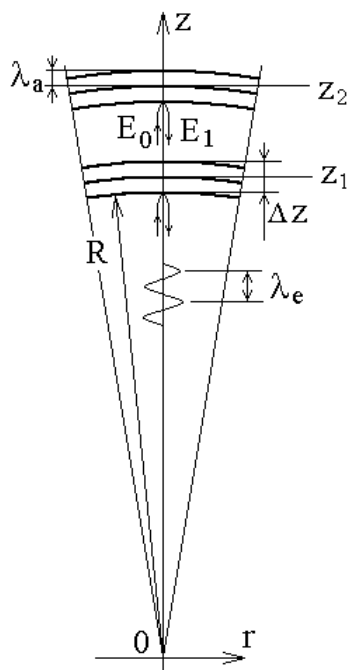


Рис. 1. Схема формирования информационного сигнала

При анализе необходимо учесть следующие физические механизмы. Малая величина коэффициента отражения электромагнитных волн позволяет пренебречь изменением амплитуды прошедшей волны. Дифракционная схема формирования сигнала осесимметричная. Расходимость волн, с одной стороны, и фокусировка отраженного поля сферической поверхнос-

тью зондирующего пакета – с другой, приводит к уменьшению принимаемого сигнала пропорционально z^{-1} [16,17]. Используя результаты этих работ, можно последовательно записать параметры отражательной способности акустической зондирующей посылки, падающего и отраженного электромагнитного поля. Отражение волн происходит от перепадов волнового сопротивления среды ΔZ_c и при плавном изменении отражение пропорционально производной $\partial Z_c / \partial R$. При синусоидальном сигнале в посылке имеем:

$$\partial Z_c / \partial R = A_0 K_0 \cos[\Omega(t - R / C_s)] \exp(-\alpha R) R^{-1}, \quad (4)$$

где A_0 – амплитуда сигнала посылки; Ω – частота звукового сигнала; α – коэффициент затухания звука.

Коэффициент K_0 включает постоянные множители, определяющие ∂Z_c . Он может быть получен на основании соотношений (1), (2) и коэффициента передачи электроакустического преобразователя. Поскольку далее можно ограничиться решением задачи в одном измерении вдоль оси z , то при дифференцировании в (4) расстояние R можно заменить на z , а интегрирование по площади акустического пакета можно опустить. Его результат, согласно [16,17], компенсирует влияние сферической расходимости падающего и отраженного электромагнитного поля и войдет в K_0 как постоянный множитель. В связи с ограниченным объемом работы этот и другие постоянные множители рассматривать не будем.

Интегрируя отражение вдоль пакета, для принятого сигнала в случае зондирования одиночной посылкой получаем:

$$u(t) = E_0 A_0 K_0 \int_{C_s(t-\Delta t/2)}^{C_s(t+\Delta t/2)} \cos[\Omega(t - z / C_s)] \times \exp[i\omega(t - 2z / C_e)] \cdot \exp(-\alpha z) z^{-1} dz, \quad (5)$$

где E_0 – амплитуда падающего поля; Δt – длительность зондирующей посылки; ω – частота электромагнитного сигнала.

Время t синхронизировано с моментом запуска акустического пакета.

Косинус в (5) раскладываем согласно известному выражению: $\cos \varphi = 0.5[\exp(i\varphi) + \exp(-i\varphi)]$. Первое слагаемое приведет в подынтегральном выражении (5) к быстро осциллирующей функции, ее интегралом можно пренебречь. Со вторым слагаемым получим:

$$u(t) = \frac{E_0 A_0 K_0}{2} \frac{\exp[i(\omega - \Omega)t]}{z_0} \times \int_{C_s(t-\Delta t/2)}^{C_s(t+\Delta t/2)} \exp\{[i(k_s - 2k_e) - \alpha]z\} dz, \quad (6)$$

где k_s, k_e – постоянные распространения акустических и электромагнитных волн: $k_s = 2\pi/\lambda_s$, $k_e = 2\pi/\lambda_e$.

Функция z^{-1} вынесена в (6) из-под интеграла, и заменена постоянной величиной z_0^{-1} , в которой $z_0 = C_s t$ – расстояние до центра акустического пакета. Такое упрощение допустимо, так как на дистанции зондирования z^{-1} приводит к практически линейному уменьшению отражательной способности вдоль пакета. После несложных преобразований имеем:

$$u(t) = E_0 A_0 K_0 \frac{\exp\{[i(\omega - 2k_e C_s)t] - \alpha z_0\}}{i(k_s - 2k_e)z_0 - \alpha z_0} \times \\ \times \{\exp[i(k_s - 2k_e)\Delta z / 2] \operatorname{ch}(\alpha \Delta z / 2) - \\ - \exp(\alpha \Delta z / 2) \cos[(k_s - 2k_e)\Delta z / 2]\}, \quad (7)$$

где Δz – протяженность акустического пакета.

Двойная звуковая посылка сформирует в воздухе пакет акустических волн, состоящий из двух частей. Если промежуток между ними обеспечивает приход отраженного ЭМП в противофазе, то в полученном сигнале можно существенно усилить зависимость амплитуды от затухания. Для этого необходимо, чтобы обе части пакета имели одинаковую длительность, а амплитуду необходимо изменить так, чтобы скомпенсировать радиальную расходимость. Эти условия приводят к следующему: расстояние между центрами частей пакета $z_2 - z_1 = \Delta z + \lambda_e(0.25 + 0.5 \cdot n)$, где $n = 0, 1, 2, \dots$, и $A_1/z_1 = A_2/z_2$, где A_1 и A_2 – амплитуда первой и второй частей пакета, а Δz здесь и далее – протяженность каждой из частей акустического пакета и $z_\alpha = 0.5(z_1 + z_2)$ – высота определения α . При выполнении этих соотношений в передающих устройствах RASS результирующий сигнал равен:

$$U(t) = A \exp[i(\omega - 2k_e C_s)t] \times \\ \times \{\exp[-(i2k_e + \alpha)z_1] + \exp[-(i2k_e + \alpha)z_2]\} \times \\ \times \{\exp[i(k_s - 2k_e)\Delta z / 2] \operatorname{ch}(\alpha \Delta z / 2) - \\ - \exp(\alpha \Delta z / 2) \cos[(k_s - 2k_e)\Delta z / 2]\} / [i(k_s - 2k_e) - \alpha]. \quad (8)$$

Здесь A – результирующий коэффициент, в который входят постоянные коэффициенты выражения (7) и скорректированная амплитуда обеих частей пакета:

$$A_c = A_1 \cdot z_2 = A_2 \cdot z_1.$$

Данное выражение содержит все необходимые компоненты для оценки возможностей RASS с двойной звуковой посылкой.

3. Анализ результатов и перспективы реализации

Первая строка в формуле (8) показывает доплеровский сдвиг частоты принимаемого сигнала. Как известно

[16,17], при соблюдении условия Брэгга доплеровский сдвиг частоты принимаемого сигнала совпадает с частотой зондирующей посылки. При этом амплитуда принимаемого сигнала максимальна. Современная элементная база позволяет при доступных затратах создать RASS с доплеровским локатором, частота которого изменяется в соответствии с изменением сдвига частоты принимаемого сигнала.

Множитель соотношения Брэгга $K_b(k_e, \alpha)$ при $\alpha \rightarrow 0$ определяют третья и четвертая строки (8). При увеличении затухания его поведение представлено на рис.2. Для расчетов выбраны два значения коэффициента затухания: $\alpha_1 = 0.001$, $\alpha_2 = 0.01$ и $\Delta z = 20\lambda_{e0}$, где λ_{e0} – длина волны при строгом выполнении условия Брэгга.

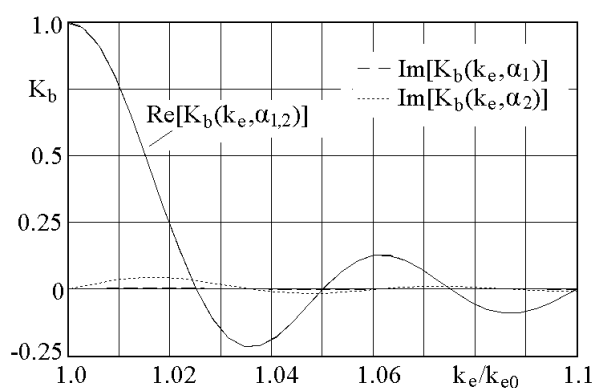


Рис. 2. Множитель соотношения Брэгга

Различие между зависимостями действительных частей $K_b(k_e, \alpha)$ столь мало, что в данном масштабе показать невозможно. Но при выбранных значениях коэффициента затухания уменьшение амплитуды на протяжении каждой части пакета составит соответственно 2 и 20%. Таким образом, можно считать, что изменение затухания в широких пределах не влияет на зависимость резонансного отражения электромагнитных волн от зондирующего пакета. Происходит только небольшой фазовый сдвиг вследствие изменения отражательной способности в соседних полупериодах пакета, что вызывает некоторый рост мнимой части $K_b(k_e, \alpha)$. Влияние этого фактора можно существенно уменьшить, используя в доплеровском локаторе RASS систему автоматической подстройки частоты. При этом погрешность слежения за частотой отраженного сигнала можно не учитывать. Эту же величину можно использовать для вычисления текущего значения множителя соотношения Брэгга.

Для оценки результирующей зависимости амплитуды принятого сигнала от затухания к множителю соотношения Брэгга необходимо добавить множитель, представленный во второй строке (8). Для иллюстрации поведения этой зависимости на рис.3 показано нормированное значение функции (8), равное

$$U_0 = U(z_\alpha / C_s) \cdot 4z_\alpha / A\Delta z^2.$$

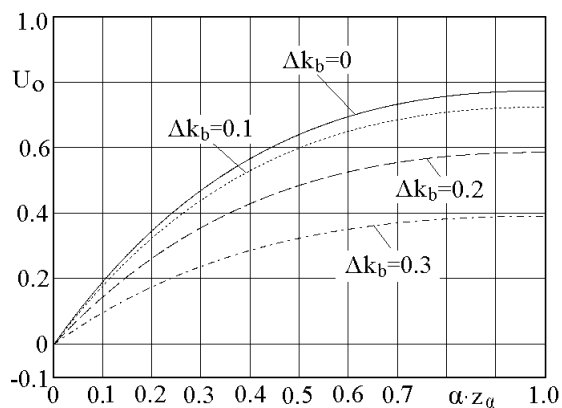


Рис. 3. Результирующая зависимость амплитуды принимаемого сигнала

В качестве параметра на этих графиках взяты значения обобщенной расстройки условия Брэгга – Δk_b . При увеличении протяженности пакета острота резонансной кривой (см. рис.2) увеличивается. Поэтому Δk_b выбрана как $\Delta k_b = (k_s / 2k_e - 1)\Delta z / \lambda_{e0}$, и ее значения взяты на первом лепестке множителя соотношения Брэгга.

Дальнейшие расчеты показали, что характер зависимостей не изменяется в широком диапазоне расстояний: $z_\alpha > 20\lambda_{e0}$ и $\Delta z > 0.2 \cdot z_\alpha$, а для малых расстояний можно взять $\Delta z > 4\lambda_{e0}$. Кроме того, при увеличении затухания $\alpha > (1...2) / z_\alpha$ существенно уменьшается уровень принятого сигнала. Но это уменьшение не является особенностью использования двойной посылки. Ограничение максимальной высоты зондирования величиной $z_{\max} \approx 1 / \alpha$ вследствие затухания звука на всей трассе распространения будет и при зондировании обычными одиночными посылками.

Производная при $\alpha \ll z_\alpha^{-1}$ практически постоянна, что упрощает процесс измерений. Выражение для ее точного значения весьма громоздко. В качестве параметров в него входят Δz , z_1 и z_2 и текущее значение множителя соотношения Брэгга. При необходимости точное значение производной можно реализовать в рабочей программе вычислительного комплекса RASS.

Не менее значительную проблему представляет совокупность иных факторов, влияющих на амплитуду принимаемого сигнала. Для оценки этих факторов можно использовать режим работы RASS с обычной одинарной посылкой. При чередовании посылок частота принимаемого сигнала от одинарной посылки несет информацию о температуре и ее градиенте, а амплитуда позволит определить текущие значение результирующего коэффициента в (8). Таким образом может быть компенсировано действие изменений отражательной способности пакета, его ветрового переноса, а также изменение множителя соотношения

Брэгга в каждой из частей посылки вследствие температурного градиента. Тем не менее, ввиду флуктуаций метеопараметров и динамических процессов в области измерений может сохраняться значительная величина погрешности.

Более эффективным решением этой проблемы может служить создание дополнительного канала частотной обработки сигнала в доплеровском локаторе RASS. Фильтрация сигнала рабочей частоты дополнительного канала может быть осуществлена благодаря резонансным свойствам дифракции Брэгга. При $\alpha \rightarrow 0$ из (7) получаем:

$$u(t) = \frac{E_0 K_0 A}{z_0} \exp[i(\omega - 2k_e C_s)t] \frac{\sin[(k_s - 2k_e)\Delta z / 2]}{(k_s - 2k_e)}. \quad (9)$$

Здесь последний сомножитель представляет функцию взаимодействия Брэгга. При выполнении условия $\lambda_{e,n} = 2N\lambda_s(N-n)^{-1}$, где N – число акустических волн в зондирующем пакете, $n = 1, 2, \dots, N$, отражение Брэгга будет равно нулю – нули на графике рис.2. Если рабочие частоты основного и дополнительного каналов RASS будут связаны этим соотношением, то можно будет одновременно, из одной точки пространства получать информацию о температуре и влажности воздуха. Значение n можно выбирать так, чтобы частота дополнительного канала отличалась от частоты основного в пределах 5...10%. При этом можно с полным основанием считать, что условия распространения и отражения волн в обоих каналах одинаковы.

Зондирующая посылка дополнительного канала может излучаться непосредственно перед или после двойной посылки основного, или же одновременно с посылкой основного канала. Как правило, входные и выходные устройства приемопередающего тракта доплеровского локатора широкополосные – это согласующие и антенно-фидерные устройства, входные и выходные усилители, предварительные фильтры и т.д. Поэтому дополнительно потребуется создание генераторных устройств и устройств конечной обработки аналогового сигнала, что не вызовет существенного повышения стоимости системы в целом.

Выводы

Показаны возможности, которые открывает использование модулированных зондирующих сигналов в RASS. Рассматриваемые ранее варианты сложных зондирующих посылок были ориентированы в основном на увеличение мощности принимаемых сигналов. Это само по себе является важной задачей, но не всегда сопряжено с увеличением количества получаемой информации. Решена задача формирования сигнала, который непосредственно связан с получением информации о параметрах воздуха.

Оценка вариантов реализации RASS с двойной посылкой показывает, что при умеренных экономических затратах может быть достигнуто существенное увеличение точности измерений и расширение диапа-

зона метеорологических состояний, при которых RASS может уверенно давать информацию о состоянии воздушной массы.

Дальнейшее развитие методик применения модулированных зондирующих сигналов в RASS позволит расширить возможности метода РАЗ и будет способствовать его активному применению в практике метеорологических наблюдений.

Литература: 1. *Каллистратова М.А., Кон А. И.* Радиоакустическое зондирование атмосферы. М.: Наука, 1985. 197 с. 2. *Smith P.I.* Remote measurement of wind velocity by the electromagnetic-acoustic probe. I System analysis. // In: Conf. proc. 5th Annu. convention on military electronics. Wash. (D.C.) 1961. rep. N419. P.43-53. 3. *Fetter R.V.* Remote measurement of wind velocity by the electromagnetic-acoustic probe. II Experimental system. // In: Conf. proc. 5th Annu. convention on military electronics. Wash. (D.C.) 1961. rep. N 420. P. 54-59. 4. *Панченко А.Ю.* Радиоакустический способ определения модуля скорости ветра // А.с. № 1545781 22.10.89. 5. *Берлинер М.А.* Измерение влажности. Изд. 2-е, перераб. и доп. М.: Энергия, 1973. 400 с. 6. *Усольцев В.А.* Измерение влажности воздуха. Методы и пробы. Л.: Гидрометеоздат, 1959. 182 с. 7. *Коряков В.И. Запорожец А.С.* Приборы и системы контроля влажности твердых веществ и их метрологические характеристики // Практика приборостроения. 2002. №1. С. 5-11. 8. *Казаков Л.Я., Ломакин А.Н.* Неоднородности коэффициента преломления воздуха в тропосфере. М.: Наука, 1976. 164 с. 9. *Справочник по радиолокации.* Т.1. Основы радиолокации. Пер. с англ под ред. Я.С. Ицхоки. М.: Сов. радио. 1976. 456 с. 10. *Бин Б. Р., Дантон Е.Дж.* Радиометеорология. Ленинград: Гидрометеоздат, 1971. 362 с. 11. *Кошель К.В., Славутский Л.А., Шевцов Б.М.* Распространение УК и СВЧ радиоволн над морем. Владивосток: Дальнаука, 1993. 160 с. 12. *Андрюханов В.А., Ракитин Б.В.* Восстановление высотных профилей показателя преломления радиоволн в пограничном слое атмосферы // Радиотехника и электроника, 1978. Т. 23. 10. С. 2031-2038. 13. *Орлов М. Ю., Юрчак Б.С.* О возможности определения влажности в приземном слое атмосферы радиоакустическим способом // Труды института экспериментальной метеорологии. 1985. Т.38, №121. С. 14-20. 14. *Ульянов Ю.Н., Бутакова С.В.* и др. Способ радиоакустического зондирования атмосферы // Патент РФ 2196345, 10.01.2003, G01S13/95. 15. *Бергман Л.* Ультразвук и его применение в технике. М.: Мир. 1957. 726 с. 16. *Кон А.И.* Бистатическая система радиоакустического зондирования // Изв. АН СССР. Физика атмосферы и океана. 1981. Т.17, №6. С.657-660. 17. *Панченко А.Ю.* Дифракция электромагнитных волн на акустических при радиоакустическом зондировании атмосферы // Электромагнитные волны и электронные системы (Москва. Россия). 1997. Т.2, №5. С.37-42.

Транслитерированный список литературы:

1. *Kallistratova M. A., Kon A. I.* Radioacoustic sounding of the atmosphere. M.: Nauka, 1985. 197p. 2. *Smith P.I.* Remote measurement of wind velocity by the electromagnetic-acoustic probe. I System analysis // In: Conf. proc. 5th Annu. convention on military electronics. Wash. (D.C.) 1961. rep. N419, p.43-53. 3. *Fetter R.V.* Remote measurement of wind velocity by the electromagnetic-acoustic probe. II Experimental system. // In: Conf. proc. 5th Annu. convention on military electronics. Wash. (D.C.) 1961. rep. N 420, p. 54-59. 4. *Panchenko A.Yu.* Radioacoustic method for the wind speed module determining // Patent SU. 1545781, 22.10.89. 5. *Berliner M.A.* Humidity measurement. Sec. Edition, M.: Energija, 1973. 400p. 6. *Usoitcev V.A.* Measurement of humidity of air. Methods and tests. L.: Gidrometeoizdat, 1959. 182p. 7. *Koryakov V.I. Zaporozhets A.S.* Devices and systems for humidity control solid substances

and their metrological characteristics // Practice Instrumentation. 2002. No. 1. pp 5-11. 8. *Kozakov L.Ya. Lomakin A.N.* The inhomogeneities of the refractive index of air in the troposphere. M.: Nauka, 1976. 164p. 9. Radar handbook. V.1. Radar basics. Translation from English under the editorship of Ya.S. Itskhoki. M.: Sov. radio. 1976. 456p. 10. *B.R. Bin. E.J. Datton.* Radiometeorology. Leningrad: Gidrometeoizdat, 1971. 362p. 11. *Koshel K.V., Slavutsky L.A., Shevtsov B. M.* Distribution of US and UH radio waves over the sea. Vladivostok: Dalnauka, 1993. 160p. 12. *Andrianov V.A., Rakitin B. V.* Recovering vertical profiles of radio waves index refraction in the atmospheric boundary layer // Radio Engineering and Electronics, 1978. T. 23. 10. pp 2031-2038. 13. *Orlov M.Yu., Yurchak B.S.* On the possibility of determining the humidity in the surface atmospheric layer by radio acoustic method // Proc. of Experimental meteorology institute. 1985. V.38 #121. pp 14-20. 14. *Ulyanov Y.N., Butakova S.V. et al.* Radioacoustic atmospheric sounding method // Patent RU 2196345, 10.01.2003, G01S13/95. 15. *Bergman L.* Ultrasound and its application in technics. Translated from German. Second edition. M.: Mir. 1957. 726p. 16. *Con A.I.* Bistatic system of radioacoustic sounding // Izv. USSR Ac. of Sciences. Atm. and ocean phys. 1981, v.17.-#6. pp 657-660. 17. *Panchenko A.Yu.* Diffraction of electromagnetic waves on acoustic at radio acoustic sounding of the atmosphere // Electromagnetic waves and electronic systems (Moscow. Russia). 1997. V.2, T 5. P. 37-42.

Поступила в редколлегия 10.12.2015

Рецензент: д-р физ.-мат. наук Бондаренко И.Н.

Лю Чан, канд. техн. наук, старший преподаватель, начальник отдела внешних связей, Хэйлунцзянский Бауи аграрный университет, город Дачин, провинция Хэйлунцзян, КНР. Научные интересы: неконтактное зондирование газовых сред и пограничного слоя атмосферы с помощью акустических и радиоволн, СВЧ устройств. Адрес: ул. Синфон 5, город Дачин, Хэйлунцзян, КНР 163319, кон. тел. +86-459-6819896.

Панченко Александр Юрьевич, д-р физ.-мат. наук, профессор каф. ПЭЭА ХНУРЭ. Научные интересы: зондирование атмосферного пограничного слоя, СВЧ устройства. Адрес: Украина, Харьков, 61166, пр. Науки, 14, к. 400и, тел. 0577021494.

Ульянов Юрий Николаевич, канд. техн. наук, старший научный сотрудник НТУ «ХПИ». Научные интересы: неконтактное зондирование различных газовых сред акустическими и радиоволнами, вибродиагностика. Хобби: увлеченный фотограф, радио- и автолюбитель. Адрес: Украина, 61000, Харьков, ул. Харьковских дивизий, 18, кв. 67, тел. 7174898, 7076879.

Liu Chang, Ph.D, lecturer, section head of Foreign Affairs, Heilongjiang Bayi Agricultural university (city Daqing, province Heilongjiang, China PR). Scientific interests: non-contact sensing of gaseous media and boundary layer of atmosphere by acoustic and radio waves, UHF devises. Address: road Xinfeng 5, city Daqing, Heilongjiang, China PR 163319, telephone: +86-459-6819896

Panchenko Aleksandr Yuriyovich, Doctor of Science, professor, professor of dep. PEEA, KhNURE. Scientific interests: sensing of boundary layer of atmosphere, UHF devises. Science av. 14, aud. 400 "i", Kharkov, Ukraine. Tel. +380577021494

Ulianov Yuriy Nickolaevich. Candidate of Science. Senior research fellow. Senior Researcher of NTU «KhPI». Scientific interests: non-contact sensing of gaseous media by acoustic and radio waves, vibration monitoring. Fascinated car enthusiast and photographer. Kharkov, Kharkovskikh diviziya str. 18, ap. 67, phones 7174898, 7076879.



МЕТОД КРИПТОСЕМАНТИЧЕСКОГО ПРЕДСТАВЛЕНИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ПЛАВАЮЩЕЙ СХЕМЫ В БАЗИСЕ ПОВЕРХНИМ ГРАНИЦАМ

БАРАННИК В.В., ТУПИЦА И.М.,
СИДЧЕНКО С.А.

В целях создания комбинированных систем для скрытия видеoinформационного ресурса на основе технологий устранения избыточности с сохранением целостности и оперативности доставки информации разрабатывается метод криптосемантического представления изображений на основе плавающей схемы системы полиадического кодирования в базисе по верхним границам. Данный метод обеспечивает: одновременное выполнение процессов сжатия и шифрования (кодирования) видеоданных; исключение избыточности одновременно без внесения погрешности; уменьшение количества незначимых элементов (незначимых нулевых бит) в начале каждой битовой последовательности кодов-номеров; формирование кодограмм равномерной длины на основе переменного (заранее неопределенного) количества элементов исходного изображения; дополнительное снижение исходного объема изображений.

Ключевые слова: криптосемантическое представление изображений; защита информации; шифрование; кодирование; компрессия изображения; полиадический код.

1. Введение

Развитие мультимедийных приложений и их внедрение в различные сферы деятельности человека послужило причиной роста требований относительно времени доставки видеоданных, качества их восстановления и обеспечения требуемого уровня конфиденциальности передаваемой информации.

Поэтому актуальной научно-прикладной задачей является сокращение времени на цифровую обработку и доставку видеоданных при обеспечении заданного уровня конфиденциальности семантической информации, передаваемой на основе изображений.

Для повышения эффективности обеспечения безопасности видеoinформации, доводимой в реальном времени, возможны два направления, а именно:

1. Провести модификацию существующих технологий компрессии и криптографических преобразований с позиции их последовательного использования.
2. Разработать принципиально новый подход, который заключается в создании технологий, одновре-

менно обеспечивающих повышение оперативности доведения и защиту видеoinформации на основе методов семантической и синтаксической обработки изображений.

В пользу выбора второго направления указывают следующие преимущества:

- обеспечивается сокращение объемов видеоданных, передаваемых с использованием инфокоммуникационных систем;
- разработка процессов сжатия и шифрования рассматривается как единый этап обработки, что исключает необходимость в организации их совместимости и согласованности;
- исключается возможность несанкционированного доступа к видеoinформации после этапа компрессии;
- существует возможность учитывать для обеспечения информационной скрытности особенности семантического содержания изображений и психовизуального восприятия их зрительной системой. В том числе возможно учитывать и тот факт, что шифрование осуществляется одинаково для всех частей фрагмента изображения, т.е. затрачивается одинаковое количество операций для всех блоков изображения, в то время как разные блоки несут различное количество семантической нагрузки, т.е. разные блоки изображения имеют различную важность и ценность информации. Учет такой семантической неоднородности блоков изображения позволяет сократить вычислительные затраты. Это можно сделать с помощью методов кодирования источников изображений;
- сокращается время обработки за счет слияния двух этапов в один.

Для решения поставленной научно-прикладной задачи в работах [1–4] была предложена технология криптосемантического представления изображений, предназначенная для скрытия семантического смысла изображения с учетом как статистических, так и структурных особенностей источника информации. В [5,6] предложен метод криптосемантического представления изображений на основе статической схемы полиадического кодирования в двумерном базисе. В работе [7] предложена методика тестирования для оценки статистических характеристик криптосемантического представления изображений и на их основе проведено тестирование последовательностей кодов-номеров для статической схемы полиадического кодирования.

Одним из недостатков разработанного метода криптосемантического представления изображений на основе статической схемы полиадического кодирования является построение кода-номера криптосемантического представления изображения на основе одинакового количества исходных элементов фрагмента видеоданных [5,6]. На выходе криптосемантического представления получают кодограммы разной длины в битовом представлении (меньше длины, выделя-

емой для хранения кодового слова), что приводит к появлению большого количества незначимых нулевых элементов в выходных битовых последовательностях [8]. Этот недостаток влияет, с одной стороны, на степень сжатия изображения (выходной объем криптосемантического представления), а с другой – на выходные статистические характеристики криптосемантического представления и на уровень конфиденциальности в целом.

Поэтому для формирования кодограмм равномерной длины на основе переменного (заранее неопределенного) количества элементов исходного изображения предлагается формировать информационную часть криптосемантического представления на основе плавающей схемы полиадического кодирования. Для этого в работах [8,9] предложена плавающая схема криптосемантического представления в двумерном базисе по верхним границам. Недостатком данного подхода является то, что сначала формируются промежуточные коды-номера по отдельным столбцам, а уже потом формируется интегрированный код-номер, что в свою очередь может так же привести к появлению кодов-номеров с длиной, меньшей, чем длина выделяемого кодового слова. Это связано с тем, что формирование интегрированного кода-номера происходит на основе больших промежуточных данных. Кроме того, для формирования кода-номера в двумерном базисе необходимо хранить (передавать) двойной комплект оснований (служебных данных), что может привести к увеличению общего выходного объема криптосемантического представления изображения.

Цель исследований заключается в разработке метода кодирования изображений на основе плавающей схемы полиадического кодирования в базисе по верхним границам, обеспечивающего формирование кодограмм равномерной длины на основе переменного (заранее неопределенного) количества элементов исходного изображения.

2. Основная часть

Исходное изображение разбивается на фрагменты размерностью $m \times n$ точек, где m – количество строк фрагмента изображения, а n – количество столбцов. Фрагмент изображения рассматривается как двумерная матрица $A = \{a_{i,j}\}$, $i = \overline{1, m}$, $j = \overline{1, n}$, которую можно преобразовать в одномерный вектор:

$$A = \{a_{i,j}\} = \{a_{\tau}\}_{\tau=\overline{1, mn}} = \{a_{m(j-1)+i}\}_{i=\overline{1, m}, j=\overline{1, n}}. \quad (1)$$

На предварительном этапе определяется система оснований $G^{(m)} = \{g_i\}$, $i = \overline{1, m}$, исходного фрагмента изображения по строкам. Основание элементов i -й строки g_i определяется как максимальный элемент строки исходного массива, увеличенный на 1:

$$g_i = \max_{1 \leq j \leq n} (a_{i,j}) + 1 = \max_{1 \leq j \leq n} (a_{m(j-1)+i}) + 1. \quad (2)$$

В дальнейшем система оснований будет выступать в роли ключевого элемента (служебных данных) для формирования информационной части криптосемантического представления изображения и должна храниться в секрете или дополнительно шифроваться с использованием одного из стандартов блочного шифрования данных.

Для удобства проведения расчетов и для определения взаимно-однозначного соответствия элементов фрагмента изображения с основаниями предлагается расширить систему оснований до мощности исходного фрагмента изображения в одномерном векторном виде. Для этого воспользуемся формулой:

$$S^{(m \times n)} = \{s_{\tau}\} = \{g_{\tau-m \left[\frac{\tau-1}{m} \right]}\}_{\tau=\overline{1, mn}}. \quad (3)$$

Процесс представления данных в полиадической системе в базисе по верхним границам на основе плавающей схемы задается следующими выражениями:

$$N = \sum_{\tau=1}^Q a_{\tau} V_{\tau}; \quad (4)$$

$$V_{\tau} = \begin{cases} \prod_{\xi=\tau+1}^Q s_{\xi} = \prod_{\xi=\tau+1}^Q g_{\xi-m \left[\frac{\xi-1}{m} \right]}, & \tau < Q; \\ 1, & \tau = Q, \end{cases} \quad (5)$$

$$Q \leq mn, \quad (6)$$

где Q – плавающее количество элементов, принимающих участие в формировании кода-номера в базисе по верхним границам на основе плавающей схемы с учетом проверки на переполнение кодового слова; $[\bullet]$ – целая часть.

Для контроля переполнения кодового слова при формировании кода-номера N введем дополнительную величину T_Q , равную накопленному произведению оснований для Q элементов, принимающих участие в формировании кода-номера, которая определяется по формуле:

$$T_Q = \prod_{\xi=1}^Q s_{\xi} = \prod_{\xi=1}^Q g_{\xi-m \left[\frac{\xi-1}{m} \right]}. \quad (7)$$

Переполнения кодового слова не произойдет, если выполняется неравенство:

$$T_Q \leq 2^M - 1, \quad (8)$$

где $2^M - 1$ – наибольшее число, которое может храниться в кодовом слове длиной M элементов.

Действительно, поскольку выполняется неравенство $T_Q \geq N$, тогда: $N \leq 2^M - 1$.

Максимальное количество элементов $Q_{\lim}$, принимающих участие в формировании кода-номера, опреде-

ляется как значение аргумента, при котором величина T_Q достигает максимума при условии выполнения неравенства (8) и рассчитывается по формуле:

$$Q_{\lim} = \operatorname{argmax}_Q(T_Q) = \operatorname{argmax}_Q\left(\prod_{\xi=1}^Q s_{\xi}\right). \quad (9)$$

С учетом соотношения (9) выражения (4) и (5) для определения кода-номера примут вид

$$N = \sum_{\tau=1}^{Q_{\lim}} a_{\tau} V_{\tau}; \quad (10)$$

$$V_{\tau} = \begin{cases} \prod_{\xi=\tau+1}^{Q_{\lim}} s_{\xi} = \prod_{\xi=\tau+1}^{Q_{\lim}} g_{\xi-m\left[\frac{\xi-1}{m}\right]}, & \tau < Q_{\lim} < mn; \\ 1, & \tau = Q_{\lim} \leq mn. \end{cases} \quad (11)$$

Формирование кода-номера возможно и на основе рекуррентной схемы путем добавления очередного элемента фрагмента изображения. Процесс формирования кода-номера задается следующими выражениями:

$$N_1 = a_1; \quad (12)$$

$$N_{\tau} = N_{\tau-1}s_{\tau} + a_{\tau} = N_{\tau-1}g_{\tau-m\left[\frac{\tau-1}{m}\right]} + a_{\tau}, \quad (13)$$

где N_{τ} , $N_{\tau-1}$ – код-номер для τ -го и $(\tau-1)$ -го элементов.

Для исключения переполнения кодового слова перед каждым добавлением к коду-номеру $N_{\tau-1}$ очередного элемента a_{τ} проводится проверка на переполнение кодового слова, которая с учетом соотношения $\tau = Q$ определяется с помощью дополнительной величины T_{τ} на основе выражения (7) с учетом выполнения неравенства (8).

Действительно, поскольку выполняется неравенство $T_{\tau} \geq N_{\tau}$, тогда $N_{\tau} \leq 2^M - 1$.

Процесс формирования кода-номера N заканчивается тогда, когда будет обработан последний Q -й элемент:

$$N = N_Q = N_{Q-1}s_Q + a_Q = N_{Q-1}g_{Q-m\left[\frac{Q-1}{m}\right]} + a_Q \quad (14)$$

при $T_Q \leq 2^M - 1$ и $Q \leq mn$.

В данном случае Q -й элемент будет равен максимальному количеству элементов $Q_{\lim}$ фрагмента изображения, принимающих участие в формировании кода-номера, рассчитанному по формуле (9).

3. Выводы

Разработанный метод криптосемантического представления изображений на основе плавающей схемы полиадического кодирования в базисе по верхним границам обеспечивает:

- одновременное выполнение процессов сжатия и шифрования (кодирования) видеоданных;
- исключение избыточности одновременно без внесения погрешности;
- уменьшение количества незначимых элементов (незначимых нулевых бит) в начале каждой битовой последовательности кодов-номеров;
- формирование кодограмм равномерной длины на основе переменного (заранее неопределенного) количества элементов исходного изображения;
- дополнительное снижение исходного объема изображений.

Литература: 1. Баранник В.В. Метод криптосемантического представления изображений на основе комбинированного подхода / В.В. Баранник, С.А. Сидченко, В.В. Ларин // Сучасна спеціальна техніка. 2010. №3 (22). С. 33–38. 2. Баранник В.В. Методологічні основи криптосемантичного представлення відеозображень в інформаційних комунікаціях / В.В. Баранник, С.О. Сідченко, В.В. Ларін // Наукові технології. К., 2012. № 3(15). С. 78-82. 3. Баранник В.В. Методологическая база криптокомпрессионного представления видеоинформационных ресурсов / В.В. Баранник, С.А. Сидченко, В.В. Ларин // Захист інформації. Квітень–червень 2013. Том 15, № 2. С. 97–104. 4. Barannik V.V. The methodological base of cryptocompression presentation of videoinformation resources / V. V. Barannik, S. A. Sidchenko, V. V. Larin // XII International Conference CADSM'2013 [IEEE The Experience of Designing and Application of CAD Systems in Microelectronics] (Lviv, Ukraine, February 19–23, 2013). Lviv Polytechnic National University, 2013. P. 27–28. 5. Баранник В.В. Метод дешифруемо-стойкого представления изображений / В.В. Баранник, С.А. Сидченко, В.В. Ларин // Сучасна спеціальна техніка. 2011. №1 (24). С. 24–29. 6. Barannik V.V. The Decoded-proof Presentation of Images on the Basis of the Polyadical Encoding Systems / V. V. Barannik, S. A. Sidchenko, V. V. Larin // XIth International Conference CADSM 2011, The Experience of Designing and Application of CAD Systems in Microelectronics, Lviv-Polyana, Ukraine, Lviv Polytechnic National University, February 23–25, 2011. P. 182. 7. Баранник В.В. Методика статистического тестирования дешифруемо-стойкого представления изображений / В.В. Баранник, С.А. Сидченко, В.В. Ларин // Сучасна спеціальна техніка. 2011. №2 (25). С. 13–20. 8. Сидченко С.А. Способ представления изображений, стойких к дешифрованию на основе плавающей схемы кодирования / С.А. Сидченко // Системи озброєння і військова техніка. 2011. Вип. 3 (27). С. 68–70. 9. Barannik V.V. Methodology Constructions of Floating Chart of Decoded-proof Presentation of Images / V. V. Barannik, S. A. Sidchenko // International Conference TCSET'2012 [Modern problems of radio engineering, telecommunications and computer science] (Lviv-Slavsko, Ukraine, February 21–24, 2012). Lviv Polytechnic National University, 2012. P. 437.

Транслитерированный список литературы: 1. *Barannik V.V.* Metod kriptosemanticheskogo predstavlenija izobrazhenij na osnove kombinirovannogo podhoda / V.V. Barannik, S.A. Sidchenko, V.V. Larin // Suchasna special'na tehnika. 2010. №3 (22). S. 33 – 38. 2. *Barannik V.V.* Metodologichni osnovy kriptosemantychnogo predstavlenija videozobrazhen' v informacijnyx komunikacijax / V.V. Barannik, S.O. Sidchenko, V.V. Larin / / Naukoyemni tehnologiyi. K., 2012. # 3(15). S. 78-82. 3. *Barannik V.V.* Metodologicheskaja baza kriptokompressionnogo predstavlenija videoinformacionnyh resursov / V.V. Barannik, S.A. Sidchenko, V.V. Larin // Zaxy'st informaciyi. Kvitěn'-cherven' 2013. Tom 15, # 2. S. 97–104. 4. *Barannik V.V.* The methodological base of cryptocompression presentation of videoinformation resources / V. V. Barannik, S. A. Sidchenko, V. V. Larin // XII International Conference CADSM'2013 [IEEE The Experience of Designing and Application of CAD Systems in Microelectronics] (Lviv, Ukraine, February 19–23, 2013). Lviv Polytechnic National University, 2013. P. 27–28. 5. *Barannik V.V.* Metod deshifruemo-stojkogo predstavlenija izobrazhenij / V.V. Barannik, S.A. Sidchenko, V.V. Larin // Suchasna special'na tehnika. 2011. #1 (24). S. 24 – 29. 6. *Barannik V.V.* The Decoded-proof Presentation of Images on the Basis of the Polyadycal Encoding Systems / V. V. Barannik, S. A. Sidchenko, V. V. Larin // XIth International Conference CADSM 2011, The Experience of Designing and Application of CAD Systems in Microelectronics, Lviv-Polyana, Ukraine, Lviv Polytechnic National University, February 23 – 25, 2011. P. 182. 7. *Баранник В.В.* Методика статистического тестирования дешифрируемо-стойкого представления изображений / В.В. Баранник, С.А. Сидченко, В.В. Ларин // Сучасна спеціальна техніка. 2011. №2 (25). С. 13 – 20. 8. *Sidchenko S.A.* Sposob predstavlenija izobrazhenij stojkih k deshifirovaniju na osnove plavajushhej shemy kodirovanija / S.A. Sidchenko // Systemy

ozbroyennya i vijs'kova tehnika. 2011. Вип. 3 (27). С. 68–70. 9. *Barannik V.V.* Methodology Constructions of Floating Chart of Decoded-proof Presentation of Images / V. V. Barannik, S. A. Sidchenko // International Conference TCSET'2012 [Modern problems of radio engineering, telecommunications and computer science] (Lviv-Slavsko, Ukraine, February 21–24, 2012). Lviv Polytechnic National University, 2012. P. 437.

Поступила в редколлегию 17.10.2015

Рецензент: д-р техн. наук, проф. Безрук В.М.

Баранник Владимир Викторович, д-р техн. наук, профессор, начальник кафедры Харьковского университета Воздушных Сил им. И. Кожедуба. Адрес: Украина, 61000, Харьков, ул. Сумская, 77/79, тел. 050-303-89-71.

Тупица Иван Михайлович, заместитель начальника учебно-тренировочного комплекса Харьковского университета Воздушных Сил им. И. Кожедуба. Адрес: Украина, 61000, Харьков, ул. Сумская, 77/79, тел. 096-795-57-39.

Сидченко Сергей Александрович, канд.техн. наук, старший научный сотрудник научного центра Харьковского университета Воздушных Сил им. И. Кожедуба. Адрес: Украина, 61000, Харьков, ул. Сумская, 77/79, тел. 066-299-82-73.

Barannik Vladimir Victorovich, doctor of sciences by technical, professor, chief of department of the Kharkov university of Air Force.

Tupitsya Ivan Mikhailovich, Dep.chief of educational-training centre of the Kharkov university of Air Force.

Sidchenko Sergey Aleksandrovich, philosophy doctor by technical, senior research worker, senior research worker of scientific center of the Kharkov university of Air Force.

МОДЕЛЬ ОЦЕНКИ ЦЕЛОСТНОСТИ ДИНАМИЧЕСКОГО ВИДЕОИНФОРМАЦИОННОГО РЕСУРСА В СЛУЧАЕ МЕЖТРАНСФОРМАНТНОЙ ОБРАБОТКИ

БАРАННИК В.В., ШУЛЬГИН С.С.

Обосновывается необходимость повышения безопасности динамических видеоинформационных ресурсов. Показывается направление для повышения эффективности синтаксического представления последовательности Р-кадров на основе межтрансформантной обработки их базовых структурных единиц – дифференциально-описанных спектрограмм. Раскрывается направление дополнительного снижения интенсивности кодового представления видеопотока путем сокращения межкадровой (временной) психовизуальной избыточности на уровне обработки дифференциально-описанных спектрограмм, что обусловлено особенностями ограниченной чувствительности зрительной системы относительно коррекции отдельных частотных составляющих. Излагаются этапы построения модели оценки целостности динамического видеоинформационного ресурса.

Ключевые слова: кадр, трансформанта, видеопоток, ресурс, обработка, код, технология.

1. Введение

Современное развитие кибернетического пространства вызывает необходимость обеспечения безопасности информационных ресурсов. Особенно это важно для видеоинформационных ресурсов. Здесь приходится сталкиваться с проблемными аспектами, вызванными необходимостью одновременного решения вопросов относительно сокращения избыточности, снижения битовой интенсивности, повышения конфиденциальности, целостности и доступности видеоинформации [1 - 3].

Одно из направлений таких направлений исследований заключается в использовании селективных методов защиты видеоинформации, совмещенных с базовыми технологиями MPEG и H264. В случае обработки видеопотоков (динамических видеоинформационных ресурсов) вариант селективного подхода заключается в закрытии базового кадра [3; 4]. Тогда значимая нагрузка на обеспечение доступности и целостности возлагается на процесс обработки последовательности предсказанных кадров (Р-кадров) [3].

В то же время такой подход обработки потока видеокадров связан с наличием дисбаланса между уровнем снижения битовой интенсивности и уровнем внесения потерь целостности информации. Поэтому актуальным требованием, определяющим *научно-прикладную задачу*, является создание систем эффективного синтаксического представления динамических видео-

информационных ресурсов в режимах сохранения необходимого уровня целостности информации. Для решения такой задачи необходимо построение технологий обработки ДВИР с использованием методов, устраняющих межкадровую избыточность на базе структурно-комбинаторного подхода. Одной из реализаций такого подхода в случае обработки динамических видеоинформационных ресурсов является метод обработки слотов Р-кадров с выявлением межтрансформантных структурных закономерностей [5]. Здесь возникает потребность в оценке целостности информации в режиме снижения битовой интенсивности видеопотока. Поэтому *цель исследований* заключается в создании модели для оценки целостности динамических видеоинформационных ресурсов в случае межтрансформантной обработки слотов Р-кадров.

2. Основная часть исследований

Для повышения эффективности формирования и обработки кадров Р-типа *предлагается* предварительно осуществлять трансформирование видеокadra из пространственно-временного в пространственно-спектральное описание [5]. После получения трансформант двумерного преобразования проводится построение дифференциального представления на основе формирования величин разностей между соответствующими компонентами по позициям в кадрах.

Отсюда последовательность исходных кадров в группе X_T в структурном описании выражается через ДОС на основе такого выражения:

$$X_T = \{Y_T; Z_T\},$$

где Z_T - последовательность кадров-знаков, несущих информацию о знаках компонент трансформированных кадров.

Соответственно группа Y_T трансформированных кадров $Y(\tau)$, $Y_T = \{Y(\tau)\}$, $\tau = \overline{1, T}$ формируется как

$$Y_T = Y(1) \cup E_{T-1} = Y(1) \cup \bigcup_{\chi=1}^{w_{стр}} \bigcup_{\gamma=1}^{w_{стб}} \bigcup_{k=1}^w \bigcup_{\ell=1}^w E(\chi; \gamma)^{(k, \ell)}.$$

Здесь $Y(1)$ – базовый трансформированный кадр; E_{T-1} – последовательность дифференциально-представленных трансформированных кадров $E(\tau)$, $\tau = \overline{2, T}$.

В то же время последовательность E_{T-1} образуется совокупностью слотов $E(T-1)_{\chi, \gamma}^{(2)}$, а именно:

$$E_{T-1} = \bigcup_{\chi=1}^{w_{стр}} \bigcup_{\gamma=1}^{w_{стб}} E(T-1)_{\chi, \gamma}^{(2)}.$$

При этом, исходя из условий структурирования группы кадров и процесса предварительной обработки, слот $E(T-1)_{\chi,\gamma}^{(2)}$ формируется как двумерный пакет дифференциально описанных спектрограмм $E(\chi;\gamma)^{(k,\ell)}$. Отсюда выполняется соотношение:

$$E(T-1)_{\chi,\gamma}^{(2)} = \{E(\chi;\gamma)^{(k,\ell)}\}_{\substack{k=1,\overline{w} \\ \ell=1,\overline{w}}}.$$

Дифференциально описанная спектрограмма (ДОС) $E^{(k,\ell)}$ представляет собой срез вдоль слота по координате $(k;\ell)$ в каждой трансформанте, т.е. $E^{(k,\ell)} = \{e(2)^{(k,\ell)}, \dots, e(\tau)^{(k,\ell)}, \dots, e(T)^{(k,\ell)}\}$. Структурной характеристикой ДОС является динамический диапазон $d_e^{(k,\ell)}$ ее элементов. Поскольку в общем случае межтрансформантные разности $e(\tau)^{(k,\ell)}$ принимают как положительные, так и отрицательные значения, то величина $d_e^{(k,\ell)}$ без учета знака находится по формуле $d_e^{(k,\ell)} = \max_{2 \leq \tau \leq T} \{|e(\tau)^{(k,\ell)}|\}$, где $d_e^{(k,\ell)}$ - динамический диапазон элементов $(k;\ell)$ -й дифференциально описанной спектрограммы без учета знака величин $e(\tau)^{(k,\ell)}$; $|e(\tau)^{(k,\ell)}|$ - абсолютное значение межтрансформантной разности между $(\tau-1)$ -й и τ -й трансформантами.

Для выстроенной структуры потока видеок кадров формирование эффективного синтаксического представления нужно проводить по структурно-комбинаторному принципу. В этом случае **предлагается** разрабатывать **направление**, базирующееся на дополнительном выявлении закономерностей, основанных на учете [5] психовизуальных особенностей восприятия незначительных изменений в последовательности кадров.

При этом предлагается устранять психовизуальную избыточность в направлении временной оси. Для

этого нужно использовать технологию, базирующуюся на коррекции значения сохраняются (обрабатываются) без коррекции (рис. 1).

Элементы $e(\tau)_{inf}^{(k,\ell)}$ первого типа являются опорными и образуют информативную дифференциально описанную спектрограмму (ИДОС) $E_{inf}^{(k,\ell)}$, т.е.

$$E_{inf}^{(k,\ell)} = \{e(1)_{inf}^{(k,\ell)}; \dots; e(\tau)_{inf}^{(k,\ell)}; \dots; e(n_{inf})_{inf}^{(k,\ell)}\}.$$

В данной формуле n_{inf} - количество информативных элементов в ИДОС.

Информативная ДОС обрабатывается без коррекций ее элементов.

Соответственно второй тип образуют элементы $e(\tau)_{int}^{(k,\ell)}$, значения которых на приемной стороне будут интерполироваться по информативным. Такие элементы формируют интерполяционную составляющую $E_{int}^{(k,\ell)}$ ДОС. Это задается соотношением:

$$E_{int}^{(k,\ell)} = \{e(1)_{int}^{(k,\ell)}; \dots; e(\tau)_{int}^{(k,\ell)}; \dots; e(n_{int})_{int}^{(k,\ell)}\}.$$

Здесь n_{int} - количество интерполируемых элементов в ДОС

По условию интерполяции элементы составляющей $E_{int}^{(k,\ell)}$ распределяются между информативными элементами ИДОС, как показано на рис. 1.

С учетом механизма выделения интерполяционной составляющей дифференциально описанная спектрограмма будет выражаться следующим соотношением (рис. 2):

$$E^{(k,\ell)} = E_{inf}^{(k,\ell)} \cup F_{int}(E_{inf}^{(k,\ell)}; v_{inf}; v_{int}) = E_{inf}^{(k,\ell)} \cup E_{int}^{(k,\ell)}$$

где $F_{int}(E_{inf}^{(k,\ell)}; v_{inf}; v_{int})$ - функционал реконструкции элементов интерполяционной составляющей $E_{int}^{(k,\ell)}$

ДОС. $E_{int}^{(k,\ell)} = F_{int}(E_{inf}^{(k,\ell)})$.

Информативные элементы, $E_{inf}^{(k,\ell)}$

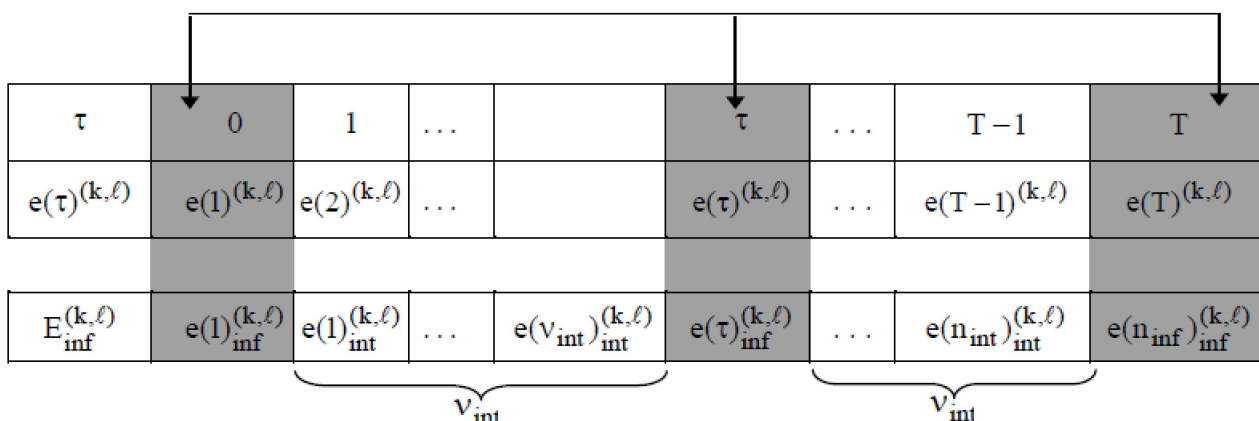


Рис. 1. Схема варианта формирования информативной ДОС

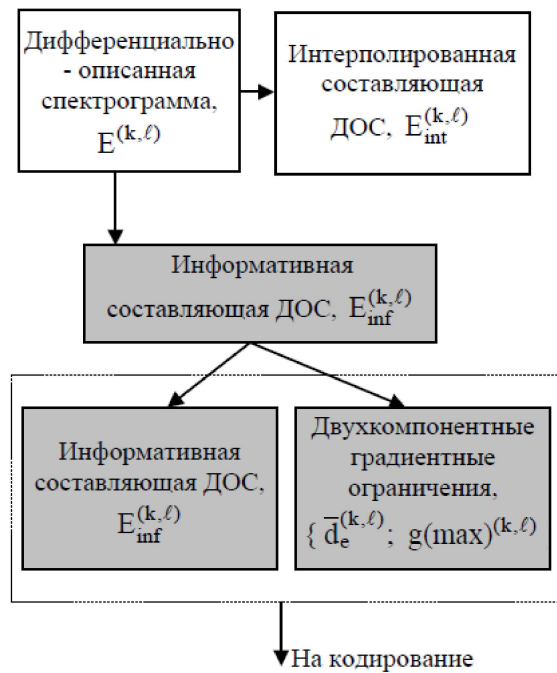


Рис. 2. Схема формирования синтаксического описания ДОС

Данный вариант основывается на возможности межкадровой интерполяции элементов внутри ДОС за счет свойств функционала $F(E^{(k, \ell)})_{\text{apг}}$.

Согласно особенностям интерполяции ДОС соответствующая технология, заданная функционалом $F_{\text{int}}(E_{\text{inf}}^{(k, \ell)}; v_{\text{inf}}; v_{\text{int}})$, определяется таким набором параметров (см.рис. 1):

- v_{int} - количество интерполируемых элементов между информативными элементами;
- v_{inf} количество информативных элементов между двумя интерполируемыми элементами.

Для сокращения вычислительной сложности и увеличения количества интерполируемых элементов **предлагается** выбирать режим, когда:

- 1) участки интерполирования являются равномерными, т.е. $v_{\text{int}} = \text{const}$, с одним базовым элементом между ними, т.е. $v_{\text{inf}} = 1$;
- 2) реконструкция интерполируемых элементов проводится на основе усреднения информативных элементов.

При этом величины n_{inf} и n_{int} для выбранного режима интерполяции определяются следующим образом: $n_{\text{inf}} = \lceil (T-1)/(v_{\text{int}}+1) \rceil$; $n_{\text{int}} = \mu_{\text{int}} v_{\text{int}}$.

Здесь μ_{int} - количество интерполируемых участков в ДОС.

Для заданной позиции τ интерполируемого элемента $e(\tau)_{\text{int}}^{(k, \ell)}$ допускается определение его позиции относительно участка интерполирования. В этом случае получим элементы $e(\tau; \phi)_{\text{int}}^{(k, \ell)}$ - интерполируемый элемент на ϕ -й позиции v -го участка интерполяции для $(k; \ell)$ -й ДОС.

Если $v_{\text{inf}} = 1$ и $v_{\text{int}} = \text{const}$, то выражение для пересчета индекса τ позиции в ДОС в индекс ϕ позиции для участка интерполяции будет задаваться формулой $\phi = \tau - \mu - (\mu - 1)v_{\text{int}}$.

Номер μ участка интерполяции определяется следующим образом: $\mu = \lceil \tau / (v_{\text{int}} + 1) \rceil$.

Тогда получим $\phi = \tau - \lceil \tau / (v_{\text{int}} + 1) \rceil (v_{\text{int}} + 1) + v_{\text{int}}$.

Данные выражения позволяют для заданного индекса позиции интерполируемого элемента в ДОС и длины участка интерполяции получить координату интерполируемого элемента для участка интерполяции.

Для информативной ДОС в результате процесса интерполяции количество комбинаций $Q(n_{\text{inf}})_e^{(k, \ell)}$ определяется только по информативным элементам. В то же время величина $Q(n_{\text{inf}})_e^{(k, \ell)}$ определяется как количество различных информативных ДОС заданной длины n_{inf} в рамках динамического диапазона. Значит, значение величины $Q(n_{\text{inf}})_e^{(k, \ell)}$ зависит от количества n_{inf} элементов и значения их динамического диапазона $\bar{d}_{\text{inf}}^{(k, \ell)}$. Поэтому для оценки количества информации определим величину динамического диапазона $\bar{d}_{\text{inf}}^{(k, \ell)}$ информативных элементов ДОС. Возможны два варианта:

1. Когда динамический диапазон $\bar{d}_{\text{inf}}^{(k, \ell)}$ находится с учетом только информативных элементов, т.е.

$$\bar{d}_{\text{inf}}^{(k, \ell)} = |e_{\text{inf, min}}^{(k, \ell)} - e_{\text{inf, max}}^{(k, \ell)}| + 1.$$

При этом поскольку обрабатываемых элементов меньше, чем количество обрабатываемых элементов для исходной ДОС, т.е.

$$n_{\text{inf}} < T - 1,$$

то выполняются неравенства:

$$|e_{\text{inf, min}}^{(k, \ell)}| = \min_{1 \leq \tau \leq n_{\text{inf}}} \{e(\tau)_{\text{inf}}^{(k, \ell)}\} \leq |e_{\text{min}}^{(k, \ell)}|;$$

$$|e_{\text{inf, max}}^{(k, \ell)}| = \min_{1 \leq \tau \leq n_{\text{inf}}} \{e(\tau)_{\text{inf}}^{(k, \ell)}\} \leq |e_{\text{max}}^{(k, \ell)}|.$$

Отсюда динамический диапазон $\bar{d}_{\text{inf}}^{(k,\ell)}$ ИДОС не будет превышать динамический диапазон $\bar{d}_e^{(k,\ell)}$ исходной ДОС, а именно: $\bar{d}_{\text{inf}}^{(k,\ell)} \leq \bar{d}_e^{(k,\ell)}$.

Поэтому количество комбинаций $Q(n_{\text{inf}})_e^{(k,\ell)}$ для информативной ДОС будет меньше, чем количество комбинаций $Q(T-1)_e^{(k,\ell)}$ для исходной ДОС, что задается неравенством

$$Q(n_{\text{inf}})_e^{(k,\ell)} \leq Q(T-1)_e^{(k,\ell)}.$$

Следовательно, происходит дополнительное снижение битовой интенсивности потока кадров. В то же время такой подход имеет недостаток с позиции обеспечения целостности реконструируемых интерполируемых элементов. Это обусловлено тем, что динамический диапазон несет базовую информацию об элементах ДОС. Поэтому в случае потери информации о динамическом диапазоне интерполируемых элементов произойдет искажение их значений в процессе реконструкции.

2. Для исключения выявленного недостатка *предлагается* оценивать динамический диапазон $\bar{d}_{\text{inf}}^{(k,\ell)}$ информативной составляющей ДОС по всем элементам исходной ДОС. Тогда величина $\bar{d}_{\text{inf}}^{(k,\ell)}$ будет определяться по формуле

$$\bar{d}_{\text{inf}}^{(k,\ell)} = |e_{\text{min}}^{(k,\ell)} - e_{\text{max}}^{(k,\ell)}| + 1 = \bar{d}_e^{(k,\ell)}.$$

При таком варианте количество комбинаций для информативной ДОС вычисляется с использованием соотношения

$$Q(n_{\text{inf}})_e^{(k,\ell)} = (|e_{\text{min}}^{(k,\ell)} - e_{\text{max}}^{(k,\ell)}| + 1)^{n_{\text{inf}}} = (\bar{d}_e^{(k,\ell)})^{n_{\text{inf}}}.$$

Из анализа полученного выражения можно заключить, что за счет интерполирования ДОС и выполнения условия $(n_{\text{inf}} < T-1)$ количество комбинаций $Q(n_{\text{inf}})_e^{(k,\ell)}$ будет меньше, чем количество комбинаций $Q(T-1)_e^{(k,\ell)}$ для исходной ДОС, т.е.

$$Q(n_{\text{inf}})_e^{(k,\ell)} \leq Q(T-1)_e^{(k,\ell)}.$$

При этом выигрыш в количестве двоичных разрядов $V(n_{\text{inf}})_e^{(k,\ell)}$ на представление информативной ДОС относительно количества разрядов $V(T-1)_e^{(k,\ell)}$ на представление исходной ДОС составит следующую величину:

$$V(T-1)_e^{(k,\ell)} - V(n_{\text{inf}})_e^{(k,\ell)} =$$

$$\begin{aligned} &= ((T-1)[\log_2 \bar{d}_e^{(k,\ell)}] + 1) - (n_{\text{inf}}[\log_2 \bar{d}_e^{(k,\ell)}] + 1) = \\ &= ((T-1) - n_{\text{inf}})[\log_2 \bar{d}_e^{(k,\ell)}]. \end{aligned}$$

Данный выигрыш будет тем больше, чем меньше величина n_{inf} и значение динамического диапазона $\bar{d}_e^{(k,\ell)}$ элементов ДОС.

Следовательно, в результате интерполяции дифференциально описанной spectroграммы с последующим ее синтаксическим представлением по структурно-комбинаторному подходу достигается сокращение количества межкадровой психовизуальной избыточности.

Оценим технологию интерполяции ДОС с позиции сохранения целостности информационного ресурса. Для этого требуется оценить тип происхождения и характер искажений, которые образуются в процессе интерполяции дифференциально описанной spectroграммы.

Предпосылками для появления искажений является то, что информация об интерполируемых элементах $e(\tau)_{\text{int}}^{(k,\ell)}$ составляющей ДОС формируется на приемной стороне по ближайшим опорным (информативным) элементам $e(\tau)_{\text{inf}}^{(k,\ell)}$. При этом значения реконструируемых элементов $e'(\tau)_{\text{inf}}^{(k,\ell)}$ могут не совпадать с исходными, т.е. в общем случае выполняется неравенство $e'(\tau)_{\text{inf}}^{(k,\ell)} \neq e(\tau)_{\text{inf}}^{(k,\ell)}$.

В соответствии с принятым режимом интерполяции ближайшими информативными элементами являются элементы на границах участка интерполяции. Позиции $\tau(\mu)_0$, $\tau(\mu)_{v_{\text{int}}+1}$ граничных информативных элементов для μ -го участка интерполяции определяются соответственно по формулам:

$$\tau(\mu)_0 = \mu + (\mu - 1)v_{\text{int}}, \quad \text{для } \phi = 1;$$

$$\tau(\mu)_{v_{\text{int}}+1} = \mu(v_{\text{int}} + 1) + 1, \quad \text{для } \phi = v_{\text{int}}.$$

Реконструкция интерполируемых элементов $e'(\mu; \phi)_{\text{int}}^{(k,\ell)}$ на приемной стороне по граничным информативным элементам $e(\tau(\mu)_0)_{\text{inf}}^{(k,\ell)}$ и $e(\tau(\mu)_{v_{\text{int}}+1})_{\text{inf}}^{(k,\ell)}$ для μ -го участка интерполяции задается следующим соотношением:

$$e'(\mu; \phi)_{\text{int}}^{(k,\ell)} = \frac{e(\tau(\mu)_0)_{\text{inf}}^{(k,\ell)} + e(\tau(\mu)_{v_{\text{int}}+1})_{\text{inf}}^{(k,\ell)}}{2}.$$

Аналогичным образом восстанавливаются интерполируемые элементы для других участков интерполяции. При этом реконструкция интерполируемых эле-

ментов проводится независимо от других элементов. Данная особенность блокирует возможность распространения ошибок в одном интерполируемом элементе на другие элементы как текущего участка так и других участков интерполяции. Значит, в случае сохранения информации об информативных элементах ДОС исключается возможность появления лавинного эффекта относительно распространения искажений.

Ошибка $\varepsilon(\mu; \phi)^{(k, \ell)}$ в процессе реконструкции интерполируемого элемента $e'(\mu; \phi)_{\text{int}}^{(k, \ell)}$ называется ошибкой интерполирования. Такая ошибка зависит от степени отклонения значения элемента $e'(\mu; \phi)_{\text{int}}^{(k, \ell)}$ от значения исходного интерполируемого элемента $e(\mu; \phi)_{\text{int}}^{(k, \ell)}$, а именно:

$$\varepsilon(\mu; \phi)^{(k, \ell)} = |e(\mu; \phi)_{\text{int}}^{(k, \ell)} - e'(\mu; \phi)_{\text{int}}^{(k, \ell)}|.$$

В соответствии с данным соотношением наибольшее значение модуля разности $|e(\mu; \phi)_{\text{int}}^{(k, \ell)} - e'(\mu; \phi)_{\text{int}}^{(k, \ell)}|$ не будет превышать величины динамического диапазона $\bar{d}_e^{(k, \ell)}$ дифференциально описанной спектрограммы, т.е.

$$|e(\mu; \phi)_{\text{int}}^{(k, \ell)} - e'(\mu; \phi)_{\text{int}}^{(k, \ell)}| \leq \bar{d}_e^{(k, \ell)}.$$

Отсюда значение ошибки интерполяции для предложенного структурно-комбинаторного подхода относительно синтаксического представления информативной ДОС будет ограничено величиной $\bar{d}_e^{(k, \ell)}$:

$$\varepsilon(\mu; \phi)^{(k, \ell)} \leq \bar{d}_e^{(k, \ell)}.$$

Для оценки целостности видеоинформационного ресурса используется количественный показатель степени потерь качества реконструируемых видеок кадров с позиции их визуального восприятия. Одним из таких показателей является пиковое отношение сигнал/шум h . Формула для определения h при известном значении δ_{int} среднеквадратического отклонения реконструируемого видеок кадра относительно исходного задается следующим образом:

$$h = 20 \lg(256/\delta_{\text{int}}).$$

Здесь значение δ_{int} обусловлено ошибками интерполирования ДОС. Тогда, если оценка среднеквадратического отклонения проводится для отдельной спектрограммы, формулы для ее среднего $\delta_{\text{int}}^{(k, \ell)}$ и максимального $\delta(\max)_{\text{int}}^{(k, \ell)}$ значений имеют соответственно такой вид:

$$\delta_{\text{int}}^{(k, \ell)} = \sqrt{\frac{\sum_{\mu=1}^{\mu_{\text{int}}} \sum_{\phi=1}^{\phi_{\text{int}}} (\varepsilon(\mu; \phi)^{(k, \ell)})^2}{T-1}};$$

$$\delta(\max)_{\text{int}}^{(k, \ell)} = \bar{d}_e^{(k, \ell)} \sqrt{n_{\text{int}}/(T-1)}.$$

Оценка величины h для разных режимов интерполяции ДОС представлена в виде диаграмм на рис. 3.

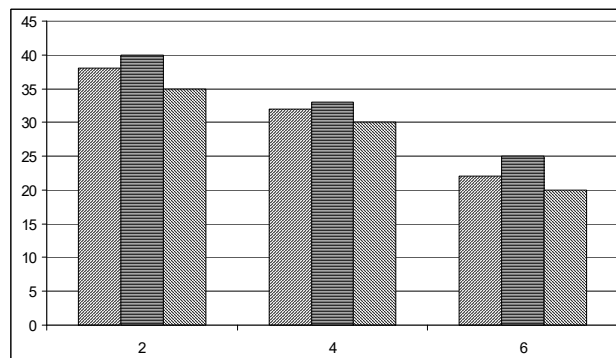


Рис. 3. Диаграммы зависимости величины h_{min} от

$$n_{\text{int}} \text{ и } \bar{d}_e^{(k, \ell)}$$

Оценка проводилась в зависимости от количества n_{int} интерполируемых элементов и значения динамического диапазона $\bar{d}_e^{(k, \ell)}$ ДОС. По результатам анализа полученных диаграмм можно утверждать следующее:

- с одной стороны, степень потери качества реконструируемых видеок кадров с позиции оценки ПОСШ для разных режимов интерполяции находится на допустимом уровне (не ниже 25 дБ). Это создает потенциал для реализации предложенного структурно-комбинаторного подхода в системах обеспечения безопасности динамических ВИР;

- с другой стороны, с ростом динамического диапазона элементов ДОС величина ПОСШ резко снижается (в среднем на 15 дБ при увеличении длины ДОС в 2 раза). Это ограничивает возможности по решению вопросов дисбаланса между доступностью и целостностью ВИР.

Поэтому можно заключить, что для дальнейшего повышения безопасности динамического ВИР на основе предложенного подхода по обработке потока видеок кадров необходимо создать технологии для:

- 1) уменьшения зависимости количества устраняемой избыточности от количества интерполируемых элементов ДОС;
- 2) снижения уровня динамического диапазона элементов дифференциально описанной спектрограммы, как параметра, влияющего одновременно на повыше-

ние количества исключаемой избыточности и уровня целостности ВИР.

3. Выводы

1. В процессе обработки Р-кадров, обеспечивающей дополнительное снижения интенсивности их кодового представления, устраняются следующие виды избыточности:

1) пространственная избыточность, учитывающая наличие внутрикадровых закономерностей, а именно когерентность свойств фрагментов кадров;

2) временная избыточность, которая основывается на выявлении межкадровых закономерностей, а именно наличие корреляционных закономерностей между соответствующими компонентами трансформант смежных кадров;

3) психовизуальная избыточность, т.е. избыточность вызванная особенностями зрительной системы по восприятию видеоизображений. Такой вид избыточности учитывается как для внутрикадровой обработки, так и для межкадровой. На внутрикадровом уровне учитывается меньшая чувствительность зрительной системы относительно коррекции высокочастотных компонент;

4) межкадровая (временная) психовизуальная избыточность на уровне обработки дифференциально описанных спектрограмм, что обусловлено особенностями ограниченной чувствительности зрительной системы относительно коррекции отдельных частотных составляющих.

2. Обоснован и построен подход для эффективного синтаксического описания дифференциально описанных спектрограмм, являющихся составляющими слотов Р-кадров, на основе структурно-комбинаторного представления. Здесь учитываются два направления, связанных с учетом психовизуальных особенностей восприятия незначительных изменений в последовательности кадров. В данном случае дополнительно устраняется психовизуальная избыточность в направлении временной оси. Для этого используется технология, базирующаяся на коррекции элементов ДОО под особенности модели зрительного восприятия путем интерполяции элементов ДОО.

3. Построена модель оценки целостности динамического видеоинформационного ресурса путем нахождения нижней границы пикового отношения сигнал шум реконструируемых ДОО относительно исходных с учетом процесса интерполяции.

По результатам анализа полученных диаграмм можно утверждать, что степень потери качества реконструируемых видеокадров с позиции оценки ПОСШ для разных режимов интерполяции находится на допустимом уровне (не ниже 25 дБ). Это создает потенциал для реализации предложенного структурно-комбина-

торного подхода в системах обеспечения безопасности динамических ВИР.

Литература: 1. Андреев А. Применение видеоконференцсвязи в Вооружённых силах иностранных государств / А.Андреев, В.Аржанов, К.Семёнов // Зарубежное военное обозрение. 2008. № 7. С.19 – 25. 2. Баранник В.В. Метод повышения информационной безопасности в системах видеомониторинга кризисных ситуаций / В.В. Баранник, Ю.Н. Рябуха, О.С. Кулица // Монография. Черкассы, 2015. 143 с. 3. Баранник В.В. Обоснование значимых (актуальных) угроз безопасности видеоинформационного ресурса систем видеоконференцсвязи профильных систем управления / В.В. Баранник, А.В. Власов // Информационно-управляющие системы на железнодорожном транспорте. 2014. № 3. С. 23 – 27. 4. Баранник В.В. Селективный метод шифрования видеопотока в телекоммуникационных системах на основе приховування базового I-кадру / В.В. Баранник, Д.І. Комолов, Ю.М. Рябуха // Наукоємні технології. 2015. № 2. С. 69 – 77. 5. Баранник В.В. Модель оценки информативности слота Р-кадров на основе выявления структурно-градиентных межатрансформантных ограничений / В.В. Баранник, С.С. Шульгин // АСУ и приборы автоматики. 2015. №171. С. 12 – 21.

Транслитерированный список литературы: 1. Andreev A. Primenenie videokonferencsvjazi v Vooruzhjonnyh silah inostrannyh gosudarstv / A.Andreev, B.Arzhanov, K.Semjonov // Zarubezhnoe voennoe obozrenie. 2008. № 7. S.19 – 25. 2. Barannik V.V. Metod povyshenija informacionnoj bezopasnosti v sistemah videomonitoringa krizisnyh situacij / V.V. Barannik, Ju.N. Rjabuha, O.S. Kulica // Monografija. Cherkassy, 2015. 143 s. 3. Barannik V.V. Obosnovanie znachimyh (aktual'nyh) ugroz bezopasnosti videoinformacionnogo resursa sistem videokonferencsvjazi profil'nyh sistem upravlenija / V.V. Barannik, A.V. Vlasov // Informacionno-upravljajushhie sistemy na zheleznodorozhnom transporte. 2014. № 3. S. 23 – 27. 4. Barannik V.V. Selektivnij metod shifruvannja videopotoku v telekomunikacijnih sistemah na osnovi prihovuvannja bazovogo I-kadru / V.V. Barannik, D.I. Komolov, Ju.M. Rjabuha // Naukoemni tehnologii. 2015. № 2. S. 69 – 77. 5. Barannik V.V. Model' ocenki informativnosti slotu R-kadrov na osnove vyjavlenija strukturno-gradientnyh mezhttransformantnyh ogranichenij / V.V. Barannik, S.S. Shul'gin // ASU i pribory avtomatiki. №171. 2015. S. 12 – 21.

Поступила в редколлегия 11.11.2015

Рецензент: д-р техн. наук, проф. Безрук В.М.

Баранник Владимир Викторович, д-р техн. наук, профессор, начальник кафедры Харьковского университета Воздушных Сил им. И. Кожедуба. Научные интересы: системы, технологии преобразования, кодирования, защиты и передачи информации, семантической обработки изображений. Адрес: Украина, 61023, Харьков - 23, ул. Сумская, 77/79, тел. 8 050-3038971.

Шульгин Сергей Сергеевич, соискатель Киевского Национального авиационного университета. Научные интересы: обработка видеоинформации и безопасность инфокоммуникационных систем. Адрес: Украина, Киев, пр. Космонавта Комарова, 1.

ТЕХНОЛОГИЯ ФОРМИРОВАНИЯ КОДОВОЙ КОНСТРУКЦИИ ДЛЯ СЕЛЕКТИВНОГО МЕТОДА ОБРАБОТКИ ВИДЕОДАНЫХ

КОМОЛОВ Д.И.

Рассматривается селективный метод шифрования видеокадров, основанный на скрытии базового I-кадра. Работа данного метода базируется на основе обработки группы кадров, с учетом алгоритма MPEG, который реализован по принципу формирования последовательности видеокадров разных типов. Разрабатывается технология формирования кодовой конструкции для селективного метода обработки видеоданных. Развивается технология формирования битового кода в селективном методе шифрования видеoinформационного ресурса с учетом энергетически значимых структурных единиц базового видеокадра. Она позволяет рассчитать пропускную способность закрытого видеoinформационного канала связи с учетом интенсивности битового потока зашифрованных и открытых структурных единиц.

Ключевые слова: видеокадр, группа кадров, интенсивность, шифрование, селективный метод, кодовая конструкция.

1. Введение

В современных телекоммуникационных системах большое внимание уделяется внедрению технологий безопасности. То же касается и систем видеоконференцсвязи. Существующие технологии скрытия видеoinформационных ресурсов обеспечивают необходимую конфиденциальность. Однако они имеют существенный недостаток: их работа основана на закрытии всего потока передаваемой информации вне зависимости от типа и содержания видеосцены. Такой подход закрытия информации называется полным. Его использование для открытых видеoinформационных ресурсов в инфокоммуникационных системах реального времени является непрактичным.

Для решения этой проблемы применяется селективный подход шифрования. Его суть заключается в скрытии наиболее значимых компонент видеопотока. Эти компоненты формируются в процессе сжатия видеоданных. Поэтому такое шифрование относится к селективному.

Предлагается закрывать только базовый I-кадр. Это позволит уменьшить объем и время обработки шифрованных сжатых видеоданных.

Дополнительно предлагается рассматривать подход, основанный на закрытии видеопотока на базе внутрикадровой селекции.

Под внутрикадровой селекцией подразумевается закрытие не всего видеокадра, а только значимых его составляющих. Под значимой составляющей понимается такая составляющая базового видеокадра,

которая несет в себе наибольшую семантическую и структурную информативность. В процессе автоматической селекции значимых составляющих предлагается учитывать структурные особенности формирования видеопотока.

Для селекции значимых структурных единиц разработана технология, которая базируется на оценке информации, содержащейся в низкочастотных и высокочастотных компонентах трансформанты ДКП блока яркостной составляющей. Значит, необходимо разработать механизм для реализации внутрикадровой селекции видеоданных.

Таким образом, целью исследования является разработка технологии формирования кодовой конструкции для селективного метода обработки видеоданных.

2. Основная часть

На рисунке показана схема кодовой конструкции представления скрытой группы видеокадров. Видно, что кодограмма скрытого базового видеокадра формируется следующим образом:

1) Сначала располагается общая служебная информация о базовом видеокадре ($V_{I_{\text{служ}}} = 113$ байт), которая включает в себя такие данные:

- маркер начала кадра [FF D8] (2 байта);
- маркер параметров квантования [FF DB] (2 байта) и сами параметры (67 байт);
- маркер таблицы служебных данных [FF C4] (2 байта), длину параметров (2 байта), идентификатор таблиц (1 байт), длину кодов таблиц;
- маркер метода кодирования [FF C0] (2 байта), длину информационного кода о методе кодирования (2 байта), информацию о методе кодирования (размер видеокадра, разрядность значений каналов, формат цветового представления, параметры вертикального и горизонтального прореживания компонент) (17 байт).

2) После этого идут поля кодовой конструкции, которые соответствуют информации о структурных единицах базового видеокадра. Интенсивность кодового потока зашифрованной структурной единицы определяется как $V_{S_{\text{Iскр}}}^{(\xi, \gamma)}$ и включает в себя следующие составляющие:

– служебную часть информации о скрытой структурной единице, которая включает в себя маркер начала сканирования структурной единицы [FF DA] и признак закрытия ($V_{I_{\text{служ}}}^{(\xi, \gamma)} = 3$ байта);

– кодограмму информационной части (значения компонент матрицы ДКП), интенсивность которой определяется как $V_{S_{\text{Iскр}}}^{(\xi, \gamma)}$.

В селективном методе обработки видеоданных кодовые конструкции служебной информации о компо-

нентах и информационной части энергетически значимых структурных единицы $S_{\text{зн}}^{(\xi, \gamma)}$ подлежат шифрованию.

3) Кодовая конструкция открытой структурной единицы, которая состоит из следующих составляющих:

– кодограмма информационной части об открытой

структурной единицы $V_{I_{\text{служ}}}^{(\xi, \gamma)}$, которая включает в себя маркер начала сканирования структурной единицы [FF DA] (2 байта) и признак закрытия (1 байт), длину заголовка, количество компонент сканирования, номера компонент сканирования;

– двоичный код $V_{I_{\text{сж}}}^{(\xi, \gamma)}$ компрессионного представления DC, AC-компонент.

Кодовая конструкция Р-кадра состоит из такой информации:

1. Служебная информация о Р-кадре ($V_{P_{\text{служ}}} = 113$ байт), которая включает в себя:

– маркер начала кадра [FF D8] (2 байта);

– маркер параметров квантования [FF DB] (2 байта) и сами параметры (67 байт);

– маркер таблицы служебных данных [FF C4] (2 байта), длину параметров (2 байта), идентификатор таблиц (1 байт), длину кодов таблиц;

– маркер метода кодирования [FF C0] (2 байта), длину информационного кода о методе кодирования (2 байта), информацию о методе кодирования (размер видеокадра, разрядность значений каналов, формат цветового представления, параметры вертикального и горизонтального прореживания компонент) (17 байт);

2. Потом идут поля кода, которые включают в себя информацию о структурных единицах Р-кадра. Интенсивность битового кода структурной единицы Р-кадра определяется как $\overline{V}_{S_{P_{\text{сж}}}}^{(\xi, \gamma)}$ и включает в себя такие составляющие:

– служебную информацию о компонентах (длина заголовка, количество компонент сканирования, номера компонент сканирования), $V_{P_{\text{служ}}}^{(\xi, \gamma)}$ – длину кода служебной части (ξ, γ)-й сжатой структурной единицы Р-кадра;

– двоичный код компрессионного представления DC, AC-компонент структурных единиц Р-кадра, $V_{S_{P_{\text{сж}}}}^{(\xi, \gamma)}$ – длину кода компрессионного представления DC, AC-компонент ξ, γ -й структурной единицы Р-кадра.

Двоичный код В-кадра состоит из следующей информации:

1. Служебная информация о В-кадре ($V_{B_{\text{служ}}} = 113$ байт), которая включает в себя:

– маркер начала кадра [FF D8] (2 байта);

– маркер параметров квантования [FF DB] (2 байта) и сами параметры (67 байт);

– маркер таблицы служебных данных [FF C4] (2 байта), длину параметров (2 байта), идентификатор таблиц (1 байт), длину кодов таблиц;

– маркер метода кодирования [FF C0] (2 байта), длину информационного кода о методе кодирования (2 байта), информацию о методе кодирования (размер видеокадра, разрядность значений каналов, формат цветового представления, параметры вертикального и горизонтального прореживания компонент) (17 байт).

2. Потом идут поля кода, которые включают в себя информации о структурных единицах В-кадра. Интенсивность кодового потока структурной единицы В-кадра определяется как $\overline{V}_{S_{B_{\text{сж}}}}^{(\xi, \gamma)}$ и состоит из следующих составляющих:

– служебная информация о компонентах (длина заголовка, количество компонент сканирования, номера компонент сканирования), $V_{B_{\text{служ}}}^{(\xi, \gamma)}$ – длина кода служебной части (ξ, γ)-й сжатой структурной единицы В-кадра;

– двоичный код компрессионного представления DC, AC-компонент структурных единиц В-кадра, $V_{S_{B_{\text{сж}}}}^{(\xi, \gamma)}$ – длина кода компрессионного представления DC, AC-компонент ξ, γ -й структурной единицы В-кадра.

Длина кодовой конструкции закрытого базового видеокадра $V_I^{\text{скр}}$ – это сумма интенсивностей битового потока скрытых и компрессионно представленных структурных единиц. Данное определение можно представить следующим образом:

$$V_I^{\text{скр}} = V_{I_{\text{служ}}} + V_{S_{I_{\text{сж}}}} + V_{S_{I_{\text{скр}}}},$$

где $V_{S_{I_{\text{сж}}}}$ – длина кода всех компрессионно представленных структурных единиц I-кадра; $V_{S_{I_{\text{скр}}}}$ – длина кода всех скрытых структурных единиц I-кадра; $V_{I_{\text{служ}}}$ – длина кода служебной информации базового видеокадра.

Кодовое представление $V_{S_{I_{\text{сж}}}}^{(\xi, \gamma)}$ не скрытой структурной единицы базового видеокадра K_I определяется как:

$$V_{S_{I_{\text{сж}}}}^{(\xi, \gamma)} = V_{I_{\text{служ}}}^{(\xi, \gamma)} + V_{S_{I_{\text{сж}}}}^{(\xi, \gamma)} \cdot k_I,$$

где $V_{S_{I_{\text{сж}}}}^{(\xi, \gamma)}$ – длина кода служебной информации (ξ, γ)-й структурной единицы базового видеокадра;

$V_{S_{I_{\text{сж}}}}^{(\xi, \gamma)}$ – длина битового потока компрессионного

представления (ξ, γ) -й структурной единицы базового видеокadra.

Интенсивность кода всех открытых структурных единиц $V_{S_{I_{сж}}}$ базового кадра K_I будет рассчитываться как:

$$V_{S_{I_{сж}}} = \sum_{\xi=1}^m \sum_{\gamma=1}^n (V_{I_{сж}}^{(\xi, \gamma)} + V_{S_{I_{сж}}}^{(\xi, \gamma)}).$$

Интенсивность $V_{S_{I_{скр}}}^{(\xi, \gamma)}$ зашифрованной структурной единицы определяется по формуле:

$$V_{S_{I_{скр}}}^{(\xi, \gamma)} = V_{I_{сж}}^{(\xi, \gamma)} + V_{S_{I_{скр}}}^{(\xi, \gamma)},$$

где $V_{I_{сж}}^{(\xi, \gamma)}$ – длина кода открытой части служебной информации (ξ, γ) -й зашифрованной структурной единицы базового видеокadra; $V_{S_{I_{скр}}}^{(\xi, \gamma)}$ – длина битового потока зашифрованной информационной части (ξ, γ) -й структурной единицы базового видеокadra.

Интенсивность кода всех зашифрованных структурных единиц $V_{S_{I_{скр}}}$ базового кадра K_I будет рассчитываться так:

$$V_{S_{I_{скр}}} = \sum_{\xi=1}^m \sum_{\gamma=1}^n (V_{I_{сж}}^{(\xi, \gamma)} + V_{S_{I_{скр}}}^{(\xi, \gamma)}).$$

Таким образом, длина кодового потока $V_{I_{скр}}$ закрытого базового видеокadra будет определяться по следующей формуле:

$$V_{I_{скр}} = V_{I_{сж}} + \sum_1^{N_{скр}} (V_{I_{сж}}^{(\xi, \gamma)} + V_{S_{I_{сж}}}^{(\xi, \gamma)}) + \sum_1^{N_{сж}} (V_{I_{сж}}^{(\xi, \gamma)} + V_{S_{I_{скр}}}^{(\xi, \gamma)}).$$

Длина кода компрессионного представления $\bar{V}_{S_{P_{сж}}}^{(\xi, \gamma)}$ структурной единицы Р-кадра определяется так:

$$\bar{V}_{S_{P_{сж}}}^{(\xi, \gamma)} = V_{S_{P_{сж}}}^{(\xi, \gamma)} + V_{S_{P_{сж}}}^{(\xi, \gamma)},$$

где $V_{S_{P_{сж}}}^{(\xi, \gamma)}$ – длина кода служебной информации (ξ, γ) -й структурной единицы Р-кадра; $V_{S_{P_{сж}}}^{(\xi, \gamma)}$ – длина битового потока компрессионного представления (ξ, γ) -й структурной единицы Р-кадра.

Интенсивность кодового потока компрессионного представления Р-кадра V_P определяется как сумма битового потока компрессионного представления всех

структурных единиц Р-кадра. Это описывается следующим выражением:

$$V_P = V_{P_{сж}} + \sum_{\xi=1}^m \sum_{\gamma=1}^n (V_{S_{P_{сж}}}^{(\xi, \gamma)} + V_{S_{P_{сж}}}^{(\xi, \gamma)}).$$

Длина кода компрессионного представления структурной единицы $\bar{V}_{S_{B_{сж}}}^{(\xi, \gamma)}$ В-кадра определяется так:

$$\bar{V}_{S_{B_{сж}}}^{(\xi, \gamma)} = V_{S_{B_{сж}}}^{(\xi, \gamma)} + V_{S_{B_{сж}}}^{(\xi, \gamma)},$$

где $V_{S_{B_{сж}}}^{(\xi, \gamma)}$ – длина кода служебной информации (ξ, γ) -й структурной единицы В-кадра; $V_{S_{B_{сж}}}^{(\xi, \gamma)}$ – длина битового потока компрессионного представления (ξ, γ) -й структурной единицы В-кадра.

Интенсивность компрессионного представления В-кадра $V_{B_{сж}}$ определяется как сумма всех кодовых последовательностей компрессионного представления структурных единиц В-кадра. Это описывается таким выражением:

$$V_{B_{сж}} = V_{B_{сж}} + \sum_{\xi=1}^m \sum_{\gamma=1}^n (V_{S_{B_{сж}}}^{(\xi, \gamma)} + V_{S_{B_{сж}}}^{(\xi, \gamma)}).$$

Интенсивность V_{GOP} скрытой группы видеокadров определяется как сума битовых последовательностей всех видеокadров в группе и описывается выражением:

$$V_{GOP} = V_{сж}^{GOP} + V_{I_{скр}} + \sum_{z=1}^{N_B} V_{B_{сжz}} + \sum_{z=1}^{N_P} V_{P_{сжz}},$$

где $V_{сж}^{GOP}$ – длина кода служебной информации группы видеокadров; N_P – количество Р-кадров в группе видеокadров; N_B – количество В-кадров в группе видеокadров.

Тогда формула для вычисления интенсивности V_{GOP} скрытой группы видеокadров с учетом интенсивности структурных единиц будет иметь вид:

$$\begin{aligned} V_{GOP} = & V_{сж}^{GOP} + V_{I_{сж}} + \sum_1^{N_{скр}} (V_{I_{сж}}^{(\xi, \gamma)} + V_{S_{I_{сж}}}^{(\xi, \gamma)}) + \\ & + \sum_1^{N_{сж}} (V_{I_{сж}}^{(\xi, \gamma)} + V_{S_{I_{скр}}}^{(\xi, \gamma)}) + V_{P_{сж}} + \\ & + \sum_{\xi=1}^m \sum_{\gamma=1}^n (V_{S_{P_{сж}}}^{(\xi, \gamma)} + V_{S_{P_{сж}}}^{(\xi, \gamma)}) + V_{B_{сж}} + \\ & + \sum_{\xi=1}^m \sum_{\gamma=1}^n (V_{S_{B_{сж}}}^{(\xi, \gamma)} + V_{S_{B_{сж}}}^{(\xi, \gamma)}) \end{aligned}$$

Выводы

Разработана технология формирования кодовой конструкции для селективного метода обработки видеоданных, которая базируется на оценке кодового представления структурных единиц видеокадров с учетом их энергетической значимости.

Разработана методологическая база для оценки битовой скорости видеопотока с учетом наличия выделенных структурных единиц для закрытия видеоинформационного ресурса. При расчетах интенсивности группы видеокадров учитывается длина двоичного кода энергетически значимых структурных единиц базового видеокадра.

Дальнейшее развитие получила технология формирования битового кода в селективном методе шифрования видеоинформационного ресурса с учетом энергетически значимых структурных единиц базового видеокадра. Она позволяет рассчитать пропускную способность закрытого видеоинформационного канала связи с учетом интенсивности битового потока зашифрованных и открытых структурных единиц.

Литература: 1. Ватолин Д., Ратушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео М.: Диалог-Мифи, 2003. 381с. 2. Ян Ричардсон. Видеокодирование. H.264 и MPEG-

4 – стандарты нового поколения. М.: Техносфера, 2005. 368 с. 3. Баранник В.В. Кодирование трансформированных изображений в инфокommunikационных системах / В.В. Баранник, В.П. Поляков. Х.: ХУПС, 2010. 212 с. 4. Баранник В.В. Методологическая база для управления битовой скоростью видеопотока в процессе компрессии / Баранник В.В. // Праці УНДІРТ. 2013. 22с.

Транслитерированный список литературы: 1. Vatoлин D., Ratushnyak A., Smirnov M., Yukin V. Metody szhatija dannyh. Ustrojstvo arhivatorov, szhatie izobrazhenij i video M.: Dialog-Mifi, 2003. 381s. 2. Jan Richardson. Videokodirovanie. N.264 i MPEG-4 – standarty novogo pokolenija. Moskva: Tehnosfera, 2005. 368 s. 3. Barannik V.V. Kodirovanie transformirovannyh izobrazhenij v infokommunikacionnyh sistemah / V.V. Barannik, V.P. Poljakov. H.: HUPS, 2010. 212 s. 4. Barannik V.V. Metodologicheskaja baza dlja upravlenija bitovoj skorost'ju videopotoka v processe kompressii / Barannik V.V. // Praci UNDIRT. 2013. 22с.

Поступила в редколлегию 13.11.2015

Рецензент: д-р техн. наук, проф. Безрук В.М.

Комолов Дмитрий Иванович, главный специалист, отдел связи Главного управления Национальной полиции в Харьковской области, соискатель ХНУРЭ. Научные интересы: технологии защиты информации в инфокommunikационных системах. Адрес: Украина, 61000, Харьков, ул. Совнаркомовская, 5.



ДОДАТНІ РОЗВ'ЯЗКИ ДЛЯ ЕЛІПТИЧНОГО РІВНЯННЯ З ДВОМА ПАРАМЕТРАМИ

ЛУХАНІН В.С.

Розглядаються питання існування, єдиності та побудови двосторонніх наближень до додатного розв'язку однієї лінійної еліптичної крайової задачі з двома параметрами. Описуються умови, яким мають задовольняти параметри, щоб двосторонні наближення можна було побудувати.

Ключові слова: функція Гріна, двосторонні наближення, інваріантний конусний відрізок, додатний розв'язок, угнутість, монотонність.

Key words: Green's function, two-sided approximations, invariant cone segment, positive solution, concavity, monotonicity.

Вступ

Багато фізичних процесів зводиться до задачі

$$\begin{aligned} -\Delta u &= f(x, u) \quad \forall x \in \Omega \subset \mathbb{R}^m, \\ u &> 0, \quad u|_{\partial\Omega} = 0, \end{aligned}$$

де $f(x, u)$ є лінійною відносно u функцією.

Актуальність дослідження: до такої крайової задачі зводиться достатньо велика кількість фізичних процесів. Отримати точний розв'язок цієї задачі вдається дуже рідко. Застосування багатьох наближених методів, зокрема варіаційних або сіткових, пов'язано з дослідженням точності отриманого розв'язку, що в загальному випадку виявляється досить складною задачею. Вважаємо, що побудова двосторонніх наближень позбавляє дослідника цих труднощів.

Метою роботи є дослідити можливість побудови двосторонніх наближень для розв'язання даної задачі.

Метод двосторонніх наближень належить до ітераційних методів. Вони є універсальним інструментом як при дослідженні питань існування та єдиності розв'язків операторних рівнянь, так і для фактичного їх знаходження. При цьому двосторонні наближення дозволяють отримати верхню та нижню оцінку розв'язку на кожній ітерації.

1. Постановка задачі

Розглянемо крайову задачу для лінійного еліптичного рівняння

$$-\Delta u = au(x) + b \quad \forall x \in \Omega \subset \mathbb{R}^m, \quad (1)$$

$$u|_{\partial\Omega} = 0, \quad b \geq 0, \quad a = \text{const}. \quad (2)$$

Якщо рівняння (1) набуває вигляду

$$-\Delta u = \kappa^2 u(x),$$

маємо задачу про розповсюдження, випромінювання та розсіювання звуку на твердих тілах [1].

Якщо вивчається процес дифузії за наявності "ланцюгових" реакцій (частинки дифундуючої рідини або газу вступають у реакцію з навколишнім середовищем і розмножуються), також маємо рівняння (1), в якому стала a є коефіцієнтом пропорційності швидкості реакції розпаду до концентрації газу.

2. Побудова послідовних наближень

Відомо [2], що задача (1), (2) у класі неперервних функцій еквівалентна інтегральному рівнянню

$$u(x) = \int_{\Omega} G(x, s) [au(s) + b] ds,$$

де $G(x, s)$ – функція Гріна оператора Лапласа для першої крайової задачі в області Ω , $x = (x_1, \dots, x_m)$, $s = (s_1, \dots, s_m)$.

На конусі K невід'ємних в $C(\Omega)$ функцій введемо в розгляд лінійне операторне рівняння $u = Tu$, де

$$Tu = \int_{\Omega} G(x, s) [au(s) + b] ds. \quad (3)$$

Відомо, що конус невід'ємних в $C(\Omega)$ функцій є нормальним, крім того, оскільки функція

$$f(x, u) = au(x) + b$$

неперервна за u , оператор T , відображаючи простір $C(\Omega)$ в себе, цілком неперервний [2, 3].

Розглянемо деякі властивості оператора T вигляду (3).

1) Оператор T монотонний, тобто з $u_1 \leq u_2$ повинно випливати $Tu_1 \leq Tu_2$. Складаємо різницю

$$\begin{aligned} Tu_1 - Tu_2 &= \int_{\Omega} G(x, s) [au_1(s) + b] ds - \\ &- \int_{\Omega} G(x, s) [au_2(s) + b] ds = \int_{\Omega} G(x, s) a(u_1(s) - u_2(s)) ds \leq 0. \end{aligned}$$

Останнє виконується, якщо

$$a > 0. \quad (4)$$

2) Для побудови конусного відрізка $\langle v_0, w_0 \rangle$, $v_0 \leq u \leq w_0$, інваріантного для оператора T , в (3) покладемо $u = v_0 = 0$ та складемо елемент

$$v_1 = Tv_0 = \int_{\Omega} G(x, s) [a v_0(s) + b] ds = \\ = \int_{\Omega} G(x, s) b ds \geq v_0 = 0.$$

Потім побудуємо елемент

$$v_2 = \int_{\Omega} G(x, s) [a v_1(s) + b] ds \geq v_1$$

і так далі.

Тепер в (3) покладемо $u = w_0 = \beta$, $\beta = \text{const} \geq 0$ – визначиться в майбутньому, маємо

$$w_1 = \int_{\Omega} G(x, s) [a w_0(s) + b] ds = \int_{\Omega} G(x, s) [a\beta + b] ds.$$

Підбираємо параметри a та β так, щоб $w_1 \leq w_0$. Ця вимога приводить нас до умови

$$\max_{x \in \Omega} \int_{\Omega} G(x, s) ds \leq \frac{\beta}{a\beta + b}. \quad (5)$$

При цьому

$$w_2 = \int_{\Omega} G(x, s) [a w_1(s) + b] ds \leq \int_{\Omega} G(x, s) [a\beta + b] ds = w_1.$$

Таким чином, маємо $v_0 \leq v_1 \leq w_1 \leq w_0$, отже, конусний відрізок $\langle v_0, w_0 \rangle$, $v_0 = 0$, $w_0 = \beta$, є інваріантним для оператора T вигляду (3).

3) Дослідимо оператор T на угнутість на $\langle v_0, w_0 \rangle$. Для цього має виконуватися умова $T(tu) \geq tTu \quad \forall t \in [0, 1]$, $u \in \langle v_0, w_0 \rangle$. Складемо

$$T(tu) - tTu = \\ = \int_{\Omega} G(x, s) b(1-t) ds, \quad t \in [0, 1]. \quad (6)$$

Щоб (6) була невід'ємною, треба вимагати виконання умови

$$b(1-t) \geq 0.$$

Для $t \in [0, 1]$ та $\forall x \in \Omega$ ця умова виконується завжди.

4) Дослідимо оператор T вигляду (3) на u_0 -угнутість, де

$$u_0 = \int_{\Omega} G(x, s) ds.$$

Угнутий оператор T називається u_0 -угнутим на $\langle v_0, w_0 \rangle$, якщо для кожного $t_0 \in (0, 1)$ можна вказати таке $\eta = \eta(u, t_0) > 0$, що $T(t_0 u) \geq (1 + \eta)t_0 Tu$ на відрізку,

сумірному з u_0 [2] (будь-який елемент вигляду $\text{const} \cdot u_0 \in \langle v_0, w_0 \rangle$ сумірний з u_0 за визначенням).

Складаємо

$$T(t_0 u) - (1 + \eta)t_0 Tu = \\ = \int_{\Omega} G(x, s) (b - t_0 b - \eta t_0 [a u(s) + b]) ds. \quad (7)$$

Щоб (7) була невід'ємною, вимагаємо виконання нерівності

$$b - t_0 b - \eta t_0 [a u(x) + b] \geq 0,$$

$\forall t_0 \in (0, 1)$, $\eta > 0$, звідки маємо умову

$$\eta \leq \frac{b(1-t_0)}{t_0(a u(x) + b(x))},$$

яка виконується, якщо чисельник $b(1-t_0) \geq 0$, що, очевидно, має місце.

Із виконання властивостей 1)–4) випливає існування та єдиність додатного розв'язку у задачі (1), (2) [2, с. 283].

Ітераційний процес для задачі (1), (2) будемо за схемою

$$v_n(x) = \int_{\Omega} G(x, s) [a v_{n-1}(s) + b] ds, \quad n = 1, 2, \dots,$$

$$w_n(x) = \int_{\Omega} G(x, s) [a w_{n-1}(s) + b] ds, \quad n = 1, 2, \dots,$$

де $v_0 = 0$, $w_0 = \beta$. За умови виконання вимог (4), (5) маємо рівномірну збіжність до єдиного додатного розв'язку $u^* \in \langle v_0, w_0 \rangle$. При цьому

$$0 = v_0 \leq v_1 \leq \dots \leq v_n \leq \dots \leq u^* \leq \dots$$

$$\dots \leq w_n \leq \dots \leq w_1 \leq w_0 = \beta.$$

Якщо в задачі (1), (2)

$$b = b(x), \quad b(x) \geq 0 \quad \forall x \in \Omega,$$

то умова (5) приймає вигляд

$$\max_{x \in \Omega} \int_{\Omega} G(x, s) ds \leq \frac{\beta}{a\beta + \tilde{b}}, \quad \tilde{b} = \max_{x \in \Omega} b(x). \quad (8)$$

3. Результати обчислювального експерименту

Обчислювальні експерименти проведено у випадку $b = \text{const}$ та $b = b(x)$ у крузі та півкрузі відповідно.

1) Розглянемо область

$$\Omega = \{(x_1, x_2) | x_1^2 + x_2^2 < 1\}$$

при значеннях $a = 0,1$, $b = 5$, $\beta = 1,9$. Такі значення задовольняють умовам (4), (5).

В табл. 1 наведено значення для наближень $w_3(\mathbf{x})$ та $v_3(\mathbf{x})$ у точках області Ω з полярними координатами (ρ_i, φ_j) , де $\rho_i = 0,2i$, $\varphi_j = \frac{\pi j}{10}$, $i = \overline{1,4}$, $j = \overline{1,5}$.

Таблиця 1

φ		ρ			
		0,2	0,4	0,6	0,8
$\frac{\pi}{10}$	w_3	1,219830	1,070450	0,814061	0,453726
	v_3	1,219820	1,070430	0,814052	0,453722
$\frac{\pi}{5}$	w_3	1,219830	1,069770	0,812363	0,451975
	v_3	1,219820	1,069760	0,812354	0,451970
$\frac{3\pi}{10}$	w_3	1,219830	1,069020	0,810916	0,450081
	v_3	1,219810	1,069010	0,810908	0,450077
$\frac{2\pi}{5}$	w_3	1,219830	1,069280	0,811528	0,450668
	v_3	1,219810	1,069270	0,811519	0,450664
$\frac{\pi}{2}$	w_3	1,219860	1,073530	0,820921	0,461770
	v_3	1,219850	1,073520	0,820912	0,461766

На рис. 1 та 2 представлені поверхні та лінії рівня для наближення $w_3(\mathbf{x})$ відповідно.

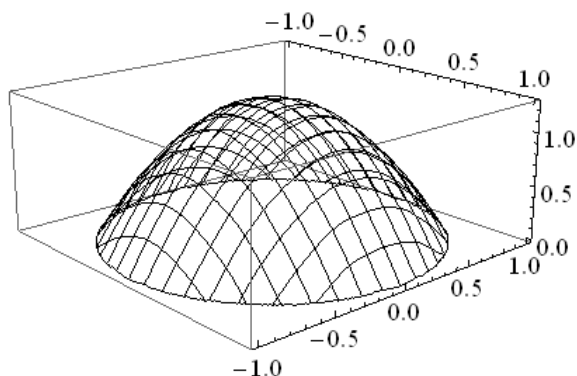


Рис. 1. Поверхня для наближення $w_3(\mathbf{x})$

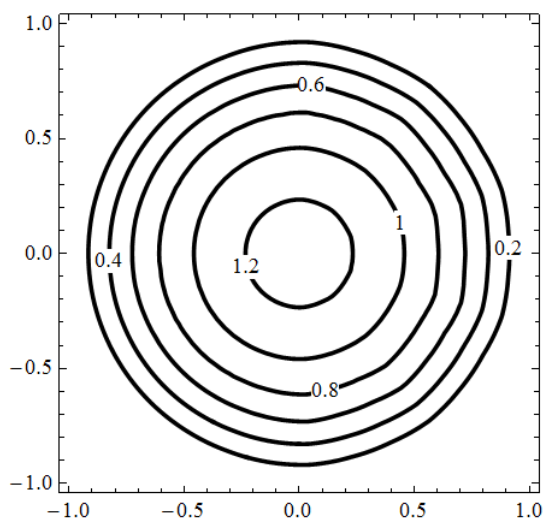


Рис. 2. Лінії рівня для наближення $w_3(\mathbf{x})$

2) Тепер розглянемо область

$$\Omega = \{(x_1, x_2) \mid x_2 > 0, x_1^2 + x_2^2 < 1\}$$

при значеннях $a = 0,5$, $\beta = 1,9$,

$$b = b(\mathbf{x}) = 10 \sin(0,1)(-\Delta \omega(\mathbf{x}) + 10 \omega(\mathbf{x})),$$

де $\omega(\mathbf{x}) = x_2(1 - x_1^2 - x_2^2)$ є рівнянням межі $\partial\Omega$ [4]. Такі значення задовольняють умовам (4), (8).

В табл. 2 наведено значення для наближень $v_3(\mathbf{x})$ та $w_3(\mathbf{x})$ у точках області Ω з полярними координатами (ρ_i, φ_j) , де $\rho_i = 0,2i$, $\varphi_j = \frac{\pi j}{10}$, $i = \overline{1,4}$, $j = \overline{1,5}$.

На рис. 3 та 4 представлені поверхні та лінії рівня для наближення $w_3(\mathbf{x})$ відповідно.

Таблиця 2

φ		ρ			
		0,2	0,4	0,6	0,8
$\frac{\pi}{10}$	w_3	0,111160	0,190904	0,206723	0,141847
	v_3	0,111160	0,190902	0,206722	0,141846
$\frac{\pi}{5}$	w_3	0,211367	0,362888	0,392750	0,269359
	v_3	0,211366	0,362886	0,392748	0,269357
$\frac{3\pi}{10}$	w_3	0,290852	0,499246	0,540053	0,370257
	v_3	0,290850	0,499243	0,54005	0,370255
$\frac{2\pi}{5}$	w_3	0,341867	0,586820	0,634845	0,435241
	v_3	0,341865	0,586816	0,634842	0,435239
$\frac{\pi}{2}$	w_3	0,359443	0,616922	0,66727	0,457381
	v_3	0,359440	0,616918	0,667266	0,457379

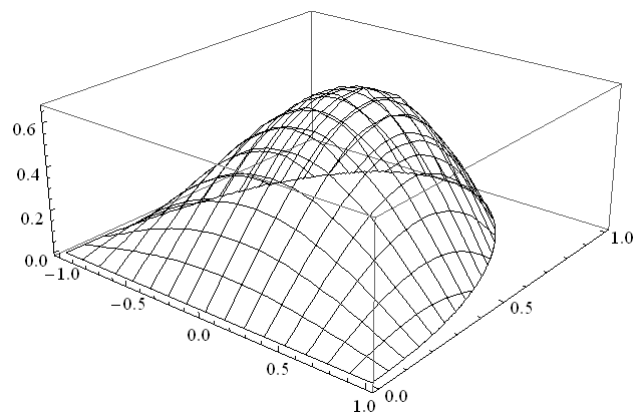


Рис. 3. Поверхня для наближення $w_3(\mathbf{x})$

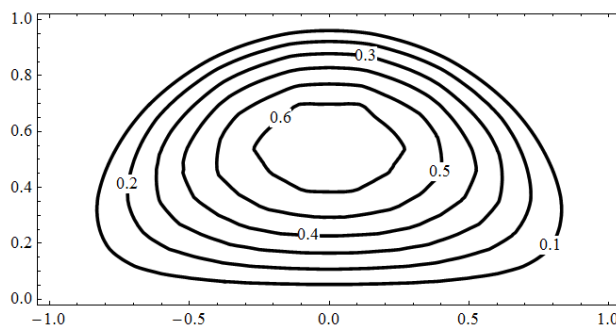


Рис. 4. Лінії рівня для наближення $w_3(\mathbf{x})$

4. Висновки

Вперше до розв'язання задачі (1), (2) з лінійною функцією було запропоновано застосувати методи теорії операторних рівнянь у напівупорядкованих просторах.

Досліджено можливість побудови двосторонніх наближень до додатного розв'язку задачі (1), (2) та отримано умову (5), яка гарантує збіжність ітераційного процесу.

Зазначимо, що побудова конусного відрізка $\langle v_0, w_0 \rangle$ по суті є апіорною оцінкою шуканого розв'язку, оскільки маємо $v_0 \leq u^* \leq w_0$. Отримані двосторонні наближення до розв'язку задачі дають можливість робити апостеріорні висновки.

Хочемо ще зазначити, що при застосуванні запропонованого методу немає необхідності робити порівняння отриманого розв'язку з розв'язками, отриманими іншими методами.

Ще однією з переваг цього методу у порівнянні з іншими є відносна простота реалізації алгоритму, що в свою чергу вимагає менше обчислювальних ресурсів.

Крім вказаного вище, нам вдалося накласти певні умови на два параметри, які входять у постановку задачі, що дозволяє довести існування єдиного додатного розв'язку та побудувати двосторонні наближення.

Література: 1. Будак Б. М., Самарский А. А., Тихонов А. Н. Сборник задач по математической физике. М.: Наука, 1980. 688 с. 2. Красносельский М. А. Положительные решения операторных уравнений. М.: Физматгиз, 1962. 394 с. 3. Опојцев В. И., Хуродзе Т. А. Нелинейные операторы в пространствах с конусом. Тбилиси: Изд-во Тбилис. ун-та, 1984. 246 с. 4. Калиниченко В. И., Коций А. Ф., Ропавка А. И. Численные решения задач теплопроводности. Харьков: Вища школа, 1987. 108 с.

Транслитерований список літератури: 1. Budak B. M., Samarskij A. A., Tihonov A. N. Sbornik zadach po matematicheskoy fizike. M.: Nauka, 1980. 688 p. 2. Krasnosel'skij M. A. Polozhitel'nye resheniya operatornykh uravnenij. M.: Fizmatgiz, 1962. 394 p. 3. Opojcev V. I., Hurudze T. A. Nelinejnye operatory v prostranstvakh s konusom. Tbilisi: Izd-vo Tbilis. un-ta, 1984. 246 p. 4. Kalinichenko V. I., Koshhij A. F., Ropavka A. I. Chislennye reshenija zadach teploprovodnosti. Har'kov: Vishha shkola, 1987. 108 p.

Надійшла до редколегії 28.08.2015

Рецензент: д-р фіз.-мат. наук Колосов А. І.

Луханін Володимир Сергійович, магістр, аспірант кафедри ПМ ХНУРЕ, інженер-програміст в EPAM Systems. Наукові інтереси: розв'язання крайових задач для диференціальних рівнянь у частинних похідних. Хоббі: читання, спорт. Адреса: Україна, 61103, Харків, вул. Космонавтів, 5А, кв. 2, тел. +38(050) 617-41-94.

Volodymyr Lukhanin, master, postgraduate student at the Department of Applied Mathematics of Kharkiv National University of Radio and Electronics, software engineer at EPAM Systems. Scientific interests: solving boundary value problems for partial differential equations. Hobby: reading, sports. Address: Ukraine, 61103, Kharkiv, Kosmonavtiv str. 5A, apt. 2, phone +38(050) 617-41-94.



ВИКОРИСТАННЯ МАШИНИ ТЮРИНГА ДЛЯ РОЗВ'ЯЗАННЯ КРИПТОГРАФІЧНОЇ ЗАДАЧІ ПОЛІНОМІАЛЬНОЇ СКЛАДНОСТІ

ПЕТРОВА О.О., БУРМЕНСЬКИЙ Р.В.

Пропонується модель процесу обчислення на детермінованій однострічковій машині Тьюринга для реалізації симетричного алгоритму шифрування з використанням полібіанського квадрату. Наводяться етапи кодування даних та програма, що моделює роботу машини Тьюринга для рішення задачі криптографії.

Ключові слова: машина Тьюринга, алгоритм шифрування, квадрат Полібія.

Key words: Turing machine, encryption algorithm, Polybius square.

Вступ

Проблеми рішення задач можна розділити на класи відповідно до складності їх розв'язання. Клас P складається з проблем, які можна вирішити за поліноміальний час, клас NP – із проблем, які можна вирішити за поліноміальний час тільки на недетермінованій машині Тьюринга (МТ). Як відмічається в роботі [1], важливість NP у криптографії полягає в тому, що більшість симетричних алгоритмів і алгоритмів з відкритими ключами можуть бути зламані за недетермінований поліноміальний час. Для даного шифротексту C криптоаналітик просто вгадує відкритий текст X і ключ k , і за поліноміальний час виконує алгоритм шифрування з входами X і k та перевіряє, чи дорівнює результат C . Клас NP включає клас P , оскільки будь-яка проблема, вирішувана за поліноміальний час на детермінованій МТ, буде також вирішена за поліноміальний час на недетермінованій машині Тьюринга, при цьому пропускається етап припущення. Якщо всі NP проблеми вирішуються за поліноміальний час на детермінованій машині, то $P = NP$.

Більшість задач, цікавих з практичної точки зору, мають поліноміальні алгоритми вирішення. Це означає, що час роботи алгоритму на вході довжини n складає не більше $O(n^k)$ для деякої константи k , яка є незалежною від довжини входу.

Задача називається поліноміальною, тобто відноситься до класу P , якщо існує константа k і алгоритм, що вирішує задачу з $F_a(n) = O(n^k)$, де n – довжина входу алгоритму в бітах.

Таким чином, задачі класу P є уточненням означення «практично вирішуваної» задачі.

Актуальність: в сучасному світі висококваліфікований спеціаліст може отримати доступ практично до будь-якої інформації на комп'ютері. Для запобігання несанкціонованого втручання необхідно використовувати методи захисту інформації, що є основою сучасної криптографії, в якій використовується симетричне та асиметричне шифрування.

Мета роботи: побудова функціональної схеми машини Тьюринга для рішення задачі криптографії.

Для досягнення поставленої мети сформульовані такі завдання:

- ознайомлення з задачами криптографії, які мають поліноміальний алгоритм вирішення;
- розробка моделі процесу обчислення на детермінованій однострічковій МТ;
- аналіз сучасних досліджень шифрування з використанням МТ;
- побудова МТ для реалізації симетричного алгоритму шифрування з використанням полібіанського квадрату.

1. Аналіз попередніх досліджень

Симетричні алгоритми, які іноді називають умовними, представляють собою алгоритми, у яких ключ шифрування, може бути розрахований за ключем дешифрування і навпаки [1]. У більшості симетричних алгоритмів ключі шифрування і дешифрування одні й ті ж. Ці алгоритми, які також називають алгоритмами із секретним ключем або алгоритмами з одним ключем, вимагають, щоб відправник і отримувач узгодили ключ, що використовується перед початком безпечної передачі повідомлень. Безпечність симетричного алгоритму визначається ключем, розкриття ключа означає, що хто завгодно зможе шифрувати і дешифрувати повідомлення. Доки повідомлення, що передаються, повинні бути таємними, ключ повинен зберігатися у секреті. Шифрування і дешифрування з використанням симетричного алгоритму позначається як: $EK(M) = C$ $DK(C) = M$.

На сьогодні розроблена велика кількість алгоритмів стійкої криптографії. В цьому аспекті цікавим представляється доведення розв'язання криптографічної задачі на МТ.

В [2] автор кодує правила роботи МТ інгібіторною мережею Петрі та відмічає, що програма не є повністю визначеною, оскільки є некоректні конфігурації МТ.

В роботі [3] розглядається побудова МТ, що шифрує текст за допомогою таблиці відповідності. Кожній літері латинського алфавіту зіставляється відповідний бінарний код. У шифротекст додаються «сміттєві символи», що ускладнюють процес дешифрування, але шифротекст дуже легко піддається розшифровці. Для цього необхідно виокремити з нього бінарні числа і розшифрувати код за таблицею відповідності.

Автором Чернушко М.М. у роботі [4] була розглянута «...задача реалізації за допомогою МТ алгоритму симетричного шифрування методом перестановки та алгоритму шифрування методом одноалфавітної підстановки». При використанні шифрування методом одноалфавітної підстановки автор розглядав алфавіт, який складається тільки з символів «АБВГДЕ», що суттєво звужує діапазон слів, які підлягають шифруванню.

В наведеній у даній статті функціональній схемі МТ подолано це обмеження і є можливість шифрування слів з усіх літер англійського алфавіту та деяких спеціальних символів.

Як бачимо, кожен із запропонованих алгоритмів шифрування, реалізований на МТ, має свої переваги та недоліки.

2. Основний матеріал

МТ є найбільш загальною математичною моделлю «детермінованого перетворювача слів», тобто моделлю, за допомогою якої може бути обчислена будь-яка функція з множини слів в одному алфавіті в множину слів в іншому алфавіті. Кожна окрема МТ здатна виконувати тільки один алгоритм, для визначення якого можна користуватись терміном «програма МТ» – набір інструкцій, які спрощені до однотипної схеми. Всі МТ відрізняються своїми програмами [5].

МТ має в розпорядженні кінцеве число знаків (символів): $a_1, a_2, \dots, a_m$, що утворюють зовнішній алфавіт, в якому кодуються відомості, що подаються в машину, а також ті, які виробляються в ній. В МТ обробка інформації, як і в комп'ютері, виконується в логічному блоці, який може перебувати в одному з кінцевої кількості станів: $q_1, q_2, \dots, q_n$. Блок має два вхідних канали: через один із них на кожній стадії роботи машини (в кожному такті) надходить знак з клітинки, яку оглядають, через інший – знак q_i того стану, який приписується блоку на даний такт. Через вихідний канал блок посилає в клітинку, яку оглядає, відповідний «перепрацьований» знак a_j , що є однозначною функцією від сигналів $a_j q_i$, поданих на вхід (рис. 1).

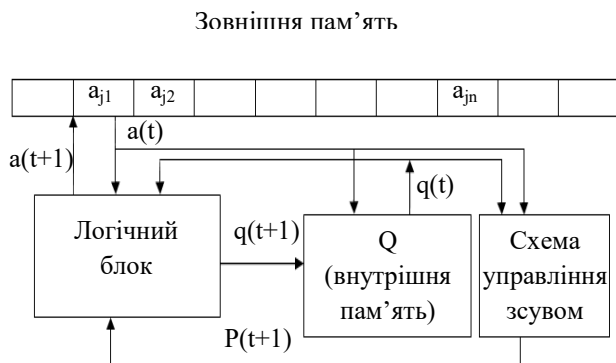


Рис. 1. Обробка інформації в МТ

Логічний блок реалізує функцію, яка ставить у залежність кожній парі знаків: a_i, q_n (кількість таких пар

складає $k*m$) трійку знаків: a_j, D, q_i . Таку логічну функцію зручно подавати у вигляді прямокутної таблиці, стовпчики якої занумеровані знаками стану, а рядки – знаками зовнішнього алфавіту. В кожній клітинці таблиці записано відповідну вихідну трійку знаків. Таку таблицю можна називати функціональною схемою машини [5].

В роботах [6,7] наведено схематичне зображення детермінованої однострічкової машини Тьюринга, описано структуру МТ та розроблено протоколи програм МТ для рішення задач обчислювальної математики.

В даній статті наведено функціональну схему МТ для симетричного алгоритму шифрування методом квадрата Полібія.

Квадрат Полібія є загальною моноалфавітною підстановкою, яка проводиться за допомогою випадково заповненої алфавітом квадратної таблиці. Класичний полібіанський квадрат – таблиця, що складається з 5 рядків і 5 стовпців, заповнена випадковим чином буквами грецького алфавіту і пробілом. При шифруванні в таблиці знаходять букву відкритого тексту і записують у шифртекст букву, розташовану нижче від неї в тому ж стовпці. Якщо літера вихідного тексту знаходиться в нижньому рядку таблиці, то їй відповідає буква першого рядка з цього ж стовпця.

Існує декілька методів використання квадрата Полібія.

1. Суть першого методу полягає в тому, що замість кожної літери в слові використовується відповідна їй літера знизу ($A = F, B = G$).
2. В другому методі зазначаються відповідні кожній літері цифри з таблиці: першою пишеться цифра по вертикалі, другою – по горизонталі ($A = 11, B = 21$).
3. Третій метод базується на попередньому методі, при цьому записаний попарно первісний код здвигується вліво на одну позицію, в другий раз розділяється попарно, в результаті чого отримується шифр [8].
4. Четвертий метод аналогічний другому методу, але на відміну від нього шифр розділяється на 2 блоки: цифри по вертикалі пишуться в лівому блоці, а по горизонталі – в правому.

В запропонованій роботі концепцію полібіанського квадрата реалізовано з використанням англійських літер та спеціальних знаків на основі четвертого методу використання квадрата Полібія в таблиці розміром 6×6 (рис. 2).

	1	2	3	4	5	6
1	A	B	C	D	E	F
2	G	H	I	J	K	L
3	M	N	O	P	Q	R
4	S	T	U	V	W	X
5	Y	Z	.	,	:	@
6	-	+	=	(	)	?

Рис. 2. Квадрат Полібія

Для кращого розуміння шифрування цим методом наведемо приклад: слово CODE шифрується двома блоками цифр 3345 1311. Якщо розділити код попарно 33 45 13 11, то згідно з символами, наведеними в таблиці (рис. 2), отримаємо сукупність символів «О,МА».

Четвертий метод використання квадрата Полібія було реалізовано в програмному інтерпретаторі машини Тьюринга ALGO 2000 [9].

Розроблена авторами програма, що моделює шифрування тексту методом квадрата Полібія, працює за таким принципом: у стані q_0 МТ переглядає символ у клітині, на якій розташована головка, після чого, якщо цей символ наявний у квадраті Полібія, головка записує відповідну йому цифру шифру по вертикалі у поточну клітину та переходить у відповідний стан $q_1 - q_6$, де індекс q вказує на цифру шифру по горизонталі. У разі, якщо в стані q_0 не було знайдено символу, що входить до квадрата Полібія (головка дійшла до кінця символної послідовності), то робота МТ завершується.

У станах $q_1 - q_6$ головка МТ переміщується у кінець символної послідовності до порожньої клітини та ставить відповідну індексу стану q цифру шифру по горизонталі, після чого МТ переходить у стан q_7 .

У стані q_7 головка МТ переміщується у початок символної послідовності, після чого МТ переходить у початковий стан q_0 .

Для перевірки роботи запропонованого алгоритму було введено прізвище Алана Тьюринга (рис. 3).

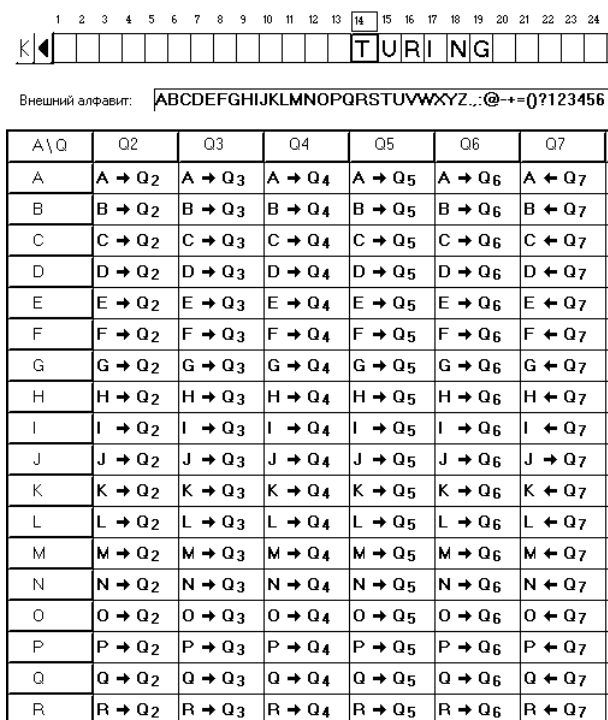


Рис. 3. Фрагмент протоколу побудованої МТ

Результат шифрування слова «TURING» методом квадрата Полібія наведено на рис. 4.

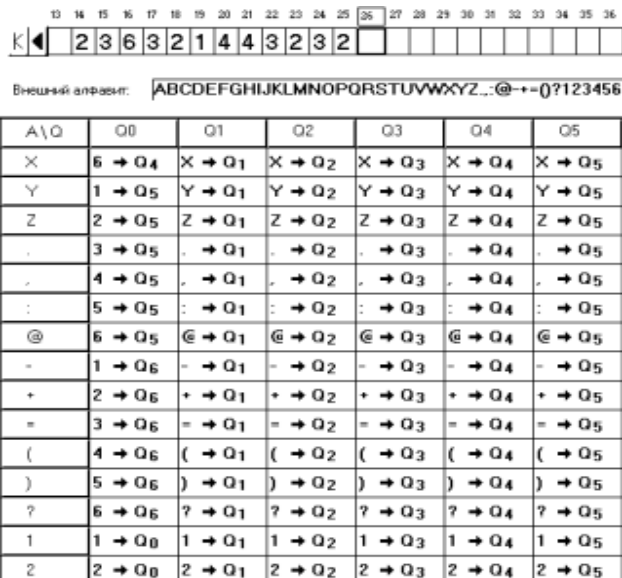


Рис. 4. Результат шифрування

Для представлення інформації в текстовому вигляді отриманий шифр розбивається попарно: 23 63 21 44 32 32 і отриманим парам цифр знаходяться відповідні літери в таблиці. Результатом шифрування слова «TURING» буде сукупність літер «NRBVII».

Висновки

На основі результатів досліджень запропонована функціональна схема машини Тьюринга, яка доводить алгоритм розв'язання запропонованої криптографічної задачі поліноміальної складності. Наведено структуру розробленої МТ, розглянуто операції, які вона виконує, виконано програмне моделювання роботи МТ для реалізації криптографічного алгоритму.

До переваг запропонованого методу шифрування належать:

- можливість довільного заповнення таблиці символами, що може ускладнити дешифрування без наявної у отримувача таблиці Полібія на відміну від методу шифру Цезаря та шифру із кодовим словом;

- неможливість дешифрування «на льоту» на відміну від шифру одноalfавітною підстановкою чи перестановкою та відносна складність визначення шифру, оскільки дешифрування тексту за трьома першими методами квадрата Полібія не приведе до успіху;

- квадрат Полібія має однакову кількість рядків та стовпців, що не завжди виконується для таблиці відповідності, а отже, неможливо одразу визначити, який індекс літери шифротексту відповідає рядку, а який – стовпцю.

З огляду на простоту правил побудови запропоновані коди можна ефективно використовувати для захисту індивідуальних користувачів. При цьому обраний метод шифрування є досить простим, оскільки реалізація більш складних алгоритмів шифрування є проблема-

тичною у плані громіздкості програми для МТ. Тому доречнішим для реалізації більш досконалих алгоритмів шифрування буде використання мов програмування.

Література: 1. *Левина А.Б.* Моделирование криптосистем. Санкт-Петербург: НИУ ИТМО, 2013. 82 с. 2. *Зайцев Д.А.* Ингибиторная сеть Петри, исполняющая произвольную заданную машину Тьюринга / Д.А. Зайцев // Систем. дослідж. та інформ. технології. 2012. № 2. С. 26-41. 3. *Z. Saqib, M. A. Shahid, M. U. Ashraf.* Encryption and Decryption Using Automata Theory/ International Journal of Multidisciplinary Sciences and Engineering, Vol. 6, No. 4, April 2015. P. 14-21. 4. *Чернушко М.М.* Применение машины Тьюринга для реализации алгоритмов шифрования [Текст] / М. М. Чернушко // Технические науки: теория и практика: материалы II междунар. науч. конф. Чита: Молодой ученый, 2014. С. 19-22. 5. *Трахтенброт Б.А.* Алгоритмы и машинное решение задач. М.: Государственное издательство технико-теоретической литературы, 1957. 96 с. 6. *Петрова О.О., Бурменский Р.В.* Моделирование машины Тьюринга обчислення додатку чисел / / Всеукраїнська студентська наукова конференція «Наукова Україна» (з міжнародною участю), м. Дніпропетровськ, 2015. С. 215-218. 7. *Петрова О., Бурменський Р.* Функціональна схема машини Тьюринга для множення числа на 11 // Матеріали VII Українсько-польської науково-практичної конференції «Електроніка та інформаційні технології» (ЕліТ-2015), Львів-Чинадієво-2015. С.139-141. 8. *Tumblr.* 14 способів шифрування. [Електронний ресурс]. Режим доступу: <http://thereichenbachblog.tumblr.com/typesofcipher> 9. Эмулятор машины Поста (ALGO 2000). [Електронний ресурс]. Режим доступу: <http://teach.sc585.spb.ru/inf/2011/11/21/эмулятор-машины-поста-algo-2000/>

Транслітерований список літератури:

Література: 1. *Levina A.B.* Modelirovanie kriptosistem. Sankt-Peterburg: NIU ITMO, 2013. 82 s. 2. *Zajcev D.A.* Ingibitornaja set' Petri, ispolnjajushhaja proizvol'niju zadannuju mashinu T'juringa / D.A. Zajcev // Sistem. doslidzh. ta inform. tehnologii. 2012. № 2. S. 26-41. 3. *Z. Saqib, M. A.*

Shahid, M. U. Ashraf. Encryption and Decryption Using Automata Theory/ International Journal of Multidisciplinary Sciences and Engineering, Vol. 6, No. 4, April 2015. C. 14-21. 4. *Chernushko M. M.* Primenenie mashiny T'juringa dlja realizacii algoritmov shifrovaniya [Tekst] / M. M. Chernushko // Tehnicheskie nauki: teorija i praktika: materialy II mezhdunar. nauch. konf. Chita: Molodoj uchenyj, 2014. S. 19-22. 5. *Trahtenbrot B.A.* Algoritmy i mashinnoe reshenie zadach. M.: Gosudarstvennoe izdatel'stvo tehniko-teoreticheskoy literatury, 1957. 96 s. 6. *Petrova O.O., Burmens'kyj R.V.* Modelyuvannya mashy'ny' T'yury'nga obchy'slennya dodatku chy'sel // Vseukrayins'ka students'ka naukova konferenciya «Naukova Ukrainy» (z mizhnarodnoyu uchastyu), m. Dnipropetrovs'k, 2015. S. 215-218. 7. *Petrova O., Burmens'kyj R.* Funkcional'na sxema mashy'ny' T'yury'nga dlya mnozhennya chy'sla na 11 // Materialy VII Ukrayins'kopols'koyi naukovo-prakty'chnoyi konferenciyi «Elektronika ta informacijni tehnologiyi» (ELIT-2015), L'viv-Chy'nadijevo-2015. S.139-141. 8. *Tumblr.* 14 sposobov shifrovaniya. [Електронний ресурс]. <http://thereichenbachblog.tumblr.com/typesofcipher> 9. Эмулятор машины Поста (ALGO 2000). [Електронний ресурс]. <http://teach.sc585.spb.ru/inf/2011/11/21/эмулятор-машины-поста-algo-2000/>

Надійшла до редколегії 12.11.2015

Рецензент: д-р техн. наук Гіль М.І.

Петрова Олена Олександрівна, канд. техн. наук, доцент каф. Економічної кібернетики та інформаційних технологій Харківського національного університету будівництва та архітектури. Наукові інтереси: штучний інтелект, експертні системи. Адреса: Україна, 20322. Харків, вул. Сумська, 40, тел. +38 098 8499 076.

Бурменський Рустам Валерійович, студент Харківського національного університету будівництва та архітектури. Наукові інтереси: програмування, тривимірне комп'ютерне моделювання. Захоплення та хоббі: читання наукової літератури про інформаційні технології та космос. Адреса: Україна, 61204. Харків, пр. Перемоги, 62Г, тел. +38 097 4352219.

КОМПЬЮТЕРНАЯ ИНЖЕНЕРИЯ И ТЕХНИЧЕСКАЯ ДИАГНОСТИКА



УДК 621.39

МЕТОД ЛОКАЛИЗАЦИИ ПОТЕРИ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ НА ОСНОВЕ СЛОТ-ТЕХНОЛОГИИ

*БАРАННИК В.В., ПОДЛЕСНЫЙ С.А.,
БАРАННИК Д.В.*

Показывается проблематичность обеспечения информационной безопасности государственного видеoinформационного ресурса. Рассматриваются основные недостатки статистического кодирования при обработке видео в случае применения кибератак. Обосновывается необходимость разработки технологии распределения кодов переменной длины для видеопотока. В результате этого формируется механизм локализации потери целостности информации.

Ключевые слова: видеoinформационный ресурс, кибератака, обработка видео, информационная безопасность.

Keywords: video information resource, cyber attack, video processing, information security.

1. Введение

В результате бурного развития информационных технологий появилась возможность применения видеoinформационного ресурса в государственных учреждениях. Итогом данного нововведения явилось улучшение качества системы управления [1]. Использование видеoinформационного ресурса для односторонней передачи реализовано в системах видеомониторинга, а для двунаправленной – в системах видеосвязи. В связи с важностью содержания видеoinформационный ресурс, как и любой другой государственный информационный ресурс, нуждается в защите [2]. Это обусловлено ростом кибернетических угроз государственным учреждениям, возникающих в результате кибератак [3].

В связи с легкостью осуществления наиболее распространенными видами кибератак являются атаки типа DDoS [4]. Существующие механизмы киберзащиты, работающие на различных сетевых уровнях [5], идентифицируют кибератаку по соответствию количественных параметров. Результатом данного типа реакции является обнаружение атаки, когда она уже перешла в активную фазу. Кибератака проявляется внешне как искажение, пропадание и полная недоступность видеoinформационного ресурса.

Вследствие этого наступает необходимость улучшения информационной безопасности видеoinформационного

ресурса путем разработки технологии кодирования с учетом воздействия кибератак на ресурс. Актуальность работы связана с важностью видеoinформационного ресурса и необходимостью увеличения его устойчивости к нарушениям информационной безопасности.

Для решения поставленной задачи необходимо рассмотреть существующие технологии обработки видеoinформационного ресурса. Существующие технологии (JPEG, MPEG-4, H.264) применяют сжатие на основе статистического кодирования (кодов переменной длины) [6]. Уменьшение информационной интенсивности связано с наличием корреляционной связи между кадрами в группе кадров. Данная группа кадров состоит из опорного кадра и последовательности разностных и обратных кадров. При этом на объем опорного кадра видео приходится малая доля объема всей группы кадров. Применение опорных кадров в процессе обработки приводит к уменьшению информационной интенсивности потока и в то же время повышает риск нарушения целостности и доступности потока к искажениям [7]. Это связано с возможностью потери содержимого всей группы кадров для потока видеoinформационного ресурса при искажении указанными кибератаками небольшого участка опорного кадра. В результате запаздывания реакции применение краткосрочных атак (медленной DDoS-атак) приводит к отсутствию идентификации угрозы при фактической недоступности видеoinформационного ресурса. В силу динамических условий использования видеoinформационного ресурса это считается недопустимым, так как указывает на недостаточную оперативность противодействия киберугрозам для существующих методов защиты. Это приводит к необходимости разработки технологии, которая локализует действие битовых ошибок на видеoinформационный ресурс.

Для этого необходимо рассмотреть недостатки современных технологий кодирования видеоданных. В существующей схеме обработки видеoinформационного ресурса после дискретно-косинусного преобразования сегментов исходного изображения используется статистическое кодирование полученных компонент линеаризованной трансформанты. Ввиду префиксности статистического кода переменной длины устраняется необходимость в символах-разделителях для декодирования компонент трансформанты изображения. В результате этого декодирование каждого кода производится только последовательно. При наличии битовой ошибки в коде происходит неверная идентификация кода и его длины, что приводит к дальнейшей неверной идентификации всех последующих VLC-кодов, которая выражается в разрушении всего изображения. Из этого вытекает, что наличие битовой ошибки в коде приводит к уязвимости целостности информации, которая содержится в последовательности кодов.

Поэтому цель работы заключается в создании метода локализации потери целостности информации вследствие неверного позиционирования статистических кодов при наличии ошибки в потоке и рассмотрении

изменения устойчивости видеоинформационного ресурса к ошибкам для предложенной технологии.

2. Разработка метода локализации потери целостности информации

Для устранения неверной идентификации начала каждого кода при битовых ошибках в целях позиционирования предлагается использовать технологию упругого к ошибкам энтропийного кодирования (Error Resilient Entropy Code – EREC). Данная технология задается функцией преобразования f_{errec} . Это определяется таким соотношением:

$$L(\theta) \xrightarrow{f_{\text{errec}}} S(\Lambda). \quad (1)$$

Здесь f_{errec} – функция распределения VLC-кодов ℓ_ξ по слотам s_λ ; Λ – количество слотов, в которые распределены VLC-коды.

Технология EREC характеризуется следующими этапами:

- размещение содержимого кодовых конструкций ℓ_ξ ;
- перераспределение содержимого кодовых конструкций ℓ_ξ .

Данная технология размещает VLC-коды ℓ_ξ в слоты пакета EREC $S(\Lambda)$ на основе перестройки битовой структуры. Здесь учитывается, что слотами являются кодовые слова равномерной длины, т.е.:

$$|s_i|_2 = |s_j|_2 = v, \text{ при } i \neq j. \quad (2)$$

В результате преобразования последовательности $L(\theta)$ VLC-кодов образуется пакет $S(\Lambda)$ слотов. Вектор слотов (пакет) записывается следующим образом:

$$S(\Lambda) = \{s_1; \dots; s_\lambda; \dots; s_\Lambda\}.$$

Здесь s_1 – начальный слот в пакете; s_Λ – последний слот в пакете.

Схематическое распределение VLC-кодов ℓ_ξ по слотам s_ξ , т.е.:

$$\ell_\xi \rightarrow s_\xi^{(1)},$$

в соответствии с технологией EREC, показано на рис. 1.

В данной формуле $s_\xi^{(1)}$ – слот, сформированный при размещении кода ℓ_ξ ; (1) – индекс начального этапа, соответствующий первичному размещению VLC-кодов по слотам.

На рис. 1 представлено распределение кодового потока $L(\theta)$, состоящего из $\Lambda = 19$ VLC-кодов ℓ_ξ по 19 слотам. Различные VLC коды ℓ_ξ представлены схематично в виде различных по окраске и размеру прямоугольников.

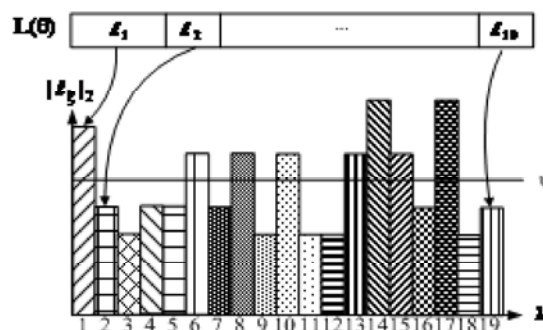


Рис. 1. Первичный этап размещения битовых составляющих кодовых конструкций при формировании пакета слотов

На первичном этапе рассматривается размещение VLC кодов ℓ_ξ по слотам s_ξ без учета их выравнивания по длине v . Порядок заполнения слотов s_ξ определяется следующими правилами:

- 1) первое правило состоит в установлении порядка расстановки VLC-кодов по слотам пакета. Согласно этому правилу 1-я кодовая последовательность ℓ_1 размещается в слоте s_1 (как показано на рис. 1);
- 2) второе правило заключается в установке порядка заполнения слотов разрядами VLC-кодов. Согласно этому правилу старшие разряды $q_{\xi,\gamma}$; $\gamma \rightarrow 1$ кодовой конструкции ℓ_ξ размещаются в нижних битовых позициях слота s_ξ . Наоборот, младшие разряды $q_{\xi,\gamma}$; $\gamma \rightarrow |\ell_\xi|_2$ кодовой конструкции ℓ_ξ размещаются в верхних битовых позициях слота s_ξ .

Следующим этапом формирования пакета слота является выравнивание длин кодовых слов s_ξ для выполнения условия (2) в случае, когда известно количество Λ слотов в пакете. Для этого сначала требуется найти длину v слота.

Длина v слота определяется как отношение суммарной длины $|L(\theta)|_2$ последовательности $L(\theta)$ кодов к количеству Λ слотов. Формула расчета длины указана в следующем выражении:

$$v = \frac{|L(\theta)|_2}{\Lambda} = \left\lceil \frac{1}{\Lambda} \sum_{i=1}^{\theta} |\ell_i|_2 \right\rceil. \quad (3)$$

Здесь $\lceil x \rceil$ – оператор округления значения x до большего натурального числа.

После определения длины υ слота возможны случаи, когда длина $|\ell_\xi|_2$ VLC-кода ℓ_ξ будет превышать длину υ слота

$$|\ell_\xi|_2 > \upsilon,$$

или будет меньше, т.е.: $|\ell_\xi|_2 < \upsilon$.

Данные случаи схематически показаны на рис. 2.

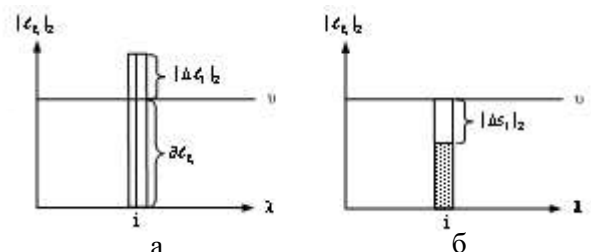


Рис. 2. Размещение VLC-кода ℓ_i при заполнении слота s_i для двух случаев длины $|\ell_i|_2$ кода ℓ_i : а – длина $|\ell_i|_2$ VLC-кода ℓ_i будет превышать длину υ слота; б – длина кода $|\ell_i|_2$ VLC-кода ℓ_i меньше длины υ слота

Для повышения эффективности заполнения слотов в соответствии с технологией EREC происходит перераспределение избыточных составляющих $\Delta\ell_\xi$ VLC кодов ℓ_ξ по избыточным составляющим Δs_i , $i \neq \xi$ слотов s_i , $i \neq \xi$, что задается формулой:

$$\Delta L(\theta) \xrightarrow{f_p} \Delta S(\Lambda), \quad (4)$$

где $\Delta L(\theta) = \{\Delta\ell_1; \dots; \Delta\ell_\xi; \dots; \Delta\ell_\theta\}$ – совокупность избыточных составляющих $\Delta\ell_\xi$ VLC-кодов ℓ_ξ ;

$\Delta S(\Lambda) = \{\Delta s_1; \dots; \Delta s_\xi; \dots; \Delta s_\Lambda\}$ – совокупность избыточных составляющих Δs_ξ слота s_ξ .

Это позволит:

- 1) сохранить информацию VLC-кодов ℓ_ξ на основе заполнения пустот слотов s_ξ ;
- 2) сократить избыточность, вызванную недогрузкой слота.

В общем случае избыточная составляющая $\Delta\ell_\xi$ VLC-кода ℓ_ξ будет размещена по нескольким слотам s_i (рис. 3).

Процесс перераспределения избыточных составляющих $\Delta\ell_\xi$ VLC-кодов ℓ_ξ , с учетом размещения по нескольким слотам s_i , включает в себя следующие этапы (рис. 4):

- 1) определение позиций i избыточных составляющих Δs_i ,

$$i = \begin{cases} \xi + 1; \Lambda & \text{при } i > \xi; \\ 1; \xi - 1 & \text{при } i < \xi \end{cases}$$

слотов s_i относительно перераспределяемой избыточной составляющей $\Delta\ell_\xi$ кода ℓ_ξ ;

- 2) определение количества υ_{cm} и размеров $|\Delta s_i|_2$ избыточных составляющих Δs_i слотов s_i , в которые будут распределены избыточные составляющие $\Delta\ell_\xi$ для ξ -о VLC-кода. Избыточные составляющие Δs_i слотов s_i образуют подпоследовательность $\Delta S(\upsilon_{cm})$, которая записывается следующим образом:

$$\Delta S(\upsilon_{cm}) = \{\Delta s_i; \dots; \Delta s_g; \dots; \Delta s_{\upsilon_{cm}}\}. \quad (5)$$

Здесь υ_{cm} – количество слотов (этапов), в которые происходит перераспределение всей избыточной составляющей $\Delta\ell_\xi$, длиной $|\Delta\ell_\xi|_2$; Δs_g – избыточная составляющая слота s_g при g -м этапе заполнения слота.

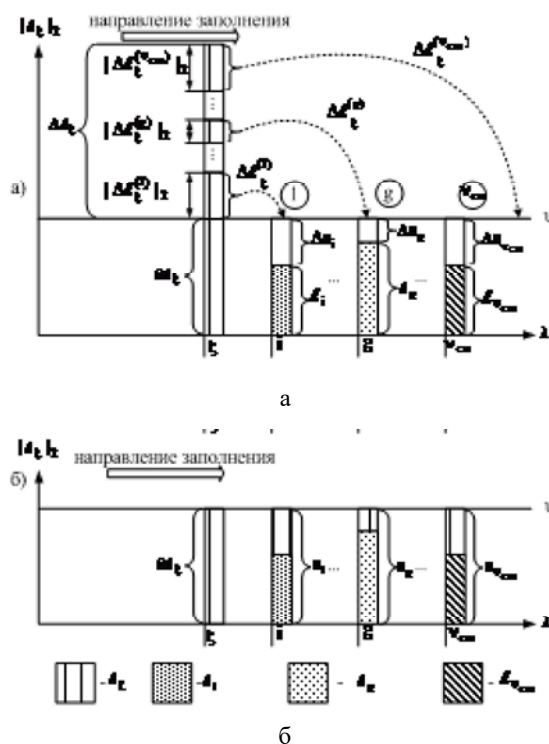


Рис. 3. Структурная схема многослотового распределения VLC: а – до распределения; б – после распределения

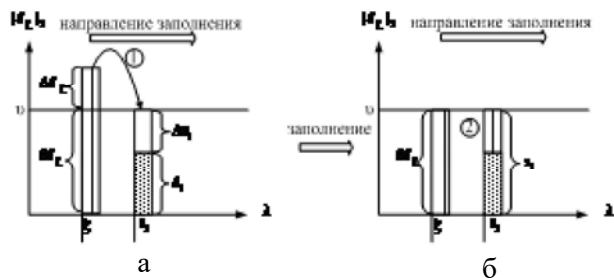


Рис. 4. Структурная схема однослотового распределения VLC: а – начало распределения; б – результат заполнения

Условие перераспределения информации без потерь заключается в обеспечении равенства суммы

$\sum_{i=1}^{v_{cm}} |\Delta s_i|_2$ размеров составляющих Δs_i подпоследовательности $\Delta S(v_{cm})$ и длины $|\Delta \ell_\xi|_2$ избыточной составляющей $\Delta \ell_\xi$ VLC-кода ℓ_ξ , т.е.:

$$\sum_{i=1}^{v_{cm}} |\Delta s_i|_2 = |\Delta \ell_\xi|_2. \quad (6)$$

Тогда для реализации процесса перераспределения избыточных составляющих $\Delta \ell_\xi$ VLC-кодов ℓ_ξ необходимо:

а) провести оценку соответствия длины $|\Delta \ell_\xi|_2$ избыточных составляющих $\Delta \ell_\xi$ относительно количества v_{cm} и размеров избыточных составляющих Δs_i слотов s_i ;

б) заполнить разрядами избыточных составляющих $\Delta \ell_\xi$ VLC-кодов ℓ_ξ позиции подпоследовательности $\Delta S(v_{cm})$ избыточных составляющих Δs_i слотов s_i .

Рассмотрим механизм оценки соответствия длины $|\Delta \ell_\xi|_2$ избыточных составляющих $\Delta \ell_\xi$ относительно количества и размеров избыточных составляющих Δs_i слотов s_i . Такая оценка проводится в направлении слева направо от текущего VLC-кода ℓ_ξ .

Для привязки i -й позиции к распределению составляющих $\Delta \ell_\xi$ VLC-кодов предлагается ввести относительную нумерацию избыточных составляющих Δs_i слотов s_i , которые будут участвовать в распределении избыточных составляющих $\Delta \ell_\xi$ VLC-кодов. Для этого вводится переменная d_g :

$$d_g = g - \xi,$$

значение которой определяет расстояния между позицией распределяемого VLC-кода ℓ_ξ и позицией слота s_g в последовательности $S(\Lambda)$ на g -м этапе оценки. В этом случае позиции избыточных составляющих Δs_i слотов s_i подпоследовательности $\Delta S(v_{cm})$ из (5) определяются вектором $D(v_{cm})$ смещения:

$$D(v_{cm}) = \{d_1; \dots; d_g; \dots; d_{v_{cm}}\}. \quad (7)$$

Вектор $D(v_{cm})$ смещения характеризуется следующими свойствами:

1) количество v_{cm} элементов вектора $D(v_{cm})$ меньше количества Λ слотов: $v_{cm} < \Lambda$;

2) значение элемента d_g меньше количества Λ слотов: $d_g < \Lambda$;

3) все элементы вектора $D(v_{cm})$ различаются по величине: $d_i \neq d_j, i \neq j$.

В результате этого выражение (5) принимает вид:

$$\Delta S(v_{cm}) = \{\Delta s_{\xi+d_1}; \dots; \Delta s_{\xi+d_g}; \dots; \Delta s_{\xi+d_{v_{cm}}}\}.$$

При этом формула, определяющая распределение избыточной составляющей $\Delta \ell_\xi$ VLC кода ℓ_ξ по слотам, будет следующая:

$$|\Delta \ell_\xi|_2 = \sum_{g=1}^{v_{cm}} |\Delta s_{\xi+d_g}|_2, \quad d_g = \overline{1; \Lambda-1}. \quad (8)$$

Теперь рассмотрим технологию непосредственного распределения избыточной составляющей $\Delta \ell_\xi$, которая включает в себя следующие этапы.

На первичном этапе $g = 1$ для избыточной составляющей $\Delta \ell_\xi$ VLC-кода ℓ_ξ с порядковым номером ξ проверяется остаток слота $\Delta s_{\xi+d_g}^{(\gamma)}$ с позицией $\xi + d_g$. Данный остаток слота $\Delta s_{\xi+d_g}^{(\gamma)}$ образовался в результате заполнения слота $s_{\xi+d_g}$ с позицией $\xi + d_g$ VLC-кодом $\ell_{\xi+d_g}$ и некоторым количеством γ избыточных составляющих $\Delta \ell_i$ кодов ℓ_i с позицией $i \neq \xi$ (рис. 5).

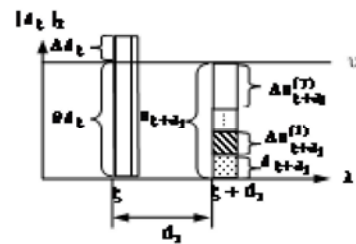


Рис. 5. Распределение VLC-кода ℓ_ξ остатка слота

$$\Delta s_{\xi+d_g}^{(\gamma)}$$

Избыточная составляющая $\Delta \ell_\xi$ распределяется в остаток слота $\Delta s_{\xi+d_1}^{(\gamma)}$, размер которого рассчитывается по формуле:

$$|\Delta s_{\xi+d_1}^{(\gamma)}|_2 = v - |\ell_{\xi+d_1}|_2 - \sum_{i=1}^{\gamma-1} |\Delta s_{\xi+d_1}^{(i)}|_2.$$

Избыточная составляющая слота $\Delta s_{\xi+d_1}^{(\gamma)}$ с порядковым номером $(\xi+d_1)$ характеризуется размером $|\Delta s_{\xi+d_1}^{(\gamma)}|_2$. При оценке соответствия длины $|\Delta \ell_{\xi}|_2$ избыточных составляющих $\Delta \ell_{\xi}$ относительно размера избыточных составляющих $\Delta s_{\xi+d_1}^{(\gamma)}$ слотов $s_{\xi+d_1}$ возможны три результирующих варианта:

1) Длина $|\Delta \ell_{\xi}|_2$ избыточной составляющей $\Delta \ell_{\xi}$ равна размеру $|\Delta s_{\xi+d_1}|_2$ избыточной составляющей $|\Delta s_{\xi+d_1}^{(\gamma)}|_2$, т.е.: $|\Delta \ell_{\xi}|_2 = |\Delta s_{\xi+d_1}^{(\gamma)}|_2$.

При первом варианте оценки размера избыточная составляющая $\Delta s_{\xi+d_1}^{(\gamma)}$ слота $s_{\xi+d_1}$ будет полностью заполнена разрядами избыточной составляющей $\Delta \ell_{\xi}$ кода ℓ_{ξ} , а именно: $\Delta \ell_{\xi} \rightarrow \Delta s_{\xi+d_1}^{(\gamma)}$.

При этом распределение VLC кода ℓ_{ξ} по слотам заканчивается. Схематически результат заполнения показан на рис. 6.

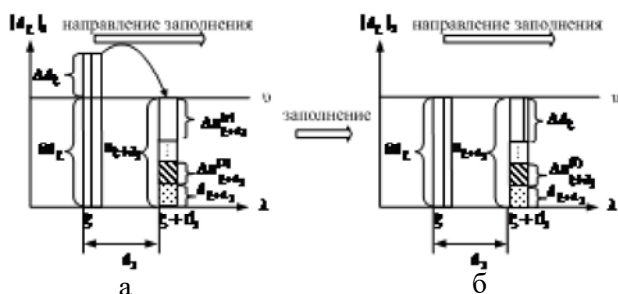


Рис. 6. Распределение VLC- кода ℓ_{ξ} для условия

$|\Delta s_{\xi+d_1}|_2 = |\Delta \ell_{\xi}|_2$: а – до распределения; б – после распределения

2) Длина $|\Delta \ell_{\xi}|_2$ избыточной составляющей $\Delta \ell_{\xi}$ меньше размера $|\Delta s_{\xi+d_1}^{(\gamma)}|_2$ избыточной составляющей $\Delta s_{\xi+d_1}^{(\gamma)}$, т.е.: $|\Delta \ell_{\xi}|_2 < |\Delta s_{\xi+d_1}^{(\gamma)}|_2$.

Для данного варианта оценки соответствия длины $|\Delta \ell_{\xi}|_2$ избыточной составляющей $\Delta \ell_{\xi}$ относительно размера избыточной составляющей $\Delta s_{\xi+d_1}^{(\gamma)}$ слота

$|\Delta s_{\xi+d_1}^{(\gamma)}|_2$ изменится избыточная составляющая $\Delta s_{\xi+d_1}^{(\gamma+1)}$ слота $s_{\xi+d_1}$ относительно длины v слота.

Длина $|\Delta s_{\xi+d_1}^{(\gamma+1)}|_2$ избыточной составляющей $\Delta s_{\xi+d_1}^{(\gamma+1)}$

находится как разность размера $|\Delta s_{\xi+d_1}^{(\gamma)}|_2$ избыточной составляющей $\Delta s_{\xi+d_1}^{(\gamma+1)}$ слота $s_{\xi+d_1}$ и длины $|\Delta \ell_{\xi}|_2$ избыточной составляющей $\Delta \ell_{\xi}$ кода ℓ_{ξ} , а именно:

$$|\Delta s_{\xi}^{(\gamma+1)}|_2 = |\Delta s_{\xi+d_1}^{(\gamma)}|_2 - |\Delta \ell_{\xi}|_2.$$

При этом избыточная составляющая $\Delta \ell_{\xi}$ кода ℓ_{ξ} заполнит старшие разряды избыточной составляющей $\Delta s_{\xi+d_1}^{(\gamma+1)}$ слота $s_{\xi+d_1}$. Распределение VLC- кода ℓ_{ξ} так же, как и для первого варианта, заканчивается. Схематически результат заполнения показан на рис. 7.

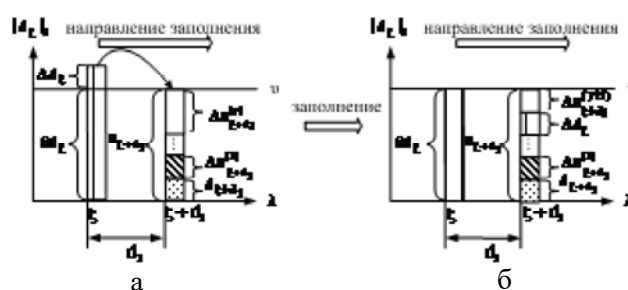


Рис. 7. Распределение VLC- кода ℓ_{ξ} при

$|\Delta \ell_{\xi}|_2 < |\Delta s_{\xi+d_1}^{(\gamma)}|_2$: а – до распределения; б – после распределения.

3) Длина $|\Delta \ell_{\xi}|_2$ избыточной составляющей $\Delta \ell_{\xi}$ превышает размер $|\Delta s_{\xi+d_1}^{(\gamma)}|_2$ избыточной составляющей $\Delta s_{\xi+d_1}^{(\gamma)}$, т.е.: $|\Delta \ell_{\xi}|_2 > |\Delta s_{\xi+d_1}^{(\gamma)}|_2$.

Для данного варианта оценки соответствия длины $|\Delta \ell_{\xi}|_2$ избыточной составляющей $\Delta \ell_{\xi}$ относительно размера избыточной составляющей $\Delta s_{\xi+d_1}^{(\gamma)}$ слота $|\Delta s_{\xi+d_1}^{(\gamma)}|_2$ будет образована избыточная составляющая $\Delta \ell_{\xi}^{(2)}$ кода ℓ_{ξ} относительно длины избыточной составляющей $\Delta s_{\xi+d_1}^{(\gamma)}$ слота $s_{\xi+d_1}$.

Избыточная составляющая $\Delta \ell_{\xi}^{(1)}$ заполнит избыточную составляющую $\Delta s_{\xi+d_1}^{(\gamma)}$ слота $s_{\xi+d_1}$:

$$|\Delta \ell_{\xi}^{(1)}|_2 = |\Delta s_{\xi+d_1}^{(\gamma)}|_2.$$

При этом длина избыточной составляющей $\Delta l_{\xi}^{(2)}$ находится как разность длины $|\Delta l_{\xi}|_2$ избыточной составляющей Δl_{ξ} кода l_{ξ} и размера $|\Delta s_{\xi+d_1}^{(\gamma)}|_2$ избыточной составляющей $\Delta s_{\xi+d_1}^{(\gamma)}$ слота $s_{\xi+d_1}$, а именно: $|\Delta l_{\xi}^{(2)}|_2 = |\Delta l_{\xi}|_2 - |\Delta s_{\xi+d_1}^{(\gamma)}|_2$.

Старшие разряды избыточной составляющей Δl_{ξ} кода l_{ξ} при этом заполняют избыточную составляющую $\Delta s_{\xi+d_1}^{(\gamma)}$ слота $s_{\xi+d_1}$. Схематически результат заполнения показан на рис. 8.

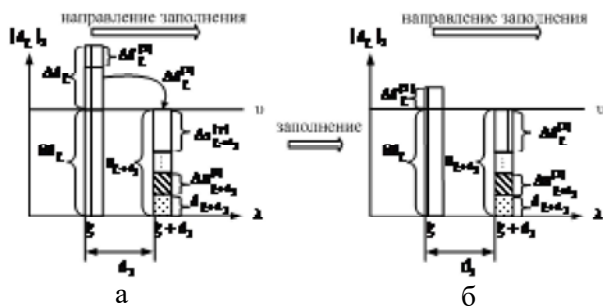


Рис. 8. Распределение VLC кода l_{ξ} при

$|\Delta l_{\xi}|_2 > |\Delta s_{\xi+d_1}^{(\gamma)}|_2$: а – до распределения; б – после распределения

Для g -го этапа распределения избыточной составляющей $\Delta l_{\xi}^{(g)}$ VLC-кода l_{ξ} с позицией ξ проверяется остаток слота $\Delta s_{\xi+d_g}^{(\gamma)}$ с позицией $\xi+d_g$. Данный остаток слота $\Delta s_{\xi+d_g}^{(\gamma)}$ образовался в результате заполнения слота $s_{\xi+d_g}$ с позицией $\xi+d_g$ VLC-кодом $l_{\xi+d_g}$ и некоторым количеством γ избыточных составляющих Δl_i кодов l_i с позицией $i \neq \xi$.

Старшие разряды избыточной составляющей Δl_{ξ} кода l_{ξ} при этом заполняют избыточную составляющую $\Delta s_{\xi+d_g}^{(\gamma)}$ слота $s_{\xi+d_g}$. Схематически результат заполнения показан на рис. 9.

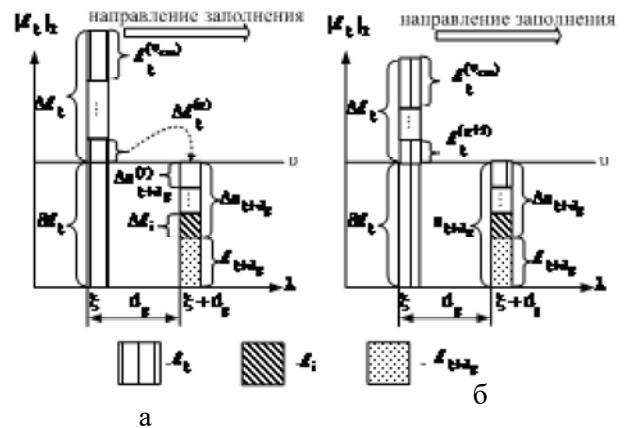


Рис. 9. Распределение VLC-кода l_{ξ} на g -м этапе: а – до распределения; б – после распределения

Этапы перераспределения VLC-кода l_{ξ} повторяются до устранения в позиции ξ положительной избыточности, вызванной перегрузкой слота.

Результат окончательного распределения VLC-кода l_{ξ} с позицией ξ за v_{cm} этапов показан на рис. 10.

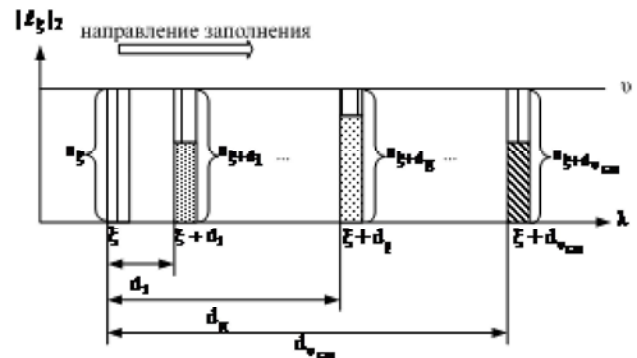


Рис. 10. Результат распределения VLC-кода l_{ξ}

Различные VLC-коды l_{ξ} представлены схематично в виде различных по окраске и размеру прямоугольников.

Распределение всей последовательности $L(\theta)$ VLC-кодов l_{ξ} происходит по аналогичному сценарию.

Остаточная избыточность δ после перераспределения находится как разность между длиной $|S(\Lambda)|_2$ пакета слотов и длиной $|L(\theta)|_2$ последовательности кодов:

$$\delta = |S(\Lambda)|_2 - |L(\theta)|_2 = \Lambda \times v - \sum_{i=1}^{\Lambda} |l_i|_2. \quad (9)$$

С учетом того, что длина v слота является целым числом

$$v = \left\lceil \frac{1}{\Lambda} \sum_{i=1}^{\Lambda} |\ell_i|_2 \right\rceil,$$

количество δ остаточной избыточности определяется значением остатка от деления длины $|L(\theta)|_2$ последовательности кодов на количество Λ слотов:

$$\delta \sim \left(\sum_{i=1}^{\Lambda} |\ell_i|_2 \right) \bmod \Lambda.$$

В связи с тем, что данный остаток $\left(\sum_{i=1}^{\Lambda} |\ell_i|_2 \right) \bmod \Lambda$

имеет значения в диапазоне $(0; \Lambda - 1)$, количество δ остаточной избыточности имеет следующую величину:

$$\delta \in [0; \Lambda - 1],$$

т.е. максимальное значение остаточных избыточных бит зависит от количества слотов:

$$\delta_{\max} = \Lambda - 1.$$

Результат распределения всей последовательности $L(\theta)$ VLC-кодов ℓ_ξ , представленной на рис. 1, по пакету $S(\Lambda)$ слотов s_ξ , в соответствии с технологией EREC, показан на рис. 11.

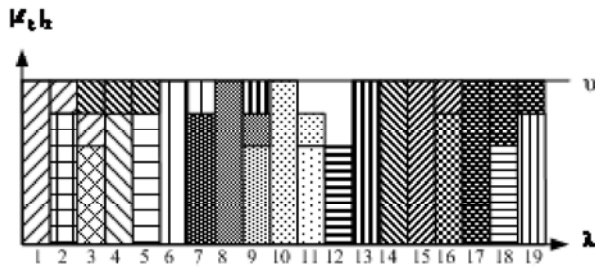


Рис. 11. Результат размещения битовых составляющих кодовых конструкций в сформированном пакете слотов

3. Оценка эффективности локализации битовой ошибки в последовательности кодов

Для оценки эффективности локализации битовой ошибки необходимо рассмотреть процесс декодирования распределенных VLC-кодов ℓ_ξ и восстановления компонент u_ξ трансформанты на приемной стороне.

По условиям предлагаемого алгоритма необходимо идентифицировать VLC-коды ℓ_ξ , полностью вошедшие в соответствующие слоты s_ξ при первичном заполнении, и определить номер i -х позиций слотов s_i , которые имеют избыточность $|s_i|_2$. Номер пози-

ции необходим для сборки VLC-кодов ℓ_ξ , которые были распределены по нескольким слотам s_i .

В предлагаемом алгоритме количество слотов s_λ составляет фиксированное значение Λ . При этом информация о длине $|S(\Lambda)|_2$ пакета слота предоставляется декодеру в служебной информации. Используя длину $|S(\Lambda)|_2$ пакета $S(\Lambda)$ слотов и количество Λ слотов, декодер определяет длину v слота:

$$v = \frac{|S(\Lambda)|_2}{\Lambda}.$$

Информация о длине слота позволяет определить позиционирование всех слотов s_λ в пакете $S(\Lambda)$. Порядок заполнения слотов s_ξ предоставляет возможность идентифицировать начало α_ξ каждого кода ℓ_ξ , как указано на рис. 12.

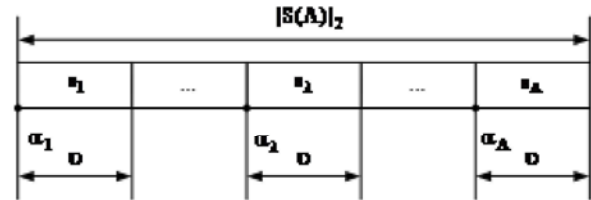


Рис. 12. Процесс разделения пакета $S(\Lambda)$ слотов s_λ и определения начала α_λ кодов ℓ_λ

Это позволяет декодеру синхронизироваться с потоком битов в начале каждого слота.

Из пакета $S(\Lambda)$ выделяется отдельный слот s_ξ и производится процесс поразрядной сборки VLC-кода ℓ_ξ . При поразрядной сборке первого VLC-кода ℓ_1 индекс позиции VLC-кода ℓ_ξ в кодовом потоке принимается равным $\xi = 1$.

На первоначальном этапе $g = 1$ старшему разряду $q_{\xi,1}$ кода ℓ_ξ приводится в соответствие значение двоичного разряда $h_{\xi,1}$ нижней битовой позиции слота s_ξ , т.е.:

$$q_{\xi,1} := h_{\xi,1}. \quad (10)$$

При этом данный разряд формирует содержимое части кода $\partial \ell_\xi$:

$$[\partial \ell_\xi]_2 = \{q_{\xi,1}\}.$$

В результате этого длина $|\partial \ell_\xi|_2$ части кода $\partial \ell_\xi$ равняется:

$$|\partial \ell_\xi|_2 = 1.$$

После этого декодер на основе функции $f_{\text{vlc}}^{-1}(\partial \ell_{\xi}, P_{\text{сл}})$ производит идентификацию окончания ξ -й кодовой комбинации ℓ_{ξ} .

Успешная идентификация приводит к таким последствиям:

- а) кодовой комбинации ℓ_{ξ} приводится в соответствие часть кода $\partial \ell_{\xi}$: $\ell_{\xi} := \partial \ell_{\xi}$;
- б) восстанавливается соответствующая компонента u_{ξ} ;
- в) фиксируется длина $|\partial \ell_{\xi}|_2$ части кода $\partial \ell_{\xi}$;
- г) дальнейшая сборка VLC-кода ℓ_{ξ} прекращается.

Если идентификация окончания ξ -й кодовой комбинации ℓ_{ξ} не удалась, то разряду $q_{\xi,2}$ кода ℓ_{ξ} приводится в соответствие двоичный разряд $h_{\xi,2}$ следующей битовой позиции слота s_{ξ} , т.е.:

$$q_{\xi,2} := h_{\xi,2}. \quad (11)$$

При этом изменяется содержимое $[\partial \ell_{\xi}]_2$ части кода $\partial \ell_{\xi}$: $[\partial \ell_{\xi}]_2 = \{q_{\xi,1}; q_{\xi,2}\}$.

Соответственно длина $|\partial \ell_{\xi}|_2$ части кода $\partial \ell_{\xi}$ при этом увеличивается: $|\partial \ell_{\xi}|_2 := |\partial \ell_{\xi}|_2 + 1$.

После этого декодер на основе функции $f_{\text{vlc}}^{-1}(\partial \ell_{\xi}, P_{\text{сл}})$ повторно производит идентификацию окончания ξ -й кодовой комбинации ℓ_{ξ} .

Данные операции первоначального этапа побитного внесения двоичных разрядов $h_{\xi,\mu}$ слота s_{ξ} в содержимое части кода $\partial \ell_{\xi}$ продолжают до момента:

- 1) идентификации окончания ξ -й кодовой комбинации ℓ_{ξ} ;
- 2) использования всех двоичных разрядов $h_{\xi,\mu}$ слота s_{ξ} .

В первом случае декодер восстанавливает соответствующую компоненту u_{ξ} . Также при этом формируется избыточная составляющая Δs_{ξ} слота s_{ξ} . Она задается следующим образом:

$$[\Delta s_{\xi}]_2 = \{h_{\xi,|\ell_{\xi}|_2+1}; \dots; h_{\xi,v}\}. \quad (12)$$

В данной формуле $h_{\xi,\mu}$ – μ -й разряд слота s_{ξ} .

Длина $|\Delta s_{\xi}|_2$ избыточной составляющей слота Δs_{ξ} находится как разница длины v слота s_{ξ} и длины $|\ell_{\xi}|_2$ идентифицированного кода ℓ_{ξ} :

$$|\Delta s_{\xi}|_2 = v - |\ell_{\xi}|_2.$$

Во втором случае процесс дальнейшей поразрядной сборки VLC-кодов ℓ_{ξ} требует обращения к содержимому избыточных составляющих Δs_i других слотов s_i , $i \neq \xi$. Это обращение производится только после идентификации других VLC-кодов ℓ_i , $i \neq \xi$, т.е. выполнения этапа $g = 1$ на позициях всех слотов s_i .

Значения позиций данных избыточных составляющих Δs_i слотов s_i в последовательности $S(\Lambda)$ задается индексом VLC-кода ℓ_{ξ} и вектором смещения $D(v_{\text{см}})$.

При этом внесения двоичных разрядов $h_{\xi+d_g,\mu}$ избыточных составляющих $\Delta s_{\xi+d_g}^{(\gamma)}$ слота $s_{\xi+d_g}$ в содержимое части кода $\partial \ell_{\xi}$ продолжают до идентификации окончания ξ -й кодовой комбинации ℓ_{ξ} . Следует заметить, что каждый этап сборки VLC-кодов ℓ_{ξ} должен происходить после завершения предыдущего на позициях всех слотов s_i .

Результат формирования кода ℓ_{ξ} при обращении к битовым составляющим нескольких слотов представлен на рис. 13.

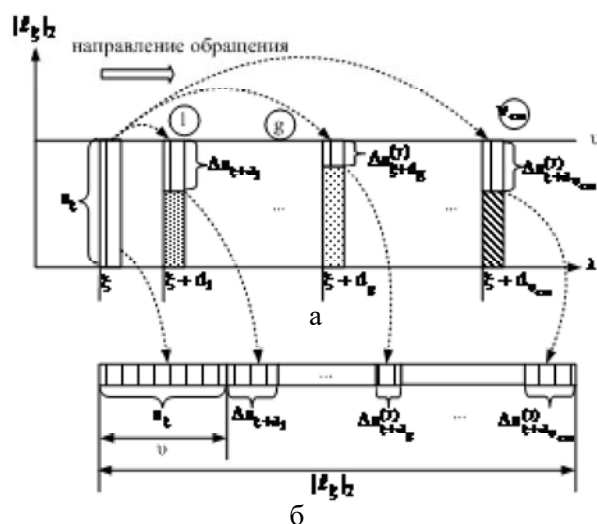


Рис. 13. Сборка VLC-кода ℓ_{ξ} по подпоследовательности $\Delta S(v_{\text{см}})$ до идентификации окончания кодовой комбинации ℓ_{ξ} : а – изъятие битовых составляющих других слотов $s_{\xi+d_g}$; б – результат формирования кода ℓ_{ξ}

Выражение (10) позволяет производить параллельную обработку всех слотов s_ξ в пакете $S(\Lambda)$. Остаточная избыточность битов, которые использовались при формировании пакета $S(\Lambda)$ слотов s_ξ , на результат декодирования не влияют. Результатом обработки всех слотов s_ξ в пакете $S(\Lambda)$ является восстановление всех компонент u_ξ линейаризованной трансформанты.

При наличии битовой ошибки в μ -м разряде $h'_{\lambda,\mu}$ λ -го слота s_λ : $h'_{\lambda,\mu} \neq h_{\lambda,\mu}$

процесс декодирования будет зависеть от битового положения в слоте:

1) Если идентификация λ -й кодовой комбинации ℓ_λ до считывания разряда $h_{\lambda,\mu}$ слота s_λ не была произведена, то возможна неверная идентификация окончания λ -й кодовой комбинации ℓ'_λ .

2) При идентификации λ -й кодовой комбинации ℓ_λ ошибка затрагивает избыточную составляющую $\Delta s_\lambda^{(\gamma)}$ слота s_λ , к которой идет обращение при сборке на g -м этапе ξ -го кода ℓ_ξ , $\xi = \lambda - d_g$. При этом также возможна неверная идентификация окончания ξ -й кодовой комбинации ℓ'_ξ . Идентификация кода ℓ_λ и ℓ_i кодов ℓ_i , избыточные составляющие которых входят в избыточные составляющие $\Delta s_\lambda^{(j)}$, $j < \gamma$ слота s_λ , будет произведена верно.

Для первого варианта положения ошибочного разряда $h'_{\lambda,\mu}$ при изменении длины $|\ell'_\lambda|_2$ кодовой комбинации ℓ'_λ :

а) в сторону увеличения $|\ell'_\lambda|_2 > |\ell_\lambda|_2$ ошибка распространяется на коды ℓ_i , которые при сборке должны были использовать разряды слотов s_i с позицией $i \in \{\lambda + d_{v_{cm}}; \dots; \lambda + d_{v'_{cm}}\}$ и битовое положение в слоте после избыточной составляющей $\ell'^{(v'_{cm})}_\lambda$ кода ℓ'_λ ;

б) в сторону уменьшения $|\ell'_\lambda|_2 < |\ell_\lambda|_2$ ошибка распространяется на коды ℓ_i , которые при сборке будут использовать разряды слотов s_i с позицией $i \in \{\lambda + d_{v_{cm}}; \dots; \lambda + d_{v'_{cm}}\}$ и битовое положение в слоте после избыточной составляющей $\ell'^{(v'_{cm})}_\lambda$ кода ℓ'_λ .

При втором варианте положения ошибочного разряда $h'_{\lambda,\mu}$ ситуация повторяется для кода ℓ'_ξ .

Наглядное представление неверного декодирования пакета слотов с рис. 11 при ошибке разряда 5 в слоте 1 показано на рис. 14.

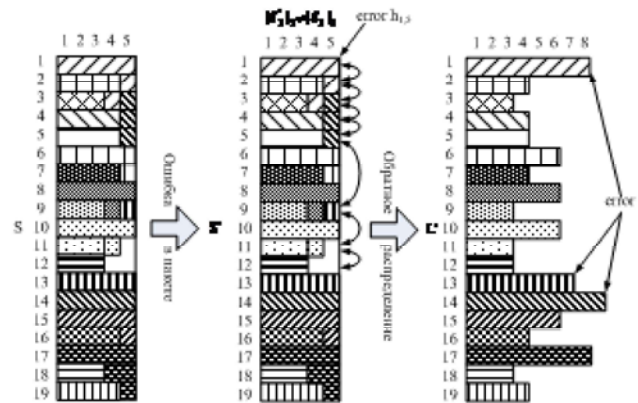


Рис. 14. Влияние ошибки в разряде $h_{1,5}$ слота s_1 на определение длин $|\ell_i|_2$ кодов ℓ_i последовательности $L(\theta)$

В случае ошибочного декодирования первого кода ℓ_1 декодер неверно определит длину первого кода. Для обратного распределения коды с 2 по 12 и с 15 по 19 останутся незатронутыми. Для кодов 1, 13 и 14 декодер может использовать как предыдущие, так и следующие значения разрядов, определенных алгоритмом распределения.

В результате ошибка в слоте 1 приведет к неверному декодированию блоков 1, 13 и 14. При отсутствии распределения блоков по слотам ошибка распространилась бы на все кодируемые блоки. В результате достигается локализация потери целостности информации на основе слот-технологии.

Обратно-пропорциональная зависимость длины статистического кода от частоты его появления позволяет при использовании слот-технологии защитить от битовой ошибки ВЧ компоненты трансформанты [8]. При этом лавинный эффект ошибки для НЧ компонент изображения устранить полностью не удастся. Для его устранения предлагается использовать изменяющуюся избыточность распределения с механизмом обратной связи между кодером и декодером.

4. Выводы

- 1) Разработан метод локализации потери целостности информации на основе слот-технологии при незначительном увеличении длины пакета, который необходим для кодирования компонент.
- 2) Создана технология, которая учитывает применение кибератак на видеoinформационный ресурс.
- 3) Для локализации ошибки декодирования для НЧ компонент впервые предложено использовать дина-

мическую избыточность технологии распределения с механизмом обратной связи между кодером и декодером.

Литература: 1. Баранник В.В., Подлесный С.А. / Анализ действия кибератак на видеоинформационный ресурс в информационно-телекоммуникационных сетях // АСУ и приборы автоматики. Вып. 164. 2014. С. 16-22 **2.** Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007. № 537-V **3.** [Електронний ресурс] http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=104662&cat_id=38712, 2012. **4.** Звіт CERT-UA за 2014 рік, [Електронний ресурс], <http://cert.gov.ua/?p=2019>, 2015. **5.** Мартынюк И. Материалы технического тренинга «Построение безопасных сетей на оборудовании D-Link». [Електронний ресурс], <http://service.d-link.ua/sites/default/files/files/Security.zip>, Киев, 2012. 190 с. **6.** Richardson E. H.264 and MPEG-4 video compression. Chichester, UK: Wiley and Sons, 2003. 306 p. **7.** Wang Y. and Zhu Q. F. Error control and concealment for video communication: A review // Proceedings of the IEEE. Vol. 86. no. 5. P. 974-997. May 1998 **8.** Баранник В.В., Подлесный С.А. / Обґрунтування підходу щодо створення технології кіберзахисту відеоінформаційного ресурсу в інфокомунікаційному просторі дії кібератаки на відеоінформаційний ресурс в інформаційно-телекомунікаційних мережах // Радіоелектроніка та інформатика. 2015. №3. С.62-66.

Transliterated bibliography: 1. Analysis of the action of cyber-attacks in the video-information's resources in the information-telecommunications networks / V. Barannik, S. Podlesny // Management Information System and Devices. 2014. N 169. P.16-22. **2.** Zakon Ukraïni «Pro Osnovni zasady rozvitku informacijnogo suspil'stva v Ukraïni na 2007–2015 roki» vid 09.01.2007 № 537-V **3.** Zahist informacijnih mrezh є pitannjam derzhavnoï bezpeki - golova Derzhspeczv'jazku Gennadij Reznikov [Electronic resource] [http://](http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=104662&cat_id=38712)

www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=104662&cat_id=38712, 2012. **4.** CERT-UA Report 2014, [Electronic resource], <http://cert.gov.ua/?p=2019>, 2015. **5.** Martynjuk I. Materialy tehničeskogo treninga «Postroenie bezopasnyh setej na oborudovanii D-Link», [Electronic resource], <http://service.d-link.ua/sites/default/files/files/Security.zip>, Kiïv, 2012. 190 p. **6.** Richardson E. H.264 and MPEG-4 video compression. Chichester, UK: Wiley and Sons, 2003. 306 p. **7.** Y. Wang and Q. F. Zhu, “Error control and concealment for video communication: A review,” Proceedings of the IEEE, vol. 86, no. 5. pp. 974-997, May 1998 **8.** Obosnovanie podhoda k sozdaniju tehnologii kiberzashhity videoinformacionnuju resursa v infokommunikacionnyh prostranstve dejstvija kiberataki na Videoinformacionnyj resurs v informacionno-telekommunikacionnyh setjah / V. Barannik, S. Podlesny // Radioelektronika i informatika. 20015. N 3. P. 62-66.

Поступила в редколлегию 08.12.2015

Рецензент: д-р техн. наук, проф. Безрук В.М.

Баранник Владимир Викторович, д-р техн. наук, профессор, начальник кафедры боевого применения и эксплуатации АСУ Харьковского университета Воздушных Сил им. И. Кожедуба. Научные интересы: обработка и передача информации. Адрес: Украина, 61023, Харьков, ул. Сумская, 77/79.

Подлесный Сергей Анатоліевич, начальник отделения ХУВС. Научные интересы: технологии кодирования и обеспечения информационной безопасности государства. Адрес: Украина, 61023, Харьков, ул. Сумская, 77/79. Email: Barannik_V_V@mail.ru

Баранник Дмитрий Владимирович, студент ХНУРЭ. Научные интересы: кодирование и защита информации для передачи в телекоммуникационных системах. Адрес: Украина, 61023, Харьков, ул. Сумская, 77/79. E-mail: barannik_v_v@mail.ru.

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 компьютеринга

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 компьютеринга. 2) Перспективы квантового компьютеринга. 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 компьютеринга 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 компьютеринга: 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. Компьютеринг – замкнутая масштабируемая система мониторинга и управления процессами и явлениями для достижения поставленной цели. Развитие компьютеринга имеет четыре выраженных фазы: 1) Сингулярный компьютеринг. 2) Сетевой компьютеринг. 3) Глобальный компьютеринг. 4) Киберфизический компьютеринг.

2. Перспективы квантового компьютеринга

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 простран-

ства. 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 компьютеринга [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 Q_i , равно как и кортеж X_i вектора номеров входных линий, имеет адресную связь с M_i -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 эквивалентных 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 $M_i = Q_i[M(X_i)]$. 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: $W = \langle Q, M, X \rangle$, включая функциональные модули, вектор моделирования, вектор адресов входных переменных, являются online перепрограммируемыми, а значит – online ремонтпригодными. 8) Примитив цифровой системы имеет формат $W = \langle Q, Y, X \rangle$, поскольку отдельный элемент не имеет связей и вектора M, создающих из отдельных компонентов систему.

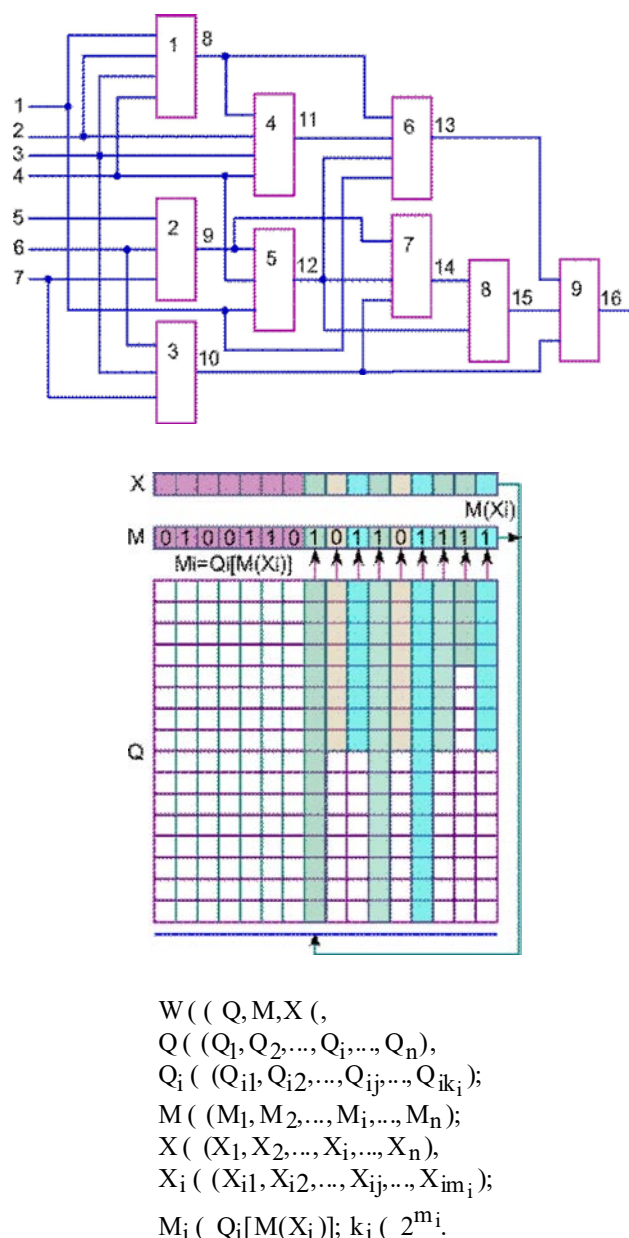


Рис. 1. Схема, кубитные структуры данных и модель квантового процессора

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 многovýchодовая, 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) Инициализация 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 X_i . Считывание соответствующего бита из кубит-покрытия Q_i 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 элемен-

тов 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 Q_i , функциональность которого задается Q-вектором. Все примитивы схемы должны быть упорядочены по принципу: очередной элемент анализируется, если все предшественники для него были обработаны.

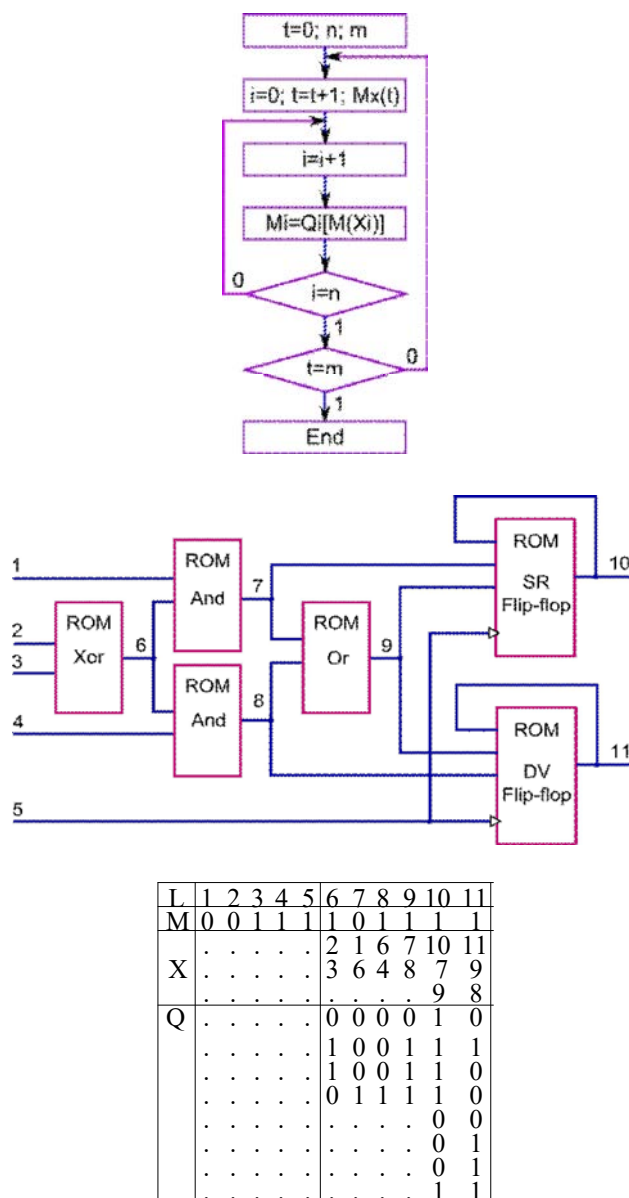


Рис. 2. Алгоритм моделирования и пример цифровой схемы с триггерами

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

довательной обработки всех Q-векторов схемной структуры формируют состояния линий M-вектора для приведенного выше примера ячейки (6 – 11). Первоначальные состояния неопределенностей на псевдоходах 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: $\text{card}(Q) \cdot 2^q$. 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 sparse-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 cifrovyyh 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., Mishchenko 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.



ОЦІНКА ГЛИБИНИ ТРІЩИНИ ЗА ЇЇ СТЕРЕОЗОБРАЖЕННЯМ НА ОСНОВІ ЛАМБЕРТІВСЬКОЇ МОДЕЛІ ВІДБИТТЯ

ГРАБОВСЬКА Н.Р., РУСИН Б.П., ІВАНЮК В.Г.

Розглядається задача тривимірної реконструкції поверхні за двома двовимірними зображеннями з метою застосування результатів її розв'язку при аналізі зображень матеріалів з тріщинами. Пропонується новий метод визначення глибини тріщини на основі аналізу двох двовимірних зображень на базі ламбертівської моделі відбиття світла. Результати роботи реалізованого алгоритму демонструються на прикладі тестового зображення.

1. Вступ

Один із методів неруйнівного контролю елементів газопроводів [1–4] пов'язаний з дослідженням металографічних зображень, на яких зафіксовано стан поверхні елементів окремих його ділянок [5–9]. Як правило, в результаті обстеження газопроводу одержуємо великі масиви зображень з тріщинами. В цьому випадку адаптація та застосування сучасних методів тривимірної реконструкції зображень до конкретних задач металографії дають можливість отримати більше інформації про об'єкти досліджуваної сцени, зокрема про тривимірну їх структуру, а також оцінити глибину тріщини за її двовимірними зображеннями, що дуже важливо для прогнозування тріщиностійкості елементів газопроводів [3]. В даній статті розглядається проблема оцінки довжини тріщини (максимальної глибини тріщини в тривимірному просторі) за її двовимірними зображеннями.

Одним з методів отримання тривимірної форми предмету на основі аналізу його зображень є класична стереорекопструкція [10]. Ця 3D реконструкція реалізується відносно нескладною установкою, та має задовільну швидкість реконструкції, що дозволяє використовувати її для напівавтоматичного обстеження поверхні конструкцій, зокрема газопроводів. Проте така реконструкція в деяких випадках може виявитись ускладненою, оскільки при практичному використанні даний метод тривимірної реконструкції має ряд обмежень, які впливають на точність отримання кінцевого результату. В першу чергу обмеження методу викликане присутністю на поверхні дефекту компонентів, які мають дзеркальне відбиття. Присутність дзеркального відбиття на стереозображеннях порушує погодження зображень, а отже, блокує тривимірну реконструкцію. Для роботи в таких умовах

запропоновано модернізацію класичної стереорекопструкції [11].

Ще один очікуваний збій тривимірної реконструкції за стереозображенням пов'язаний з виникненням ситуації, коли на одному з зображень стереопари присутня значна зона загороджених пікселів. Для роботи в таких умовах доцільно використати комплексний метод 3D реконструкції поверхні. В цьому методі за межами зони загороджених пікселів тривимірна реконструкція виконується як класичне відновлення за стереозображенням, а в межах зони загороджених пікселів вона виконується альтернативним методом. Для спрощення технічної реалізації доцільно застосувати такий метод 3D реконструкції, який усуває дзеркальні компоненти [11]. Зокрема йдеться про використання стереосвітлення при відеозйомці зображень.

Мета дослідження – розробити метод та алгоритм неруйнівного контролю стану поверхні, ураженої тріщинами, і зокрема тривимірно реконструювати тріщину та оцінити її глибину за результатами аналізу пари цифрових зображень її поверхні.

2. 3D реконструкція дифузного об'єкта за парою зображень

Розглянемо використання стереосвітлення, яке запропоновано в роботі [11] у альтернативному методі тривимірної реконструкції. Нехай під час відеозйомки дислокація камери фіксована та спочатку застосовано джерело світла $L_0 = (L_{x0}, L_{y0}, L_{z0})$, а потім $L_1 = (L_{x1}, L_{y1}, L_{z1})$. З таким змінним освітленням дифузного об'єкта відеозйомкою отримується два зображення [12]:

$$I_{\lambda j} = I_a + I_{p\lambda} k_d (L_{xj} N_x + L_{yj} N_y + L_{zj} N_z), \quad (1)$$

де $j = 0, 1$, I_a – інтенсивність розсіяного світла; $I_{p\lambda}$ – інтенсивність джерела освітлення; k_d – дифузний коефіцієнт, який визначає рівень дифузного відбиття досліджуваної точки поверхні; $N = (N_x, N_y, N_z)$ – одиничний вектор нормалі до поверхні $F(x, y, z) = 0$ у досліджуваній точці $M = (x, y, z)$:

$$N = \left\{ \frac{-p}{\sqrt{p^2 + q^2 + 1}}, \frac{-q}{\sqrt{p^2 + q^2 + 1}}, \frac{1}{\sqrt{p^2 + q^2 + 1}} \right\},$$

тут $p = \frac{\partial z}{\partial x}$, $q = \frac{\partial z}{\partial y}$ – нахил поверхні в околі точки.

Оскільки інтенсивність джерела освітлення $I_{p\lambda}$ є стала величина, то рівняння (1) є функціями чотирьох невідомих p , q , k_d та I_a .

Щоб усунути залежність від параметра I_a , визначимо його експериментально, затінюючи зразок з дефектом. Затінення формується за допомогою прямокутної

ка, просторове положення якого над зразком, а отже, і положення тіні, визначає система обробки. Використовуючи базове зображення $I_{\lambda 0}$ зі штучним затіненням, можна визначити інтенсивність фону I_a і звести систему (1) до трьох невідомих.

Щоб спростити систему (1), застосуємо джерело світла з такими параметрами, що $L_0 = (0, 0, 1)$.

Для вектора L_1 скористаємось описом [13]

$$L_1 = \left(\frac{-P}{\sqrt{P^2 + Q^2 + 1}}, \frac{-Q}{\sqrt{P^2 + Q^2 + 1}}, \frac{1}{\sqrt{P^2 + Q^2 + 1}} \right),$$

де $P = -\text{ctg}\theta$, тут θ – кут напрямку світла в площині XOZ , $Q = -\text{ctg}\varphi$; φ – кут напрямку світла в площині YOZ . Нехай $\theta = \frac{\pi}{3}$, $\varphi = \frac{\pi}{3}$. В цьому випадку

$$L_1 = (L_{x1}, L_{y1}, L_{z1}) = (0, 45, 0, 45, 0, 77).$$

Врахувавши одержані вектори L_0, L_1 в системі рівнянь (1), алгебраїчними перетвореннями трансформуємо цю систему у таку форму:

$$p = -q - b, \quad (2)$$

$$q^2 + bq + c = 0, \quad (3)$$

$$\text{де } b = \frac{1}{L_{x1}} \left[\frac{I_{\lambda 1} - I_a}{I_{\lambda 0} - I_a} - L_{z1} \right], \quad c = \frac{b^2 + 1}{2} - \frac{t^2}{2(I_{\lambda 0} - I_a)^2},$$

тут $t = I_{p\lambda} k_d$ – зважений дифузний коефіцієнт. Для його визначення використаємо точку поверхні, в якій має місце $q(x_0, y_0) = p(x_0, y_0) = 0$. До таких точок належать точки екстремумів і площини. Використовуючи таку точку та її властивість у виразі (1), отримуємо $t = I_{\lambda 0}(x_0, y_0) - I_a$.

За одержаними виразами (2), (3) можна реконструювати похідні p, q , що програмно реалізуються засобами МАТЛАБ. Як досліджуваний об'єкт реконструкції по зображеннях поверхневу тріщину. В процесі реконструкції доцільно сфокусувати увагу на параметрах, які є важливі для прогнозу тріщиностійкості.

3. Аналітична модель тріщини

Розв'язок поставленої задачі пропонуємо почати з запровадження такої аналітичної моделі тріщини

$$z(x, y) = \begin{cases} -Z_{\max} + \begin{cases} -P, & (-x_s + a) \leq x \leq a; \\ P, & (x_s + a) \geq x > a; \end{cases} \\ 0, & (x_s + a) < x, (-x_s + a) > x, \end{cases} \quad (4)$$

де $Z_{\max}$ – довжина тріщини, яка представляє собою максимальну відстань від краю до дна тріщини; $(-x_s + a)$, $(x_s + a)$ – крайні точки тріщини, $a = \eta + b$ – зміщення тріщини; $P = kx + k\eta y + kb$ – площина, яка

визначається похідними $p = k$, $q = k\eta$. Видно, що у розкритті це тріщина з V-подібним профілем. Зауважимо, що в точках, де аналітична модель (4) є непридатною до визначення похідної p або q , невизначеність буде знята при накладенні умов дискретизації по координатах x та y .

Щоб з'ясувати параметричну залежність параметрів тріщин при прогнозуванні тріщиностійкості, розглянемо один із варіантів моделі (4), коли $a=0$. Це вертикальна тріщина, яка є незмінною на деякому відрізку. $y \in [y_s, y_e]$, Нехай вертикальна тріщина розміщена на поверхні досліджуваної пластини, яку розтягнуто у випробувальній машині горизонтальним навантаженням σ . В цьому випадку поле напружень визначається коефіцієнтом інтенсивності напружень [3]

$$K_\sigma = 1,12\sigma\sqrt{\pi Z_{\max}}.$$

При досягненні K_σ критичного значення (константа матеріалу) здійсниться руйнування. За рахунок неточності 3D реконструкції виникає відносна похибка визначення коефіцієнта інтенсивності напружень

$$\delta K_\sigma = \frac{\delta Z_V}{2}. \quad (5)$$

З виразу (5) видно, що точність прогнозу тріщиностійкості визначається відносною похибкою розрахунку довжини тріщини

$$\delta Z_V = \frac{\Delta Z_{\max}}{Z_{\max}}, \quad (6)$$

де $\Delta Z_{\max}$ – абсолютна похибка реконструкції довжини $Z_{\max}$.

4. Комп'ютерне моделювання зображення тріщини

Перехід до дискретизаційних координат $\{i, k\}$ і обмежений діапазон значень поверхні z_{ik} дозволяють:

- штучно створити модель тріщини z_{ik} ;
- на основі масиву z_{ik} визначити масиви похідних p_{ik}, q_{ik} .

Виконання попередніх умов є підґрунтям до дискретного запису зображень $I_{\lambda 0} = I_{\lambda 0}(p_{ik}, q_{ik})$, $I_{\lambda 1} = I_{\lambda 1}(p_{ik}, q_{ik})$. Зауважимо, що на стадії комп'ютерного моделювання нехтуємо значенням інтенсивності фону I_a , а також додатково приймаємо, що дифузний коефіцієнт k_d є незмінним для змодельованого зразка з тріщиною z_{ik} . Крім того, не враховуватимемо вплив операцій квантування. На додаток зауважимо, що вплив точності встановлення напрямків світла L_0, L_1 в зображеннях (1) на реконструкцію на даному етапі не враховано.

5. Реконструкція висоти поверхні

Визначимо оцінки похідних p і q на основі інформації про зображення $I_{\lambda,0}, I_{\lambda,1}$ та користуючись (2), (3). Шляхом інтегрування виконаємо остаточну 3D реконструкцію глибини тріщини.

Перед початком комп'ютерної реконструкції висоти поверхні в системі обробки отримано оцінку похідних вектора нормалі поверхні у вигляді масивів $\underline{p}_{ik}, \underline{q}_{ik}$, $\forall i = \overline{1, I}; \forall k = \overline{1, K}$. Зауважимо, що реконструкція похідних отримана з абсолютними похибками

$$\begin{aligned}\Delta p_{ik} &= \underline{p}_{ik} - p_{ik}, \\ \Delta q_{ik} &= \underline{q}_{ik} - q_{ik}.\end{aligned}\quad (7)$$

Якщо прийняти за опорну точку початок координат, реконструйована глибина тріщини набуде значення

$$z_{ik} = z_{lk} + \Delta x \sum_{j=2}^i p_{jk}, \quad (8)$$

$$\text{де } z_{lk} = \Delta y \sum_{m=2}^k q_{lm}.$$

Таким чином, запропоновано метод реконструкції глибин зразка з тріщиною шляхом накопичення (8), який можна реалізувати програмно. Розглянемо оптимізаційні заходи покращення такої реконструкції.

6. Оцінка якості тривимірної реконструкції тріщини

Однією з очікуваних причин неякісної реконструкції металографічного зображення тріщини, яку потрібно враховувати, є завади, що вносить приймач зображення. Вони виникають через вплив неточності встановлення просторових параметрів положення джерела світла. Але на данному етапі досліджень приймемо, що процедура формування інтенсивності зображення тріщини (1) є ідеальна і не вносить спотворення. Оцінка глибини в значній мірі залежить від інтенсивності фону та дифузного коефіцієнта відбиття поверхні. Але на данному етапі досліджень приймемо, що процедура визначення фону та дифузного коефіцієнта відбиття поверхні є ідеальна і також не вносить спотворення.

Ще однією очікуваною причиною неякісної реконструкції металографічного зображення тріщини є завади методу реконструкції.

Визначимо аналітично вплив завад методу на якість реконструкції глибини тріщини за парою зображень. Для цього необхідно акцентувати увагу на якість реконструкції довжини тріщини $z_{\max}$ (4).

6.1. Оцінка точності реконструкції глибини тріщини. Уточнення моделі тріщини

Користуючись виразом (8), оцінку глибини тріщини z_{ik} представимо у такій формі:

$$z_{ik} = z_{lk} + \Delta z_{ik}, \quad (9)$$

де

$$\Delta z_{ik} = \Delta z_{lk} + \Delta x \sum_{n=2}^i \Delta p_{nk} \quad (10)$$

– абсолютна похибка реконструкції глибини. Перший доданок у виразі (10) приймає значення

$$\Delta z_{lk} = \Delta y \sum_{m=2}^k \Delta q_{lm}. \quad (11)$$

Нехай у поверхні з тріщиною в точках (l, m) , $\forall m = \overline{2, K}$ є площина.

Для мінімізації похибок першого доданку (11) необхідно скоректувати реконструйовану вертикальну похідну $\underline{q}_{lk}$ систематичною похибкою Δq_{sis} :

$$\underline{q}_{lk,s} = \underline{q}_{lk} - \Delta q_{sis}, \quad (12)$$

що змінить перший доданок так:

$$\Delta z_{lk,s} = \Delta y \sum_{m=2}^k (\Delta q_{lm} - \Delta q_{sis}).$$

Щоб розрахувати систематичну похибку Δq_{sis} , покладемо $\Delta z_{lk,s} = 0$, з чого одержуємо

$$\Delta q_{sis} = \frac{1}{k-1} \sum_{m=2}^k \Delta q_{lm}. \quad (13)$$

Такий вигляд має оцінка систематичної похибки, розрахована по точках площини реального металографічного зображення, де присутні флуктуації поверхні. У ідеалізованому випадку площина не має флуктуацій поверхні, тому $\Delta q_{lm} = \Delta q_p$. З цього випливає, що $\Delta q_{sis} = \Delta q_p$.

Продовжимо розгляд похибки (10), припустивши, що корекцію проведено і перший доданок у (10) дорівнює нулю.

Розглянемо другий доданок у накопиченні (10), зробивши такі припущення:

- вертикальна координата k фіксована;
- в точках (i, k) , $\forall i = \overline{2, i_1}$ маємо площину поверхні з тріщиною;
- в точках (i, k) , $\forall i = \overline{i_{l+1}, i_r}$ існує поверхня тріщини.

Виберемо точку (i, k) , в якій існує поверхня тріщини. В цьому випадку другий доданок (10) набуває форми

$$\Delta z_{ik} = \Delta z_{ik}' + \Delta z_{ik}'', \quad (14)$$

де $\Delta z_{ik}' = \Delta x \sum_{j=2}^{i_1} \Delta p_{jk}$ – абсолютна похибка реконструкції глибини в точках площини;

$$\Delta z_{ik}'' = \Delta x \sum_{j=i_l+1}^i \Delta p_{jk}$$

– абсолютна похибка реконструкції глибини тріщини в точці (i, k) .

Для мінімізації похибок першого доданку у виразі (14) необхідно скоректувати реконструйовану горизонтальну похідну $\underline{p}_{jk}$ систематичною похибкою Δp_{sis} :

$$\underline{p}_{ik,s} = \underline{p}_{ik} - \Delta p_{sis}, \quad (15)$$

що змінить перший доданок так:

$$\Delta z_{ik,s}' = \Delta x \sum_{j=2}^{i_l} (\Delta p_{jk} - \Delta p_{sis}).$$

Щоб розрахувати систематичну похибку Δp_{sis} , покладемо аналогічно $\Delta z_{ik,s}' = 0$, з чого випливає

$$\Delta p_{sis} = \frac{1}{i_l - 1} \sum_{j=2}^{i_l} \Delta p_{jk}.$$

Як було сказано раніше, такий вигляд має оцінка систематичної похибки, розрахована по точках площини реального металографічного зображення, де присутні флуктуації поверхні. У ідеалізованому випадку площина не має флуктуацій поверхні, тому $\Delta p_{jk} = \Delta p_p$, $\forall j = \overline{2, i_l}$ з цього випливає, що $\Delta p_{sis} = \Delta p_p$.

Продовжимо розгляд похибки (14), припустивши, що корекцію (15) проведено і перший доданок у (14) дорівнює нулю.

Нехай в точці (i_v, k) маємо вістря тріщини, в якому $z_{i_v,k} = -z_{\max}$. В цьому випадку (14) набуває форми

$$\Delta z_{\max} = \Delta x \sum_{j=i_l+1}^{i_v} (\Delta p_{jk} - \Delta p_{sis}) \quad (16)$$

– абсолютна похибка розрахунку довжини тріщини.

Нехай проведено реконструкцію поверхні тріщини (4). В цьому випадку

$$\underline{p}_{ik} = -P, \quad \Delta p_{ik} = \Delta p, \quad \forall i = \overline{i_{l+1}, i_r}.$$

З врахуванням сказаного вираз (16) спрощується:

$$\Delta z_{\max} = \Delta x (\Delta p - \Delta p_p) (i_v - i_l - 1), \quad (17)$$

а також спрощується вираз (8):

$$z_{\max} = -(p - \Delta p_p) \Delta x (i_v - i_l - 1). \quad (18)$$

Підставимо (17) та (18) у вираз (6), тоді відносна похибка розрахунку довжини тріщини (6) рівна

$$\delta z_v = -\frac{\Delta p - \Delta p_p}{p - \Delta p_p}. \quad (19)$$

Оскільки похибка Δp_p визначається на площині, яка є незмінним елементом у будь-якої тріщини (4), то основну увагу в аналізі похибки δz_v слід зосередити на її залежності від параметрів $\Delta p, p$, які є специфічними для кожної тріщини (4). Використовуючи опис тріщини (4) та (19), можна ввести такий клас тріщин. У класі тріщин (4) кожна тріщина має похідну p , що належить діапазону $[0, p_s]$ з заданою точністю $\delta z_{v, \max} \geq \delta z_v$. Якщо $p \gg \Delta p_p$, то

$$\delta z_v \approx -\frac{\Delta p}{p} + \frac{\Delta p_p}{p}. \quad (20)$$

Як бачимо, δz_v для кожної тріщини, яка належить класу тріщин (4), визначається відносною похибкою реконструкції горизонтальної похідної. Отриманий результат дозволяє здійснити наступне. Щоб визначити оцінку якості тривимірної реконструкції, замість класу тріщин (4) досліджувати одну модель тріщини, в якій забезпечили наявність горизонтальних похідних, що належать діапазону $[0, p_s]$ з заданою точністю $\delta z_{v, \max} \geq \delta z_v$. Одним з можливих потенційних варіантів такої моделі тріщини є модель тріщини, яка у розкритті описується виразом

$$z = k(x + y)^2 - z_{\max} \leq 0,$$

де $k = \text{const}$. Видно, що у розкритті це тріщина з U-подібним профілем. Програмно реалізувати таку модель тріщини, розміщену у площині, можна згідно з виразом

$$Z = \frac{z - |z|}{2}. \quad (21)$$

6.2. Оцінка якості тривимірної реконструкції тріщини

Роглянемо тривимірну реконструкцію тріщини та оцінку її якості.

Спочатку програмно за квадратним рівнянням (3) реконструюємо вертикальну похідну у вигляді двох масивів коренів $\underline{q}_{1,ik}$, $\underline{q}_{2,ik}$, а потім на основі цієї інформації за виразом (2) реконструюємо горизонтальну похідну у вигляді двох масивів $\underline{p}_{1,ik}$, $\underline{p}_{2,ik}$.

Для позначення параметрів: вертикальної похідної q_1, q_2 , горизонтальної похідної p_1, p_2 та глибини z моделі тріщини (21) застосуємо $u \in \{p_n, q_n, z\}$, $n=1,2$. Для оцінки якості тривимірної реконструкції для параметра u знайдемо абсолютну похибку

$$\Delta u_{ik} = \underline{u}_{ik} - u_{ik} \quad (22)$$

та відносну похибку

$$\delta u_{ik} = \frac{\Delta u_{ik}}{u_{ik}}. \quad (23)$$

Зауважимо, що при програмній реалізації, щоб уникнути виникнення полюсів, коли $u_{ik} = 0$, знаменник в (23) представлено $u_{ik} + 0,00001$. Зауважимо, що в точках, в яких похибка $|(\delta u_{ik})| > 0,25$, отримання достовірних результатів реконструкції не розглядається. Тому площина $\delta u_{ik} = \pm 0,25$ викидається з розгляду.

Для визначення оптимального масиву вертикальної та горизонтальної похідної оберемо точки (i,k) , в яких має місце розкриття тріщини.

На підставі порівняння відносних похибок $q_{1,ik} \cdot p_{1,ik}$, $q_{2,ik} \cdot p_{2,ik}$ за статистичними критеріями або за абсолютною величиною вибирається пара похідних $q_{1,ik}$, $p_{1,ik}$ або $q_{2,ik}$, $p_{2,ik}$, яка використовується для наступного проведення реконструкції.

На початку тривимірної реконструкції глибини тріщини проведемо мінімізацію абсолютної похибки реконструкції глибини Δz_{ik} (10). Для цього застосуємо дві корекції.

Корекція (12) здійснює мінімізацію першого доданку в виразі (10).

Корекція (15) здійснює мінімізацію другого доданку в (10).

Після застосування цих корекцій отримуємо скоректовані похідні $q_{ik,s}$, $p_{ik,s}$. На їх основі алгоритмом тривимірної реконструкції глибини тріщини (8) виконуємо відновлення z_{ik} .

Завершує оцінку якості тривимірної реконструкції реалізація визначення абсолютної та відносної похибки реконструкції глибини тріщини (22), (23) та визначення відносної похибки реконструкції довжини тріщини (6), (23).

7. Приклад програмного застосування

Комп'ютерна модель тріщини Z (рис. 1) використовується для визначення похідних p_{ik} , q_{ik} та комп'ютерного генерування штучних зображень $I_\lambda(L_m) = I_\lambda(L_m, p, q)$, де $m=0,1$. Для розрахунку відносних сигналів $I_\lambda(L_m)$ додатково прийнято умови

$$I_a = 0, \quad I_{p\lambda k_d} = 250. \quad (24)$$

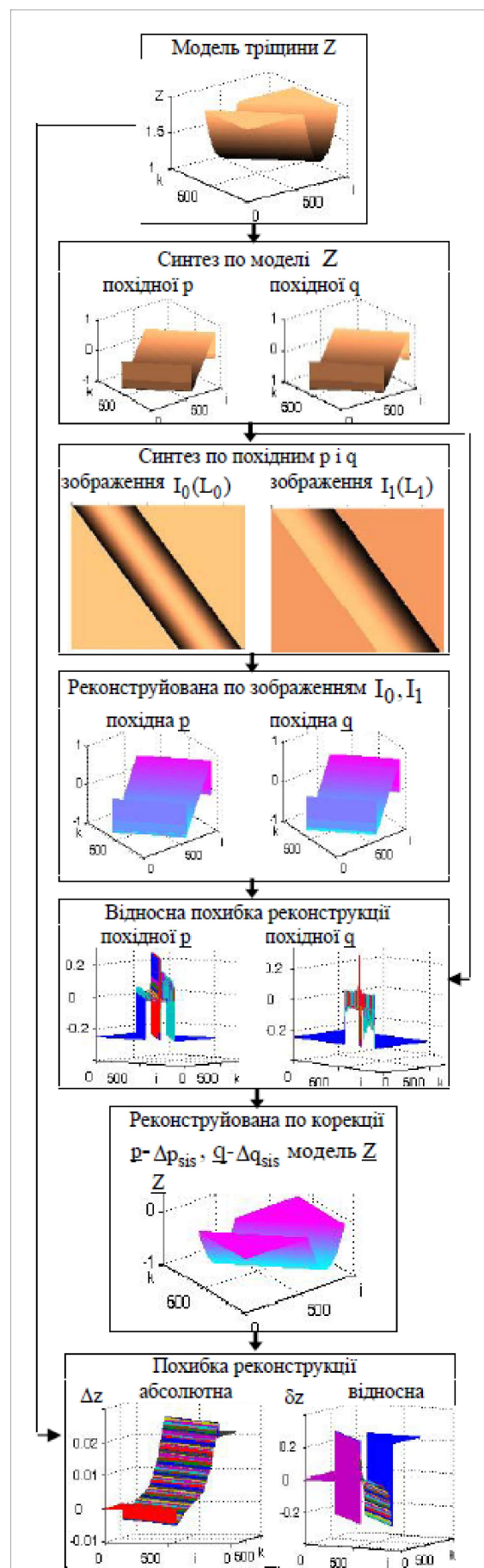


Рис. 1. Інформаційна технологія тривимірної реконструкції за стереозображенням

Ці синтезовані об'єкти та їх проміжні продукти представлені на рис. 1 у спектрі жовто-коричневих відтінків.

Процедура реконструкції глибини поверхні пластини з тріщиною на базі стереозображення містить такі основні операції:

1. На основі $I_\lambda(L_0)$, $I_\lambda(L_1)$ за виразом (3), де використано (24), визначимо два кореня вертикальної похідної $q_{1,ik}$, $q_{2,ik}$.

2. На основі $q_{1,ik}$ ($q_{2,ik}$), за виразом (2), визначимо горизонтальну похідну $p_{1,ik}$ ($p_{2,ik}$).

Реконструйовані похідні $q_{2,ik}$ і $p_{2,ik}$ представлені на рис. 1 у спектрі синіх та фіолетових відтінків.

3. За виразом (23) визначимо відносну похибку реконструкції вертикальної похідної $\delta q_{n,ik}$. Результати роботи програми по визначенню відносної похибки реконструкції вертикальної похідної $\delta q_{2,ik}$ для всіх точок апертури подані на рис. 1, а для кращої візуалізації точок, які належать самій тріщині – на рис. 2, де наведено розподіл похибки у перерізі розкриття тріщини. Як бачимо, у розподілі переважають від'ємні значення відносної похибки, які сконцентровані у правій частині тріщини. Ця особливість є аргументом на користь вибору реконструкції глибини за методом (8).

На основі спільного аналізу розподілів відносної похибки реконструкції вертикальної похідної $\delta q_{2,j}$ (j – вертикальна координата, а фіксована горизонтальна координата для спрощення індексації відсутня) та вертикальної похідної q_j (див. рис. 2) встановлено, що у лівій частині тріщини q належить діапазону $[-0,83; -0,005]$ з заданою точністю 0,25, а у правій частині тріщини q належить діапазону $[0,09; 0,83]$ з такою ж точністю.

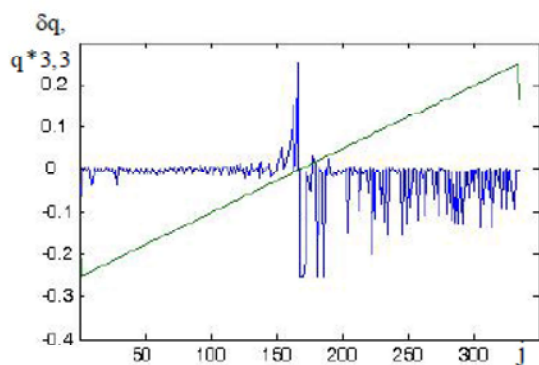


Рис. 2. Розподіл відносної похибки реконструкції вертикальної похідної $\delta q = \delta q_{2,j}$ (синій колір) та вертикальної похідної $q = q_j$ (зелений колір) в перерізі тріщини

4. За виразом (23) визначимо відносну похибку реконструкції горизонтальної похідної $\delta p_{n,ik}$, де $n=1,2$. Результати роботи програми по визначенню відносної похибки реконструкції горизонтальної похідної $\delta p_{2,ik}$ для всіх точок апертури подані на рис. 1. Аналогічно, як і у випадку, описаному вище, для кращої візуалізації точок, які належать самій тріщині, на рис. 3 наведений розподіл похибки горизонтальної похідної у перерізі розкриття тріщини.

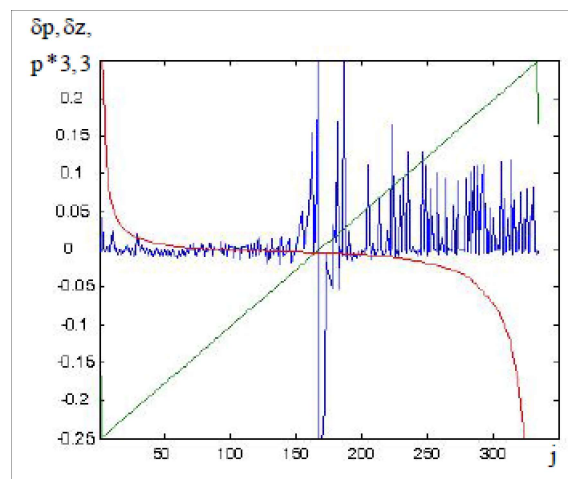


Рис. 3. Розподіл відносної похибки реконструкції горизонтальної похідної $\delta p = \delta p_{2,j}$ (синій колір), горизонтальної похідної $p = p_j$ (зелений колір), та відносної похибки реконструкції глибини $\delta z = \delta z_j$ (червоний колір) в перерізі тріщини

Видно, що переважають додатні значення відносної похибки, які сконцентровані у правій частині тріщини. Ця особливість є аргументом на користь вибору реконструкції глибини (8) і зокрема довжини тріщини.

На основі спільного аналізу розподілів відносної похибки реконструкції горизонтальної похідної $\delta p_{2,j}$ (j – горизонтальна координата, а фіксована вертикальна координата для спрощення індексації відсутня) та горизонтальної похідної p_j (див. рис. 3) встановлено, що у лівій частині тріщини p належить діапазону $[-0,83; -0,005]$ з заданою точністю 0,25, а у правій частині тріщини p належить діапазону $[0,09; 0,83]$ з такою ж точністю.

5. З огляду розподілів відносної похибки, наведених на рис. 2 та 3, видно, що вони мають однаковий діапазон координат. Ця властивість дозволила провести кількісне порівняння

$$a_j = |\delta q_{2,j} - \delta p_{1,j}|, \quad b_j = |\delta q_{1,j} - \delta p_{2,j}|.$$

За результатами роботи програми було встановлено, що різниці $a_j \leq 10^{-12}$, $b_j \leq 10^{-12}$. Таким чином, на підставі встановленого збігання масивів відносних похибок у наступному етапі реконструкції можна використовувати будь-яку пару похідних: $q_{1,ik} \cdot p_{1,ik}$ або $q_{2,ik} \cdot p_{2,ik}$.

Продовжимо реконструкцію з похідними $q_{2,ik} \cdot p_{2,ik}$.

6. Інтерактивно на площині виберемо систематичну похибку $\Delta q_{\text{sis}} = q_{10,10}$ і за виразом (12) розрахуємо корекцію вертикальної похідної $q_{1m,s}$.

7. Інтерактивно на площині виберемо систематичну похибку $\Delta p_{\text{sis}} = p_{10,10}$ і за виразом (15) розрахуємо корекцію горизонтальної похідної $p_{ik,s}$.

8. Зважаючи на кращий діапазон реконструкції похідних та менші флуктуації відносних похибок у лівій частині тріщини (див. рис. 2 і 3) доцільно наступну реконструкцію глибини тріщини провести, використовуючи опорну точку – початок координат.

На основі одномірного масиву похідних $q_{1m,s}$, $\forall m = \overline{2, K}$ (п. 6) та двомірного масиву похідних $p_{ik,s}$ (п. 7), за накопиченнями (8), визначимо двомірний масив глибин z_{ik} (див. рис. 1).

9. Для кількісної оцінки якості реконструкції 3D характеристик тріщини застосуємо такі параметри: абсолютну і відносну похибку розрахунку глибини тріщини одержуємо відповідно за виразами (22) і (23).

Як видно з рис. 1, похибки визначення різних точок площини, розташовані зліва від тріщини, не відрізняються, і що важливо, мають внаслідок проведення корекції (п. 6, п. 7) нульове значення.

Абсолютна похибка зростає починаючи від від'ємних значень на лівому краї тріщини до додатних значень на правому краї, де спостерігається найбільше по абсолютній величині значення похибки. Найінтенсивніші зміни похибки спостерігаються біля країв тріщини. Вздовж тріщини розподіл абсолютної та відносної похибок практично незмінний. Така специфіка розподілу відносної похибки дозволяє продовжити його аналіз у перетині (див. рис. 3). На основі спільного аналізу розподілів відносної похибки реконструкції глибини тріщини δz_j та глибини z_j встановлено, що у лівій частині тріщини z належить діапазону реконструкції $[-0,011, -0,7]$, а у правій частині тріщини z належить вужчому діапазону $[-0,092, -0,7]$. В обох випадках за рахунок обмеження по точності $\delta z_T = 0,25$ формується верхня межа діапазону реконструкції.

Зауважимо, що для прогнозу тріщиностійкості з усього масиву відносних похибок найбільший інтерес представляють похибки визначення довжини тріщини, які відповідають нижній межі діапазону реконструкції $z_U = -z_{\text{max}} = -0,7$. Програмно отримане таке значення відносної похибки реконструкції довжини тріщини: $\delta z_U = -4,8 \cdot 10^{-3}$. Це дозволяє проводити прогноз тріщиностійкості з відносною похибкою $\delta K = 9,6 \cdot 10^{-3}$.

8. Висновки

Наукова новизна роботи полягає в тому, що вперше запропоновано новий метод та алгоритм тривимірної реконструкції за парою зображень, що базується на ламбертівській моделі відбиття світла. Цей алгоритм реалізований у вигляді віртуальної системи обробки інформації, придатної для штучного генерування зображень стереопари. Кожне зображення синтезовано з індивідуальним кутом освітлення. Перше зображення отримується з вертикальним розташуванням джерела світла, а друге – з кутом, який не локалізований в жодній з двох вертикальних ортогональних площин тривимірного простору. Ця інформація дозволяє описати тривимірну поверхню матеріалу у вигляді системи двох рівнянь, що дає можливість реконструювати похідні векторів нормалі.

Вперше для підвищення точності реконструкції похідні векторів нормалі коректуються систематичними похибками, які визначаються на площині тріщини.

Оцінка глибини тріщини знаходиться інтегральним накопиченням скоректованих похідних векторів нормалі тріщини, починаючи від одної з точок поверхні, яку приймають за опорну. За таким підходом, використовуючи пластину з тріщиною, оцінено її похибки реконструкції. Відносна похибка розрахункової частини алгоритму реконструкції глибини тріщини становить $\pm 0,5\%$.

Практична цінність роботи полягає в тому, що запропонована система дозволить по парі зображень отримувати тривимірну інформацію про матеріали, які досліджуються, в даному випадку – про тріщини. Наведено програмно розраховані похибки реконструкції, а також діапазони реконструкції похідних векторів нормалі і глибини з заданою точністю для двох типів тріщин. Описано теоретичні прийоми корекції систематичних похибок, які дозволяють зменшити вплив похибок реконструкції на визначення глибини тріщини. В перспективі запропонований метод реконструкції тріщин дозволить проводити прогноз тріщиностійкості з кращою точністю.

Література: 1. *Похмурський В.І., Хома М.С.* Корозійна втома металів та сплавів. Львів: СПОЛОМ, 2008. 304с. 2. *Wood, W. A.* Recent observations on fatigue fracture in metals, ASTM STP 237, 1958. P. 110-121. 3. *Броек Д.* Основы механики разрушения. М.: Высшая школа, 1980. 368с. 4. *Гаркунов Д.Н.* Триботехника (износ и безызносность). М.: Из-во МСХА, 2001. 616с. 5. *Myshkin N.K., Kong H., Gngoriev A.Ya., Yoon E.-S.* The use of color in wear debris analysis // Elsevier Wear. 2001. v.251. P.1218-1226. 6. *Похмурський А. Ю., Русин Б.П., Іванюк В.Г., Капшій О.В.* Метод оцінки глибини корозійного пітинга // Фізико-хімічна механіка матеріалів. 2010. Вип. №8. С. 617-623. 7. *Русин Б.П., Іванюк В.Г., Капшій О.В., Ануфрієва Н.П., Похмурський А.Ю.* Оцінка глибини пітинга за зображеннями поверхні матеріалу // Радіоелектроніка і інформатика. 2010. № 1. С. 83-91. 8. *Синявський А.Т., Русин Б.П.* Реалізація методу реконструкції мікроструктури поверхні за її стереозображенням з оптичних камер // Радіоелектроніка та інформатика.

2005. №2. С.112-118. **9.** Русин Б.П., Лисак Ю.В., Похмурський А.Ю., Варецький Я.Ю. Реконструкція та кількісний аналіз металевих поверхонь з пітингами на основі удосконаленого методу погодження стереозображень // Фізико-хімічна механіка матеріалів. 2011. Том 47. №2. С.126-133. **10.** Richard Szeliski. Computer Vision: Algorithms and Applications. Springer, New York, 2010. 655 p. **11.** Русин Б.П., Іванюк В.Г., Лисак Ю.В., Ануфрієва Н.П. Стереозйомка та погодження зображень, що базується на Phong моделі відбиття світла // Радіоелектроніка та інформатика. 2011. №2. С. 61–69. **12.** Lambert J. H. Photometria, sive de Mensura et gradibus luminis, colorum et umbrae / sumptibus viduae E. Klett, 1760. **13.** Грабовська Н.Р., Русин Б.П., Іванюк В.Г., Капшій О.В. Похибка тривимірної реконструкції поверхні тріщини за тріадою зображень // Радіоелектроніка та інформатика. 2015. №2. С. 58–63.

Надійшла до редколегії 04.12.2015

Рецензент: д-р техн. наук, проф. Лукін В.В.

Грабовська Наталія Романівна, аспірантка Фізико-механічного інституту ім. Г.В.Карпенка НАНУ. Наукові інтереси: обробка та розпізнавання зображень. Адреса: Україна, 79601, Львів, вул. Наукова, 5а. dep32@ipm.lviv.ua

Русин Богдан Павлович, д-р техн. наук, проф., зав. відділом “Методів і систем дистанційного зондування” Фізико-механічного інституту ім. Г.В.Карпенка НАНУ. Наукові

інтереси: обробка та розпізнавання зображень. Адреса: Україна, 79601, Львів, вул. Наукова, 5а, e-mail: dep32@ipm.lviv.ua

Іванюк Віталій Григорович, інженер відділу “Методів і систем дистанційного зондування” Фізико-механічного інституту ім. Г.В.Карпенка НАНУ. Наукові інтереси: обробка та розпізнавання зображень. Адреса: Україна, 79601, Львів, вул. Наукова, 5а, тел:2296-530. e-mail: vivan@imp.lviv.ua

Rusyn B.P., doctor of engineering sciences, professor, manager of department of “Methods and systems of the remote sensing” of Karpenko Physico-Mechanical Institute of NAS of Ukraine, Address: 79601, Ukraine, Lviv, street Scientific, 5a, telephone: 2296-530, e-mail: dep32@ipm.lviv.ua

Hrabovcska N.R., graduate student of Karpenko Physico-Mechanical Institute of NAS of Ukraine, Scientific interests: treatment and artificial perception. Address: 79601, Ukraine, Lviv, street Scientific, 5a, telephone: 2296-530, e-mail: dep32@ipm.lviv.ua

Ivanyuk V.H., engineer of department of “Methods and systems of the remote sensing” of Karpenko Physico-Mechanical Institute of NAS of Ukraine, . Scientific interests: treatment and artificial perception. Address: 79601, Ukraine, Lviv, street Scientific, 5a, telephone: 2296-530, e-mail: vivan@imp.lviv.ua

ФОРМАЛИЗОВАННОЕ ПРЕДСТАВЛЕНИЕ И АНАЛИЗ АГЕНТНО-ОРИЕНТИРОВАННЫХ ЗАДАЧ

ФИЛАТОВ В.А., УЗЛОВ Д.Ю.

Рассматривается класс мультиагентных систем управления информационными ресурсами. Приводится классификация типов задач, характерных для информационных систем. Предлагается спецификация агентно-ориентированного подхода. Обосновывается выбор математического аппарата на основе сетей Петри для моделирования и анализа рассмотренного класса задач. Исследуются варианты сетей Петри, их особенности при моделировании потоков агентно-ориентированных задач. Приводится пример решения агентно-ориентированной задачи.

Ключевые слова: мультиагентная система, база данных, сеть Петри, позиция, переход, маркер, поток задач, агентно-ориентированная задача, информационная система

Keywords: multi-agent system, database, Petri net, position, transition, marker, flow problems, agent-oriented tasks, information system

Введение

Рассматривается класс мультиагентных систем управления информационными ресурсами распределенных систем. Типичным представителем такого класса задач является планирование пути достижения нужной цели из некоторой фиксированной начальной ситуации. Результатом решения задачи должен быть план действий – частично упорядоченная совокупность действий. Таким планом является сценарий, в котором в качестве отношения между вершинами выступают отношения типа: «цель-подцель», «цель-действие», «действие-результат» и т. п. Любой путь в этом сценарии, ведущий от вершины, соответствующей текущей ситуации, в любую из целевых вершин, определяет план действий. Все задачи построения плана действий можно разбить на два типа, которым соответствуют различные модели: планирование в пространстве состояний и планирование в пространстве задач.

В первом случае считается заданным некоторое пространство ситуаций. Описание ситуаций включает состояние внешней среды и состояние информационной системы. Ситуации образуют некоторые обобщенные состояния, а действия или изменения во внешней среде приводят к изменению актуализированных в данный момент состояний. Среди обобщенных состояний выделяются начальные (обычно одно) и конечные (целевые) состояния.

Планирование по состояниям. Представление задач в пространстве состояний предполагает задание ряда описаний: состояний, множества операторов и их воздействий на переходы между состояниями, целевых состояний. Описания состояний могут представ-

лять собой строки символов, векторы, двумерные массивы, деревья, списки и т. п. Операторы переводят одно состояние в другое. Пространство состояний можно представить как граф, вершины которого помечены состояниями, а дуги – операторами.

Планирование по задачам. Метод планирования по состояниям можно рассматривать как частный случай метода планирования с помощью редукций, ибо каждое применение оператора в пространстве состояний означает сведение исходной задачи к двум более простым, из которых одна является элементарной. Поиск решения в пространстве задач заключается в последовательном сведении исходной задачи к все более простым до тех пор, пока не будут получены только элементарные задачи. Частично упорядоченная совокупность таких задач составит решение исходной задачи [1].

Целью проводимых исследований является разработка эффективных методов представления и анализа взаимосвязанных агентно-ориентированных задач на основе модифицированного аппарата сетей Петри.

Спецификация представления агентно-ориентированных задач

Определение агентно-ориентированной задачи: порядок выполнения каждой задачи определяется указанием множества состояний, которые могут быть наблюдаемы извне, и множества переходов между этими состояниями. Кроме того, могут быть определены те характеристики обрабатываемых объектов, которые могут влиять на требования к выполнению задач.

Требования координации агентно-ориентированных задач: такие требования обычно выражаются через межзадачные зависимости выполнения и зависимости потоков данных.

Требования к выполнению или требования корректности: требования к выполнению определяются для ограничения выполнения потока работ таким образом, чтобы удовлетворялись критерии корректности, зависящие от приложения. Они включают требования атомарности при сбоях (failure-atomicity), требования атомарности-выполнения (execution-atomicity) (включая правила видимости, указывающие, когда результаты зафиксированной задачи становятся видимыми для других параллельно выполняющихся потоков работ), а также требования к управлению синхронным выполнением потоков работ и требования восстановления.

Определение агентно-ориентированной задачи в потоке работ

Задача в потоке работ - это единица работы, которая может быть выполнена обрабатываемым объектом, таким как прикладная система или система управления базой данных (СУБД). Задача может быть определена независимо от обрабатываемого объекта, который может ее выполнить, или на основании возмож-

ностей и поведения этого объекта. Для управления потоком работ нет необходимости моделировать все аспекты задач. Рассмотрим пример транзакции, выполняемой СУБД. С точки зрения потока работ все подробности транзакции, описывающие ее последовательную обработку, не являются необходимыми.

Каждая задача выполняет некоторые операции над определенной системой (базой данных). Следовательно, задача является программой (транзакцией) и важно, чтобы она была «корректной». Однако, как и при обеспечении корректности традиционных транзакций, на уровне потока работ мы не моделируем внутренние операции задачи – мы имеем дело только с теми аспектами задачи, которые видимы извне.

Следовательно, структура задачи может быть определена заданием:

- множества состояний выполнения задачи;
- множества переходов между этими состояниями и условий, которые делают допустимыми эти переходы, (условия переходов могут быть использованы для указания межзадачных требований выполнения).

Основные свойства агентно-ориентированных задач

Абстрактной моделью задачи является машина (автомат) состояний, поведение которой может быть определено заданием для ее диаграммы смены состояний. В общем случае каждая задача (и соответствующий ей автомат) может иметь различную внутреннюю структуру для различных диаграмм смены состояний. Это в большой степени зависит от характеристик системы, в которой выполняется эта задача.

Некоторые из свойств обрабатываемых объектов, ответственных за выполнение задачи, таких как наличие или отсутствие интерфейса двухфазной фиксации, непосредственно влияют на структуру задачи и, таким образом, на определение потока работ. Переходы между различными состояниями задачи могут вызываться различными событиями планирования. Некоторые из этих переходов контролируются планировщиком, ответственным за соблюдение межзадачных зависимостей. Например, задача может быть запущена на выполнение, что вызывает переход из состояния «Начало» в состояние «Выполнение».

Другие переходы контролируются локальной системой, ответственной за выполнение задачи. Например, выполняющаяся задача может быть прервана системой (скажем, для того чтобы избежать тупика), что вызывает переход из состояния «Выполнение» в состояние «Прервана».

Одно или более состояний задачи могут быть определены как состояния завершения. Когда задача достигает такого состояния, никакие переходы больше не разрешены. И, наконец, задача может обладать различными свойствами изолированности. Например, результаты еще незавершенной задачи могут стать

видимыми для других параллельно выполняющихся задач, или эти результаты могут быть скрыты до тех пор, пока задача не будет зафиксирована. Эти и другие свойства влияют на механизмы асинхронного выполнения и восстановления, что может быть использовано планировщиком.

Частичный вывод задачи может быть доступным для других параллельно выполняющихся задач, или задача может запросить получение информации из других задач. Предполагается, что задачи потока работ могут взаимодействовать посредством переменных, локальных относительно потока работ. Эти переменные могут содержать параметры программ задачи. Различные начальные параметры могут приводить к различному выполнению задач. Поток данных между подтранзакциями определяется присваиванием значений их входных и выходных переменных. Выполнение подтранзакции влияет на состояние базы данных и выходную переменную подтранзакции.

В любой момент времени состояние потока работ может быть определено как набор состояний входящих в поток задач и значений всех переменных. Выполнение потока работ начинается в начальном состоянии, которое задает параметры инициализации. Различные начальные состояния потока работ могут приводить к различным его выполнениям.

Некоторые характеристики системы, выполняющей задачу, могут влиять на свойства задачи, не затрагивая ее структуру. Например, система, выполняющая задачу, может гарантировать аналогичный порядок выполнения и сериализации, что позволит планировщику потока работ влиять на локальный порядок сериализации задач путем управления порядком их фиксации (старт, окончание). Подобным образом система может гарантировать идемпотентность, обеспечивая безопасное повторение задачи, если не получено положительное подтверждение или истекло время.

Задачи моделируются их состояниями вместе со значимыми событиями, соответствующими переходам между состояниями – старт, фиксация, откат, которые могут быть форсированы, отвергнуты или задержаны. Межзадачные зависимости, такие как зависимости порядка $E_1 < E_2$ и зависимости существования $E_1 \rightarrow E_2$ между значимыми событиями задач, формально определяются с использованием логики деревьев вычисления (Computation Tree Logic – CTL) и обладают соответствующими автоматами зависимостей, которые могут быть построены автоматически. Эти зависимости могут поддерживаться путем проверки нужных автоматов зависимостей [2].

Требования атомарности по сбоям в потоке работ

Используя понимание семантики потока работ и мультисистемных ограничений согласованности, проектировщик потока работ определяет требования *атомар-*

ности по сбоем для потока. Традиционное понятие атомарности отказов состоит в том, что неудача при выполнении любой задачи приводит к неудачному выполнению всего потока. Тем не менее, во многих случаях поток работ может выдержать неудачное завершение одной из задач, выполнив, например, функционально эквивалентную задачу на другой установке. Система, выполняющая поток работ (планировщик потока работ), должна гарантировать, что любое выполнение будет завершено в состоянии, удовлетворяющем требованиям атомарности по сбоем, сформулированным разработчиком. Мы будем называть такие состояния *приемлемыми состояниями завершения* потока работ. Все остальные состояния выполнения входят во множество *неприемлемых состояний завершения*, в которых атомарность по сбоем может быть нарушена.

Приемлемое состояние завершения может быть зафиксированным или прерванным. *Зафиксированное приемлемое состояние завершения* – это состояние выполнения, при котором достигнуты цели потока работ. В противоположность этому *прерванное приемлемое состояние завершения* – это правильное состояние завершения, при котором поток работ претерпел неудачу в достижении своих целей. Если достигнуто прерванное приемлемое состояние завершения, все нежелательные эффекты частичного выполнения потока работ должны быть ликвидированы в соответствии с требованиями атомарности по сбоем.

В общем случае задача может быть зафиксирована и должна освободить свои ресурсы, прежде чем поток работ достигнет состояния завершения. Однако если поток работ позднее будет прерван, атомарность по сбоем может потребовать откатки результатов уже зафиксированных задач (т.е. зафиксированных подтранзакций) посредством выполнения *компенсирующих задач*. Понятия приемлемых состояний завершения и зависимостей планирования могут быть использованы для выражения семантики компенсации без применения специальных конструкций, требуемых в других моделях транзакций. Семантика компенсации требует, чтобы компенсирующие транзакции, в конечном счете, завершили свое выполнение успешно, возможно, после нескольких попыток выполнения. В описываемой здесь модели это свойство компенсирующих транзакций может быть определено соответствующим указанием их предусловий планирования.

Аналогично требованиям атомарности по сбоем проектировщик может указать требования *атомарности выполнения* для потока работ. Традиционная модель транзакций требует, чтобы весь поток работ состоял из целиком выполняющихся единиц. Тем самым чередуемое выполнение потоков работ должно было бы иметь тот же результат, что и последовательное выполнение в некотором порядке. Ослабление свойства атомарности выполнения транзакций в централизованных базах данных обсуждается в работах. Тран-

закция разбивается на атомарные шаги и чередование с другими параллельно выполняющимися транзакциями допустимо только между этими шагами. В контексте потока работ задачи обычно являются естественными атомарными элементами, поскольку выполняются различными обрабатывающими объектами.

Растущий интерес к исследованиям по управлению потоками работ и возрастающая популярность продуктов автоматизации потоков работ привели к созданию ряда языков спецификации потоков работ. В общем случае можно разделить технологии спецификации потоков работ на две большие категории:

- графические средства спецификации потоков работ;
- языки спецификации потоков работ.

Неудивительно, что графические средства реализуются в основном в коммерческих системах, ориентированных на конечного пользователя, в то время как исследовательские прототипы потоков работ используют более формальные и мощные языки спецификации.

Практический метод спецификации потоков работ (графическое средство или язык) должен поддерживать:

- описание различных типов задач и устройств обработки, которые выполняют эти задачи;
- спецификации потока управления в потоке работ, т.е. зависимости планирования для задач;
- спецификации потока данных между задачами и, возможно, различные преобразования форматов данных.

Проектировщик потока работ может задать дополнительные свойства потока работ, например, критерии корректности выполнения задач.

Важной функцией средства спецификации потока работ является поддержка автоматического (или полуавтоматического) анализа корректности спецификаций. В общем случае автоматическая верификация спецификаций представляет собой такую же трудную проблему, что и верификация традиционных программ. Тем не менее, к некоторым аспектам координации задач можно относиться, как к протоколам обмена сообщениями, и они таким же образом могут быть проанализированы.

Методы анализа взаимосвязанных агентно-ориентированных задач на основе сетей высокого уровня

Проектирование и эксплуатация автоматизированных систем поддержки принятия решений, функционирующих в условиях жесткого ограничения на ресурсы, вызывает трудности, связанные с необходимостью обеспечения заданных функциональных и эксплуатационных свойств системы. Существующие средства диагностики и тестирования, как правило, обеспечи-

вают лишь контроль состояния системы и, в меньшей степени, контроль выполнения заданий конкретными приложениями. Функционирование системы на основе серийных программно-аппаратных средств в значительной мере определяется качеством приложений. Положение усложняется распределенным характером обработки данных и значительным влиянием субъективного фактора на этапе проектирования.

Другим известным формализмом системного, ситуационного анализа, который позволяет генерировать и изучать разнообразные сценарии работы управляющих систем, моделировать различные (в том числе конфликтные и нежелательные) ситуации, изучать и оценивать последствия решений на поведение управляемой системы, являются сети Петри. Они позволяют моделировать параллельную и распределенную работу алгоритма. В частности, многие параллельные алгоритмы управления и процессы обработки информации естественно моделируются граф-схемами. Граф-схема алгоритма представляет собой ориентированный граф: $G = \langle V, E \rangle$, где V – множество вершин, E – множество дуг.

Множество вершин состоит из вершин следующих трех видов:

Операторные вершины соответствуют действиям. Среди них выделяются две обязательные вершины начала и конца алгоритма.

Вершины альтернативного выбора соответствуют решению конфликтов в зависимости от некоторых условий. Такие вершины имеют одну входную и две выходных дуги, помеченные словами «да» и «нет» соответственно. Если условие выполнено, то процесс продолжается по дуге «да», в противном случае – по дуге «нет».

Вспомогательные вершины, которые в свою очередь подразделяются на три группы:

- вершины параллельного ветвления имеют одну входную и несколько выходных дуг и обозначают переход к параллельному выполнению нескольких независимых действий;
- вершины параллельного слияния имеют несколько входных и одну выходную дугу и означают переход к следующему действию при условии, что все предыдущие выполнены;
- вершины условного слияния также имеют несколько входных и одну выходную дугу и означают переход к следующему действию при условии выполнения одного (любого) из предыдущих.

Важным достоинством граф-схем является то, что граф-схема алгоритма может быть формально преобразована в сеть Петри специального вида – сеть Петри со свободным выбором. При этом обоснование корректности граф-схемы алгоритма сводится к проверке корректности и безопасности соответствующей сети Петри. В сетях Петри со свободным выбором

каждая позиция (условие), обуславливающая срабатывание более чем одного перехода, является единственной обуславливающей эти переходы позицией. Структурные особенности сетей Петри со свободным выбором позволили разработать эффективные алгоритмы их семантического анализа непосредственно по структуре сети.

Однако моделирование алгоритмов управления граф-схемами алгоритмов (сетями Петри со свободным выбором) имеет ряд существенных недостатков. В граф-схеме структура алгоритма задана изначально и не допускает, в частности, динамического распараллеливания задачи. Также граф-схема алгоритма не обладает модульной структурой, что делает моделирование и анализ больших задач весьма затруднительными. Для устранения этого ограничения можно использовать расширение стандартного формализма сетей Петри – вложенные сети Петри.

Методы анализа сложных взаимосвязанных процессов на основе вложенных сетей Петри

Во вложенных сетях Петри фишки, помечающие позиции, рассматриваются как объекты, имеющие самостоятельное поведение, которое в свою очередь описывается также некоторыми сетями Петри. Название «вложенные сети» указывает на то, что элементы сетей в них сами являются сетями, подобно тому, как в системе вложенных множеств элементами некоторого множества могут быть множества. Вложенные сети Петри являются удобным и мощным средством для моделирования и анализа иерархических мульти-агентных распределенных систем. Они обладают естественным механизмом модульности. Модульные сети Петри можно рассматривать как специальный случай вложенных сетей [3].

По сравнению с другими расширениями формализма сетей Петри за счет понятия и конструкции объекта вложенные сети Петри сохраняют такие важные свойства стандартных сетей Петри, как простота и выразительность модели и разрешимость некоторых важных для верификации свойств.

Вложенная сеть Петри состоит из системной (корневой) сети и множества элементарных сетей, представляющих фишки системной сети. В простейшем случае двухуровневой вложенной сети элементарные сети являются обыкновенными сетями Петри, в которых фишки, как обычно, изображаются черными точками, не имеют собственной структуры и не различимы между собой.

Поведение вложенной сети Петри включает четыре типа шагов.

Шаг переноса – это срабатывание перехода системной сети в соответствии с обычными правилами для сетей Петри высокого уровня, при этом элементарные сети рассматриваются как фишки, не имеющие собственной структуры. Шаг переноса может перемес-

тить, породить или убрать объекты, но не может изменить их внутреннее состояние.

Элементно-автономный шаг меняет только внутреннее состояние (маркировку) элементной сети, не меняя ее местонахождения в системной сети. Этот шаг выполняется также в соответствии с обычными правилами срабатывания перехода для сети Петри.

Шаг горизонтальной синхронизации есть одновременное срабатывание двух переходов в двух элементных сетях, находящихся в одной позиции системной сети. При этом переходы, которые должны срабатывать синхронно, помечаются взаимно дополнительными метками из некоторого специального множества меток для горизонтальной синхронизации.

Шаг вертикальной синхронизации используется для синхронизации перехода в системной сети с некоторыми переходами элементных сетей. Переходы, которые должны срабатывать синхронно, помечаются метками из некоторого специального множества меток для вертикальной синхронизации. При этом метка перехода в системной сети и метка соответствующего перехода в элементной сети должны быть взаимно дополнительными. Вертикальная синхронизация означает одновременное срабатывание перехода системной сети и переходов (помеченных дополнительной меткой) в задействованных в этом срабатывании элементных сетях. В том случае, когда решаются задачи управления распределенными мультиагентными системами, сложность алгоритмов управления существенно возрастает, что повышает значение моделирования различных сценариев поведения системы при различных стратегиях управления. При этом вложенные сети Петри сохраняют важные для возможности их семантического анализа свойства (являются хорошо структурированными системами переходов). В частности, доказано, что свойство останова (завершаемости алгоритма) и свойство поддержания некоторого заданного состояния управления (control-state maintainability) разрешимы для вложенных сетей Петри [4].

Методы анализа сложных взаимосвязанных процессов на основе предикатных сетей Петри

Пусть задана структура инструментальных средств принятия решений в виде некоторой совокупности последовательно-параллельно взаимодействующих задач $\{z_\gamma\}, \gamma \in H$. В процессе их выполнения некоторое подмножество задач:

$$\{z_{\gamma_1}\} \subset \{z_\alpha\}, \gamma_1 \in H_1, H_1 \subset H \quad (1)$$

может быть выполнено с привлечением дополнительно подчиненных им задач:

$$\{z'_{\gamma_1}\}, \gamma_1 \in H_1, H_1 \subset H. \quad (2)$$

Расширение подмножества задач $\{z_{\gamma_1}\} \subset \{z_\alpha\}$ на $\{z'_{\gamma_1}\}, \gamma_1 \in H_1, H_1 \subset H$ может носить как постоян-

ный, так и временный характер, что приводит к сложной, многоуровневой иерархии подзадач. Это ведет к дополнительным затратам вычислительных ресурсов.

Задача проводимых исследований может быть сформулирована следующим образом: разработать эффективные процедуры динамического анализа и синтеза иерархии взаимосвязанных подзадач (1) и (2). Методы решения должны быть ориентированы на современные информационные технологии.

Перспективным направлением комплексного решения поставленных задач является моделирование взаимодействующих процессов моделями на основе расширений предикатных сетей Петри и оценочных Е-сетей. Достоинства сетей основаны на возможностях учета множества условий, определяемых предметной областью, а также наличием механизмов управления пространством состояний и структурой сети.

Рассмотрим возможности управления пространством состояний и структурой сетей в условиях иерархии взаимодействующих задач. С этой целью введем понятие интерпретированных метапозиций

$\{p_\alpha^{(IM)}\}, \alpha \in A$ и интерпретированных метапереходов $\{p_\beta^{(IM)}\}, \beta \in B$ сети S .

Построение иерархии сетей взаимосвязанных подзадач с переменной структурой

Рассмотрим особенности построения сетей и управление динамикой моделирования процессов обработки данных с использованием модифицированных предикатных сетей и модифицированных Е-сетей.

Модифицированные предикатные сети. Учитывая известные сложности при интерпретации и моделировании процессов обработки данных предикатными сетями, признано целесообразным применение следующей модификации сетей:

$$SPR = \langle P, T, F, A_\tau, C, \{V_s\}, K, M_0 \rangle, \quad (3)$$

где P – множество позиций; T – множество переходов; F – функция инцидентностей позиций и переходов; C – функция цвета маркера; A_τ – параметр времени, отнесенный ко всем компонентам сети: P, T, F, M_0 ; V_s – условие выполнения переходов $t_k \in T, k \in K$, отнесенных к компонентам сети: $V_{p_k}^I$ – условие выполнения $t_k \in T, k \in K$, отнесенное к его входным позициям; $V_{p_k}^O$ – условие выполнения $t_k \in T, k \in K$, отнесенное к его выходным позициям; V_{t_k} – условие выполнения $t_k \in T, k \in K$, отнесенное непосредственно к этому переходу; $V_{m_{p_l}}$ – условие выполнения $t_k \in T, k \in K$, отнесенное к маркированию ему инцидентных позиций, $l \in L$; V_F – условие выполнения $t_k \in T, k \in K$, отнесенное к его входным и выходным дугам инцидентных позиций; K – ем-

кость маркеров в позициях с учетом C ; M_0 – вектор начальной маркировки.

Условие выполнения перехода V_s включает также такие свойства, как надежность, сложность, стоимость, степень достоверности конкретного события.

Анализ возможных решений показал, что для сети (3), в задачах моделирования процессов подчиненных задач на основе сетей S' удобно применение интерпретированной метапозиции

$$p_{\alpha}^{(IM)} \in \{p_{\alpha}^{(IM)}\}, \alpha \in A.$$

Это определяется тем, что собственно позиции в (3) интерпретируют условия выполнения действий моделируемых событий, а также определяют пространство состояний модели.

Модифицированные E-сети. Существующие ограничения E-сетей не позволяют эффективно использовать их в практических приложениях. В связи с этим предлагается следующее развитие E-сетей:

$$E^{(m)} = \langle P, T, I(T), O(T), Q, \Theta, M_0 \rangle, \quad (4)$$

где P – конечное множество позиций; T – конечное множество переходов; $I(T)$, $O(T)$ – соответственно связи входных и выходных позиций переходов T ;

Q – конечное множество вычислительных процедур, которые управляют выполнением переходов и исключают конфликты на переходах сети;

Θ – конечное множество условий выполнения компонент сети, пространства состояний сети и процедур перехода, которые управляют сменой цвета (атрибутов) маркера, определяют приоритеты входных и выходных позиций перехода, функцию времени A_s выполнения переходов; M_0 – вектор начальной маркировки E-сети [5].

Пример

Ресурс типа A_1 обеспечен информационной поддержкой и хранится в файлах баз данных, например $B_{11}, B_{12}, \dots, B_{1n}, n \in N$, где N – количество баз данных. Условие поиска для рассматриваемого фрагмента системы принятия решений формулируется следующим образом: определить заданное количество ресурса типа $A_1 = A_1^*$ на множестве $\{B_{11}, B_{12}, \dots, B_{1n}\}, n \in N$. Поиск решения осуществляется двумя типами действий – на первом шаге ПОИСК по базе данных B_1 , если условие не выполняется, осуществляется ОБЪЕДИНЕНИЕ баз данных $B_1 + B_2$ и поиск повторяется. Процедура поиска и объединения баз данных может осуществляться в терминах структурированного языка запросов SQL с использованием опции SELECT и INSERT:

Select sum([A1]), from b1.dbf;

Insert into b1...Select b2....From b2.

Представим фрагмент рассмотренной выше задачи в виде *модифицированной предикатной сети Петри S* (рис. 1). Множество позиций $\{p_0, p_1\}$ интерпретируют соответственно входное и выходное условие выполнения действия, что представлено на сети переходом t_0 , множество позиций $\{p_1, p_2\}$ интерпретируют соответственно входное и выходное условие выполнения действия t_1 . Вектор начальной маркировки $M_0 = (1, 0, 0)$ определяет начальное пространство состояний сети.

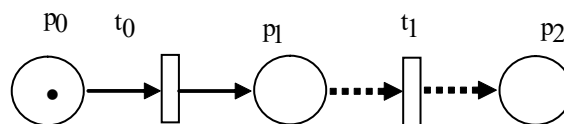


Рис. 1. Сеть Петри S

Описание основных ограничений, представленных на рис. 1: $V_{p_k}^I$ – входное условие выполнения перехода

$t_1 \in T, k \in K$; $V_{p_k}^O$ – выходное условие выполнения

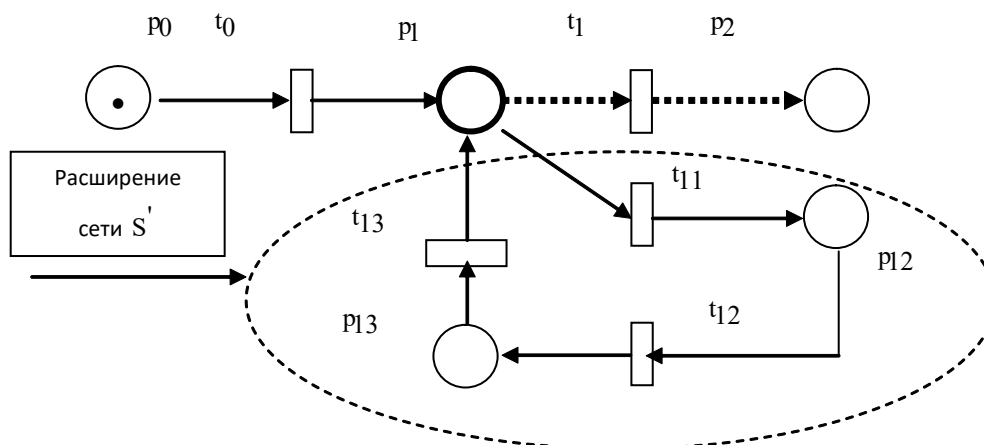


Рис. 2. Сеть Петри S с расширением S'

перехода t_1 . Если входное условие V_{p_k} выполнения перехода t_1 не удовлетворено: $V_{p_k} \neq V_{t_k}$, то для данного перехода $t_1 \in T, k \in K$ генерируется подчиненная сеть S' (рис.2), где позиция p_1 является метапозицией. Вектор начальной маркировки $M_0 = (1, 0, 0, 0, 0)$ определяет начальное пространство состояний сети.

Маркирование позиции p_{13} и выполнение перехода t_{13} маркирует метапозицию p_1 , что запускает выполнение сети S . Если искомое решение невыполнимо средствами $S \cup S'$, то осуществляем иерархию задач на основе поиска решений из множества $\{B_{11}, B_{12}, \dots, B_{1n}\}, n \in N$ путем объединения баз данных и расширения сети S' .

Выводы

В результате анализа методов управления информационными ресурсами в корпоративных системах рассмотрен подход к представлению агентно-ориентированных задач на основе анализа состояния внешней среды и состояния информационной системы. Исследованы два основных метода представления агентно-ориентированных задач: планирование по состояниям и планирование по задачам. Рассмотрены особенности управления пространством состояний и структурой модифицированных предикатных сетей в условиях иерархии взаимодействующих задач. Полученные результаты могут быть распространены на некоторую иерархию подчиненных сетей с учетом их особенностей и необходимости генерации метапозиций и метапереходов. Предложенный подход позволяет снизить временные и вычислительные ресурсы за счет подключения подчиненных задач, определения устойчивых связей и исключения из рассмотрения нерациональных и неудовлетворительных решений.

Литература: 1. Пономаренко Л.А., Цыбульник Е.Е., Филатов В.А. Агентные технологии в задачах поиска информации и принятия решений // УСМ: Управляющие системы и машины. 2003. № 1. С. 36-41. 2. Кучеренко Е.И., Филатов В.А. Модели принятия решений в задачах анализа сложных систем на основе сетей высокого уровня // Системы обработки информации. Харьков: ХВУ. 2004. Вып. 5. С. 139-148. 3. Мурата Т. Сети Петри: Свойства, анализ, приложения // ТИИЭР. 1989. Т. 77. №4. С. 41-85. 4. Girault C., Volk R. Petri nets for systems engineering – A guide to modelling, verification and applications, Springer-Verlag,

2003. 5. Филатов В.А., Кучеренко В.Е. О моделях обработки данных на основе иерархии сетей высокого уровня // Радиоэлектроника, информатика, управление. Научный журнал, Запорожье: ЗНТУ. 2004. №1(11). С. 95-100.

Транслитерированный список литературы: 1. Ponomarenko L.A., Cybul'nik E.E., Filatov V.A. Agentnye tehnologii v zadachah poiska informacii i prinjatija reshenij / / USiM: Upravljajushhie sistemy i mashyny – № 1, 2003. – S. 36-41. 2. Kucherenko E.I., Filatov V.A. Modeli prinjatija reshenij v zadachah analiza slozhnyh sistem na osnove setej vysokogo urovnja. // Sistemi obrobki informacii. – Har'kov: HVU. 2004. Vip.5. S.139-148. 3. Murata T. Seti Petri: Svojstva, analiz, prilozhenija // TIIeR. 1989. T. 77. №4. P. 41-85. 4. Girault C., Volk R. Petri nets for systems engineering – A guide to modelling, verification and applications, Springer-Verlag, 2003. 5. Filatov V.A., Kucherenko V.E. O modeljah obrabotki dannyh na osnove ierarhii setej vysokogo urovnja. // Radiojelektronika, informatika, upravlenie. Nauchnyj zhurnal, Zaporozh'e: ZNTU. 2004. №1(11). S. 95-100.

Поступила в редколлегия 14.12.2015

Рецензент: д-р техн. наук, проф. Рубан И.В.

Филатов Валентин Александрович, д-р техн. наук, профессор, заведующий кафедрой искусственного интеллекта ХНУРЭ. Научные интересы: базы данных и знаний, агентные технологии, мультиагентные системы, извлечение знаний из данных. Увлечения и хобби: велосипед, авто, мото. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел: +3 8(057) 7021337, e-mail: valentin.filatov@nure.ua

Узлов Дмитрий Юрьевич, канд.техн. наук, полковник полиции, начальник Управления информационного обеспечения ГУНП в Харьковской области. Научные интересы: интеллектуальные информационные системы, извлечение данных из знаний, интеллектуальный анализ данных, системы поддержки принятия решений. Увлечения и хобби: путешествия, фантастика. Адрес: Украина, 61000, Харьков, ул. Совнаркомовская, 5, тел: +3 8(057)7059775.

Valentin Filatov, Doctor of Sciences, Professor, Head of the Department of Artificial Intelligence in the Harkiv National University of Radioelectronics. Research interests: databases and knowledge, agent technology multi-agent systems, data mining. Interests and hobbies: bike, car, moto. Address: Harkiv, 61166, Lenin Ave, 14, Phone: +3 8 (057) 7021337, e-mail: valentin.filatov@nure.ua

Uzlov Dmitry, PhD, the colonel of police, chief the Information Department of National Policy in Harkiv region. Research interests: intelligent information systems, data mining, and decisions support systems. Interests and hobbies: traveling, fantasy. Address: Kharkiv, str. Sovnarkomovskaya, 5. Phone: +3 8(057) 7059775.

МОДЕЛЬ РАЗНОРОДНЫХ РАСПРЕДЕЛЕННЫХ ЗНАНИЙ

ПЕТРОВА Л.Г.

Рассматривается проблема формирования распределенного представления знаний, охватывающего как общие закономерности предметной области, так и индивидуальные знания о ее фрагментах. Предлагается модель распределенного представления знаний на основе структуры Крипке. Интеграция разнородных знаний в модели осуществляется на основе учета состояний предметной области, а также допустимых отношений между этими состояниями. Состояния могут быть выражены единым образом через значения свойств объектов предметной области. Модель служит основой для построения многоуровневых архитектур представления распределенных знаний.

Введение

Распределенное представление знаний в общем случае охватывает различные фрагменты гетерогенного по форме знания. Общий процесс вывода в данном случае представляет собой комбинацию вывода на различных элементах знания. Указанные подпроцессы вывода могут выполняться автономно для различных подсистем системы ИИ в целом [1].

Построение интегрального распределенного представления знаний направлено на объединение в единую систему элементов частичного знания о предметной области с тем, чтобы организовать общий логический вывод при решении интеллектуальных задач. Концепция интеграции распределенного знания позволяет строить динамически наращиваемые представления предметной области. Иными словами, различные подсистемы системы искусственного интеллекта должны обмениваться фрагментами знания при решении своих задач. Такой подход позволяет строить многоуровневые архитектуры из фрагментов распределенного знания.

Впервые идея распределенного представления концепций была предложена в работе [2]. Hinton G.E. предложил масштабировать знания путем использования выявленных для текущей концепции закономерностей при адаптации сходных концепций.

Вопросы построения распределенного представления путем интеграции отдельных элементов разнородного знания на основе логических формализмов рассматривались в работах [3-6]. Построение единой формальной системы для распределенного знания в этих работах базируется на предположении о семантической связи между истинными значениями для различных формул, соответствующих различным фрагментам общего знания о предметной области. На основе данного предположения формально описывается связь между формулами из различных фрагментов предметной области. Однако определение простых взаимосвязей между такими формулами в общем случае

не позволяет построить интегральное распределенное представление данных, поскольку эти формулы могут оперировать с различными объектами предметной области. Поэтому при формировании интегрального распределенного представления необходимо определить и, возможно, привести к единой форме контекст предметной области. Изложенное определяет актуальность темы данной работы.

Постановка задачи

Решение рассмотренной проблематики построения распределенного представления знаний требует учета не только взаимосвязи между зависимостями для различных фрагментов предметной области, но и учета свойств и состояния объектов домена.

Задача данного исследования заключается в разработке модели распределенных знаний, объединяющей как общие закономерности предметной области, так и индивидуальные знания о ее фрагментах, а также учитывающей ее текущее состояние и возможные изменения этого состояния.

Распределенное представление знаний

Формирование распределенного представления знаний, как было показано выше, требует учета контекста. Под контекстом мы будем понимать знания о состоянии и взаимосвязях объектов рассматриваемого домена. Указанные состояния и взаимосвязи могут изменяться с течением времени. Поэтому в описании знаний необходимо учитывать возможности наращивания знаний в процессе эволюции объектов. Сформулируем базовые требования к распределенному представлению знаний, учитывающие возможности их изменения и наращивания:

- непрерывное расширение знаний об объектах предметной области;
- учет временных параметров объектов предметной области;
- масштабируемость знаний;
- формализация взаимодействия объектов предметной области;
- многоуровневое представление семантики.

В соответствии с первым требованием представление знаний должно обеспечивать возможность добавлять новые атрибуты объектов, пополнять множество значений атрибутов, а также задавать новые зависимости между существующими и вновь добавленными атрибутами на единой формальной основе.

Согласно второму требованию необходимо формализовать закономерности, отражающие изменение состояния объектов во времени с учетом возможной передачи данных между ними. Иными словами, в данном случае необходимо учитывать изменение текущих значений параметров объектов.

Реализация третьего требования направлена на перенос полученных знаний в рамках предметной области либо же для сходных предметных областей. Напри-

мер, полученные в результате обучения знания о взаимосвязях между элементами базы данных продаж могут быть использованы для анализа логов продаж, т.е. для получения закономерностей процесса продаж.

Выполнение четвертого требования реализуется посредством построения многоуровневых архитектур, в которых зависимости более низкого уровня составляют набор входных данных для зависимостей более высокого уровня. Это позволяет на каждом уровне добиваться обобщения знаний о взаимодействии объектов. Более того, при интеграции разнородных знаний такой подход позволяет объединять формальные зависимости различных уровней обобщения. В результате распределенное знание отражает взаимодействие агентов (активных объектов) предметной области на различных уровнях детализации.

Пятое требование дополняет требование взаимодействия, поскольку выделение уровней детализации в большинстве случаев должно отражать многоуровневое представление семантики. В основе такой иерархии лежат наиболее простые концепции, знания более высокого уровня определяются в терминах их связей с концепциями нижележащих уровней. Рассматриваемый подход позволяет системе ИИ вывести более сложные знания из простых концепций, без формальной спецификации этих знаний человеком.

Отметим, что базовая иерархия для построения многоуровневого представления семантики имеет вид: данные-> информация-> знания-> метазнания. В этой иерархии информация представляет собой структурированные данные, знания – зависимости между информационными структурами, а метазнания – это знания об использовании знаний.

С учетом приведенных выше требований разнородное распределенное знание D будем рассматривать как совокупное знание всех агентов A_i , действующих в предметной области. При описании контекста на объектной основе, как было показано выше, в качестве агентов будем рассматривать активные сущности (объекты), которые изменяют не только свое состояние, но и состояние других объектов домена. Агенты воспринимают данные о домене (один или несколько последовательных актов восприятия) и влияют на этот домен. Иными словами, агенты реализуют некоторую интеллектуальную функцию на основе своего внутреннего представления знаний. Примером такой интеллектуальной функции является распознавание изображений. Неоднородность описания знаний состоит в том, что каждый агент может использовать свою формальную модель знаний. Все эти модели необходимо интегрировать в распределенном представлении знаний.

Таким образом, распределенное знание объединяет на единой логической основе все фрагменты знания, описанные с использованием различных формальных моделей. Поэтому оно включает в себя общее знание

о предметной области. Будем считать, что каждый фрагмент знания принадлежит отдельному агенту. Обозначим принадлежность формулы φ к распределенному знанию как $D\varphi$. Распределенное знание обобщает и, возможно, дублирует знание всех агентов:

$$D\varphi \equiv \exists i: A_i \varphi. \quad (1)$$

Формализацию распределенного знания, отражающего состояние объектов предметной области, удобно представить на основе структуры Крипке в виде: $M = (S, \{R_i\}, I)$, где S – множество состояний домена, $\{R_i\}$ – множество допустимых двоичных отношений между состояниями для различных фрагментов предметной области: $R_i \subseteq S \times S$, I – функция интерпретации, которая задает множество атомарных высказываний, истинных в состоянии $s \in S$.

Каждый элемент R_i задает допустимые отношения для i -агента. Например, знания i -агента допускают изменения состояния предметной области из текущего s в последующее w в том случае, если задано условие: $\exists R_i(s, w)$.

Истинность формулы φ в состоянии s в модели Крипке задается отношением $(M, s) \models \varphi$. Истинность формулы φ в состоянии s означает, что данное состояние интерпретируется в модели M т.е. $s \in I(\varphi)$.

Условие $\exists R_i(s, w)$ позволяет определить истинность формулы β в состоянии w при условии истинности формулы φ в состоянии s для i -агента следующим образом:

$$(M, s) \models \varphi \text{ iff } \exists w: (M, w) \models \beta \mid \exists R_i(s, w). \quad (2)$$

Согласно (2) переход в состояние w отражает выполнение формулы. Необходимым условием истинности формулы β является истинность формулы φ . Поэтому данное выражение можно интерпретировать как последовательность логического вывода $\varphi \rightarrow \beta$. Иными словами, для i -агента истинность правила β в последующем состоянии полностью зависит от истинности правила (либо действия) φ в текущем состоянии. Тогда знания одного агента о будущем определяются его знаниями о текущем состоянии и о действии в текущем состоянии. Обобщив выражение (2) для всех агентов, получим:

$$(M, s) \models R\varphi \text{ iff } \exists w: (M, w) \models \beta \mid R_i(s, w) = \text{true} \forall R_i \in R. \quad (3)$$

Это означает, что для генерализации знаний агентов необходимо объединить их допустимые отношения для каждой пары состояний. Иными словами, объединив отношения для одной пары состояний, мы получа-

ем лишь фрагмент общей последовательности вывода. Чтобы выделить последовательности вывода, приписанные всем агентам, необходимо определить транзитивное замыкание на отношениях R_i , общих для всех агентов.

Определим отношение Ω как транзитивное замыкание отношений R_i :

$$(s_{j*}, s_{j**}) \in \Omega \equiv (\exists R_i (s_{j*}, s_{j*+1}) \wedge \dots \wedge \exists R_i (s_{j*-1}, s_{j**}) \quad \forall i, j, i = \overline{1, I}, j = \overline{1, J-1}, R_i \in (\bigcup_i R_i \setminus \bigcap_i R_i)). \quad (4)$$

В соответствии с (4) мы определяем отношение между произвольными состояниями s_{j*}, s_{j**} на базе общих для всех агентов отношений R_i между парами последовательных состояний (s_j, s_{j+1}) . Это означает, что на основе локальных зависимостей между ближайшими состояниями мы формально задаем зависимости между произвольными состояниями домена, что позволяет выполнить требования 1, 2 и 4. Действительно, временные параметры предметной области отражаются через последовательность состояний. Объединение отношений R_i для различных состояний одного объекта позволяет получить новые зависимости, поскольку состояние предметной области выражается через текущие значения свойств объекта. Аналогично, R_i объединение отношений для различных агентов позволяет выстроить отношения между разными объектами предметной области.

Теперь общее знание, применимое для всех фрагментов предметной области, определяется на основе отношения Ω :

$$(M, s) \models \Omega \phi \quad \text{iff} \quad \exists w: (M, w) \models \beta \mid (s, w) \in \Omega. \quad (5)$$

Выражение (5) определяет общее (повторяющееся у всех агентов) знание, что позволяет интегрировать разнородные знания агентов в единое распределенное представление. Индивидуальные знания агентов задаются через отношение A :

$$(M, s) \models A \phi \quad \text{iff} \quad \exists w: (M, w) \models \beta \mid (s, w) \in A, A = \bigcap_i R_i. \quad (6)$$

Тогда распределенное знание задается на основе структуры Крипке через оператор D :

$$(M, s) \models D \phi \quad \text{iff} \quad (M, s) \models \Omega \phi \vee (M, s) \models A \phi. \quad (7)$$

Выводы

Предложена общая модель распределенного представления знаний на основе структуры Крипке, которая объединяет общее и индивидуальное знание агентов о предметной области.

Интеграция знаний в модели осуществляется на основе учета состояний предметной области, а также допустимых отношений между этими состояниями. Состояния могут быть выражены единым образом через значения свойств объектов предметной области.

Модель служит основой для построения многоуровневых архитектур представления распределенных знаний. В рамках таких архитектур индивидуальное знание может быть использовано для построения текущего уровня представления. Общее знание может использоваться двояко. Во-первых, для объединения уровней путем применения отношений, связывающих принадлежащие к разным уровням состояния знаний. Во-вторых, для генерализации знания текущего уровня путем параллельного использования отношений для одних и тех же пар состояний текущего уровня.

Литература: 1. *F. van Harmelen, V. Lifschitz, Porter B.* Handbook of Knowledge Representation. Edited by Foundations of artificial intelligence. 2008. 1004 p. 2. *Hinton, G.E.* Learning distributed representations of concepts. In Proc. 8th Conf. Cog. Sc. Society, 1986. P. 1–12. 3. *Luca Vigan, J. Rasga, Amílcar Sernadas, Cristina Sernadas, Luca Viganm.* Labelled deduction over algebras of truth-values. In Frontiers of Combining Systems 4 // Proceedings of FroCoS'2002. LNCS 2309, Springer-Verlag, 2002. 4. *David Basin, Sebn Matthews, Luca Viganm.* Labelled Quantified Modal Logics. In Proceedings of KI'97, LNAI 1303, Springer-Verlag, 1997. 5. *David Basin, Sebn Matthews, Luca Viganm.* Modal Logics K, T, K4, S4: Labelled Proof Systems and New Complexity Results. The Bulletin of Symbolic Logic 1999. 5(1), PP. 91-93. 6. *Russo A.* Generalising Propositional Modal Logic Using Labelled Deductive Systems. Frontiers of Combining Systems: First International Workshop, Munich, March 1996. Vol.3 of the series Applied Logic Series. P. 57-73. 7. *Kripke S.A.* Semantical considerations on modal logic. Acta Philosophica Fennica, 1963. № 16. P. 83-94. 8. *Clarke E.M.* Model Checking. The MIT Press, 1999. 330 p.

Поступила в редакцию 28.11.2015

Рецензент: д-р техн. наук, проф. Кучеренко Е. И.

Петрова Лариса Григорьевна, доцент кафедры информационно-коммуникационных технологий Сумского областного института последипломного педагогического образования. Научные интересы: методы машинного обучения. Адрес: Украина, 40007, Сумы, ул. Римского-Корсакова, 5, тел. (0542) 33-40-67.

ИСПОЛЬЗОВАНИЕ МЕТОДА СЕКВЕНЦИАЛЬНОГО АНАЛИЗА ДЛЯ МОДЕЛИРОВАНИЯ ОБЪЕКТА С ФРАКТАЛЬНОЙ СТРУКТУРОЙ

КРАВЕЦ Н.С.

Показывается возможность использования алгоритма поиска ассоциативных правил, учитывающего фактор времени и взаимосвязь событий, для восстановления параметров модели детерминированной L-системы по последовательности символов.

Ключевые слова: фрактал, L-системы, секвенциальный анализ.

Key words: fractal, L-systems, sequential pattern mining.

1. Введение

Фрактал – нерегулярное самоподобное множество. Примеры самоподобных множеств известны с XIX века. Термин «фрактал» (от лат. fractus – раздробленный) впервые ввел в 1975 году математик исследовательского центра IBM Бенуа Мандельброт.

По способу построения выделяют фракталы детерминированные (геометрические и алгебраические) и недетерминированные (стохастические). Геометрические фракталы строятся на основе исходной фигуры путем ее дробления и выполнения различных преобразований полученных фрагментов. Алгебраические фракталы – строятся на основе алгебраических формул. Стохастическими называются фракталы, при построении которых случайным образом изменяются какие-либо параметры. Свойства фракталов:

- нетривиальная структура, которая не упрощается при увеличении масштаба;
- самоподобие;
- дробная метрическая размерность;
- возможность построения при помощи рекурсивной процедуры.

Многие природные объекты обладают фрактальными свойствами. Фракталы применяются в компьютерной науке (фрактальное сжатие данных, децентрализованные сети), физике (моделирование сложных процессов), биологии (моделирование популяций, сложных ветвящихся структур), технике (фрактальные антенны), экономике (фрактальный анализ временных рядов), социологии. В компьютерной графике фракталы используются для генерации изображений природных объектов. Актуальной является задача изучения фрактальных свойств различных объектов.

Целью работы является изучение возможности использования алгоритмов секвенциального анализа для поиска самоподобных элементов изображения или геометрической фигуры. Задачи, которые необходи-

мо решить для этого: изучение моделей фракталов, построенных с помощью L-систем; выбор алгоритма поиска шаблонов последовательных событий (секвенциального анализа, sequential pattern mining или SPM), пригодного для анализа структуры геометрической фигуры с фрактальными свойствами.

2. Свойства L-систем

L-системы разработаны Аристидом Линденмайером, венгерским биологом-теоретиком и ботаником. Линденмайер использовал L-системы для описания поведения клеток растений, моделирования процессов роста и развития растений, морфологии различных организмов (рис.1). Рекурсивная природа правил L-системы ведет к самоподобию и тем самым фракталоподобные формы легко описываются L-системами [1].

Детерминированную контекстно-свободную L-систему определяют как кортеж:

$$G = (V, \omega, P),$$

где V – алфавит, набор символов; ω – аксиома или инициатор, строка символов из V , определяющая начальное состояние системы; P – набор правил, которые определяют, как переменные могут быть заменены комбинациями констант и других переменных.

Во время каждой итерации алгоритма каждый символ заменяется набором символов в соответствии с правилами. Если имеется ровно одно правило для каждого символа, то L-система называется детерминированной (детерминированная контекстно-свободная L-система, DOL-система). Если имеется несколько правил и каждое из них выбирается с определенной вероятностью при каждой итерации, L-система называется стохастической. Различные инструменты 3d моделирования используют L-системы для генерации контента.

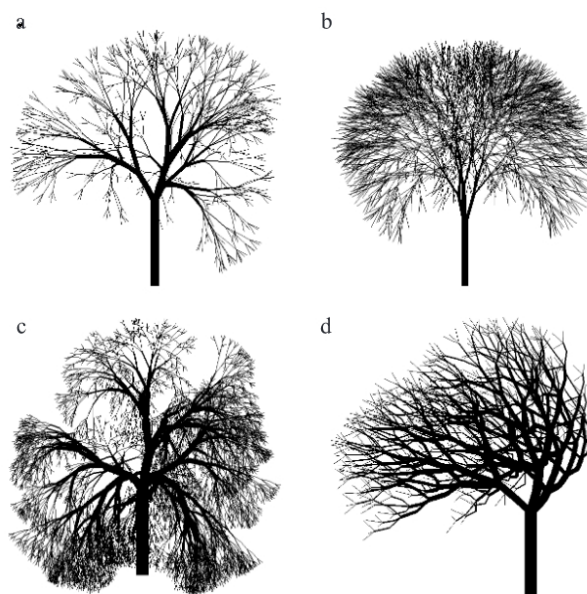


Рис. 1. Модели деревьев, построенные с использованием L-систем [2]

Рассмотрим решение противоположной задачи, а именно определение аксиом и правил L-системы по готовому изображению или его описанию.

Рассмотрим модель фрактала дракон Хартера-Хейтвея:

$$V = \{F, X, Y, +, -\}; \omega = FX; P = \{X \rightarrow X + YF; Y \rightarrow FX - Y\},$$

К символам алфавита добавим интерпретацию: F – двигаться вперед, нарисовать линию; X, Y – переменные; + – поворот на 90° ; – – поворот на -90° .

В результате выполнения четырёх итераций алгоритма получаем следующие последовательности символов (табл. 1).

Таблица 1

№	Последовательность
0	FX
1	FX+YF
2	FX+YF+FX-YF
3	FX+YF+FX-YF+FX+YF-FX-YF
4	FX+YF+FX-YF+FX+YF-FX-YF+FX+YF+FX-YF-FX+YF-FX-YF

Изображение, соответствующее 4-му поколению последовательности, представлено на рис. 2.

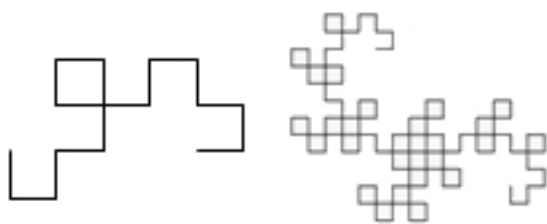


Рис. 2. Четвёртое и седьмое поколения дракона Хартера-Хейтвея

Изменение длины строки последовательности может быть представлено в виде ряда: $a_i = a_{i-1} \times 2 + 1, i = \overline{1, n}$.

Алгоритмы Data Mining по определению Пятницкого-Шапино являются методами поиска в больших объемах данных неочевидных, объективных закономерностей. Рассмотрим возможность использования для построения модели подобного изображения в терминах L-систем алгоритмов формирования ассоциативных правил.

3. Алгоритмы SPM

Поиск ассоциативных правил предполагает нахождение частых зависимостей между объектами или событиями из большого числа наборов данных. Полученные ассоциации представляются в виде правил и могут использоваться как для лучшего понимания природы анализируемых данных, так и для прогнозирования. Однако при этом не учитывается такой атрибут транзакции как время.

Секвенциальный анализ (SPM) – разновидность задачи поиска ассоциативных правил. Целью SPM является установление отношения порядка между исследуемыми наборами. Наиболее распространенными алго-

ритмами SPM являются AprioriALL и GSP. Алгоритм AprioriALL был предложен в 1995 году (Argwal и Srikant). Он, также как другие усовершенствования Apriori, основывается на утверждении, что последовательность, входящая в часто встречающуюся последовательность, также является часто встречающейся.

Исходными данными для алгоритма AprioriALL является упорядоченный набор событий.

Пусть изображение L-системы (модель геометрического фрактала) представлено в виде ломаной линии, заданной последовательностью вершин вида: $\langle P_1(x_1, y_1), \dots, P_n(x_n, y_n) \rangle$, где $n \geq 3, n \in \mathbb{Z}$. Чтобы получить последовательность символов, аналогичную L-системе, необходимо заменить каждый отрезок $P_i P_{i+1}$ из набора $P_1 P_2, P_2 P_3, \dots, P_{n-2} P_{n-1}$ последовательностью

$$\{F\} \dots \{X\} \dots, \text{ где } X = \begin{cases} "-", & (y_i - y_{i+1}) < (y_{i+2} - y_{i+1}), \\ "+", & (y_i - y_{i+1}) > (y_{i+2} - y_{i+1}) \end{cases} \quad F \text{ —}$$

единичный отрезок, длина которого равна длине самого короткого отрезка исходной ломаной; «+» или «-» соответствуют углу поворота ломаной против часовой стрелки или по часовой стрелке; размер угла вычисляется как угол α_i между векторами $\overrightarrow{P_i P_{i+1}}$ и $\overrightarrow{P_{i+1} P_{i+2}}$; количество повторений «+» или «-» равно

$$\frac{\alpha_i}{\alpha_{\min}}, \text{ где } \alpha_1, \alpha_2, \dots, \alpha_{n-2} \text{ — углы между отрезками}$$

ломаной $P_1 P_2 \dots P_n$. Отрезок $P_{n-1} P_n$ заменяется только символом F.

Представим в виде таблицы (табл. 2) данные о последовательности, описывающей L-систему в виде, соответствующем требованиям алгоритма AprioriALL.

Таблица 2

AprioriALL	L-система
D — множество всех транзакций T;	строка символов, например, строка F-F++F-F++F-F++F-F++F-F-F;
T — транзакция, заданная как (ID, дата/время, список объектов);	ID, дата/время определяются номером транзакции, список объектов — это символ строки или несколько одинаковых подряд идущих символов;
I — множество всех объектов (товаров);	символов алфавита, определяемое всеми различными символами, входящими в строку, например, {F, +, -};
s_i — набор, состоящий из элементов I;	набор символов, входящих в транзакцию;
S — последовательность, упорядоченный список наборов.	последовательность символов, входящих в строку, например, F+.

Последовательность символов будем считать клиентской, т.е. соответствующей набору всех транзакций одного клиента, упорядоченных по времени. Периоды времени между любыми двумя транзакциями T_i и T_{i+1} будем считать равными.

Поддержкой последовательности S называется отношение количества транзакций, в которое входит последовательность S , к общему количеству транзакций. Задачей SPM является поиск всех частых последовательностей, т.е. тех, для которых уровень поддержки находится в пределах, обозначенных минимальным и максимальным значением. Оба параметра задаются пользователем до начала работы алгоритма.

Работа алгоритма состоит из нескольких фаз: сортировки; отбора кандидатов; трансформации; генерации последовательностей; максимизации. Ограничением алгоритма AprioriAll является отсутствие возможности определения силы взаимосвязи, т.е. промежутка времени, разделяющего события.

В алгоритме GSP (Generalized Sequential Pattern algorithm) введены дополнительные параметры, благодаря чему стало возможным учитывать ограничения по времени между соседними транзакциями последовательности. В общем виде работа алгоритма GSP похожа на AprioriAll, при этом, как указано в [3], GSP работает быстрее почти в 20 раз. Возможность учитывать ограничения по времени важна для поиска самоподобных элементов в L-системах. Повторное применение такого алгоритма к строке L-системы и сравнение результатов позволит восстановить набор правил P , задающих L-систему.

4. Алгоритм GSP

Рассмотрим подробнее работу алгоритма GSP. Каждая итерация алгоритма предусматривает «проход» по исходному набору данных. Во время первой итерации вычисляется поддержка для каждого объекта (одноэлементной последовательности) и выполняется фильтрация. В результате исходные данные для следующей итерации алгоритма формируются из последовательностей, чья поддержка равна либо превышает пороговое значение. Далее генерируются более длинные последовательности-кандидаты, снова подсчитывается их поддержка и снова производится фильтрация, результаты которой послужат исходными данными для следующего шага алгоритма. Число элементов последовательностей-кандидатов на каждой итерации алгоритма одинаково.

К дополнительным параметрам алгоритма относятся: минимальное и максимальное допустимое время между транзакциями (min-gap и max-gap); размер скользящего окна (w), интервала времени, в пределах которого наборы объектов из одного элемента последовательности могут принадлежать разным транзакциям. Для заданных параметров последовательность $d = \langle d_1..d_m \rangle$ содержит последовательность $s = \langle s_1..s_m \rangle$, если существуют такие целые числа $l_1 \leq u_1 \leq l_2 \leq u_2 < \dots < l_n \leq u_n$, что:

- а) s_i содержится в $\bigcup_{k=l_i}^{u_i} d_k, 1 \leq i \leq n$;
- б) для периода времени между транзакциями d_{u_i} и d_{l_i} , Δ выполняются следующие условия:
 $\Delta \leq w, 1 \leq i \leq n$;
 $\Delta > \text{min-gap}, 2 \leq i \leq n$;
 $\Delta \leq \text{max-gap}, 2 \leq i \leq n$.

Генерация последовательностей-кандидатов производится объединением последовательностей меньшего размера. Объединение последовательностей s_i и $s_j, j > i$ происходит путём добавления к s_i последнего элемента из s_j , если s_j содержит смежную подпоследовательность s_i . Последовательность s является смежной подпоследовательностью $s = \langle s_1 s_2 .. s_n \rangle$, если:

- а) s получается из s при удалении элемента s_1 или s_n ;
- б) s получается из s при удалении одного объекта из элемента s_i , если в его составе не менее двух объектов;
- в) s – смежная подпоследовательность s' , если s' – смежная подпоследовательность s .

Работа алгоритма завершается тогда, когда не найдено ни одной новой последовательности с достаточным уровнем поддержки в конце очередного шага или когда невозможно сформировать новых кандидатов.

Выводы

Обоснована возможность использования алгоритмов SPM для анализа структуры геометрической фигуры с фрактальными свойствами, представленной в терминах L-систем. Для данной задачи лучше подходит алгоритм GSP благодаря его возможности учитывать минимальное и максимальное время между транзакциями. Дальнейшей проработки требуют проблемы восстановления правил L-системы, содержащих переменные, символы, не имеющие геометрической интерпретации, а также L-систем, состоящих из нескольких ломаных линий.

Литература: 1. Capasso V. et al. (ed.). Pattern Formation in Morphogenesis: problems and mathematical issues. – Springer Science & Business Media, 2012. Т. 15. Р. 137-151. 2. Prusinkiewicz P., Lindenmayer A. The algorithmic beauty of plants. Springer Science & Business Media, 2012. 3. Srikant R., Agrawal R. Mining sequential patterns: Generalizations and performance improvements. Springer Berlin Heidelberg, 1996. Р. 1-17.

Транслитерированный список литературы. 1. Capasso V. et al. (ed.). Pattern Formation in Morphogenesis: problems and mathematical issues. Springer Science & Business Media, 2012. Т. 15. Р. 137-151. 2. Prusinkiewicz P., Lindenmayer A. The algorithmic beauty of plants. Springer Science & Business Media, 2012. 3. Srikant R., Agrawal R. Mining sequential patterns: Generalizations and performance improvements. Springer Berlin Heidelberg, 1996. Р. 1-17.

Поступила в редколлегию 02.12.2015

Рецензент: д-р техн. наук, проф. Кириченко Л.О.

Кравец Наталья Сергеевна, канд. техн. наук, доцент кафедры информационно-документных систем Харьковской государственной академии культуры. Научные интересы: моделирование информационных систем, Data Mining. Адрес: Украина, 61057, Харьков, Бурсацкий спуск, 4, тел. (057) 731-32-82. E-mail:kravets_n@list.ru.

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 показника заломлення для радіохвиль або загасання і дисперсії звукових хвиль. Розглянуто один з варіантів вимірювання загасання радіоакустичним методом з використанням подвійної звукової посилювача. Показано його переваги, проведено попередній аналіз. Розглянуто питання практичної реалізації.

Л. 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. Тулиця, 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 напрямки для підвищення ефективності синтаксичного представлення послідовності Р-кадрів на основі міжтрансформантної обробки їх базових структурних одиниць – диференціально-описаних спектрограм. Розкрито напрямки додаткового зниження інтенсивності кодового представлення відеопотоку шляхом скорочення міжкадрової (тимчасової) психовізуальної 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.

Л. 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 parcel 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 intertransformant 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 intertransformant 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 redundancy 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 explained.

Fig. 3. Ref.: 5 items.

УДК681.3

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

Розглянуто селективний метод шифрування відеокادрів, 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.

УДК519.713

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.

УДК510.582

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.

UDC681.3

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.

UDC519.713

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.

UDC510.582

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 constructed 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.

Лл. 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, імplementованих в елементи пам'яті, що дає можливість істотно (в 2-3 рази) підвищити швидкість засобів моделювання.

Лл. 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 двовірними 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.

Лл. 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.

Лл. 2. Бібліогр.: 5 назв.
РИ, 2015, № 4

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 integration of diverse knowledge in the model.

Ref.: 8 items.

UDC 004.421.2:519.71

The use of sequential analysis for studying the structure of fractal objects / N. Kravets // Radioelektronika i informatika. 2015. N 4. P. 64–66.

It is shown the possibility of using the algorithm mining association rules, taking into account the time factor and the relationship of events to restore the parameters of the model L-deterministic system sequence of characters.

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

ПРАВИЛА

оформления рукописей для авторов
научно-технического журнала

"Радиоэлектроника и информатика"

Тематика: радиотехника; электроника; телекоммуникации; компьютерные науки; компьютерная инженерия и техническая диагностика; системы и процессы управления; информационные технологии в науке, образовании, культуре, медицине, экономике, экологии, социологии.

Формат страницы — А4 (210х297 мм), поля: сверху — 15, справа, слева, снизу — 20 мм. Количество колонок — 2, интервал между ними — 5 мм. Редактор: Pagemaker 6.0 (можно, но нежелательно Word), гарнитура Times ET (Times New Roman Cyr), кегль — 10 пунктов, межстрочное расстояние — 110%, табуляция — 5 мм.

Объем рукописи — от 2 до 10 с. (языки: русский, украинский, английский). Текст рукописи должен быть структурирован и содержать все *основные части, характерные для научной статьи*: **введение** (отражает актуальность, формулирование цели и задач исследования); **сущность** (изложение основного материала исследования с описанием идеи, метода, и обоснованием полученных научных результатов); **выводы** (отражают результаты исследования, их научную новизну и практическую значимость, сравнение с лучшими аналогами, перспективы).

Структура рукописи: заголовок, аннотация, текст, литература, реферат (на украинском и английском языках), сведения об авторах.

ОБРАЗЕЦ ОФОРМЛЕНИЯ

УДК519.713

НАЗВАНИЕ РУКОПИСИ

ФАМИЛИЯ И.О.

(Название желаемого раздела тематики)

Аннотация (на языке статьи, абзац 5-10 строк, кегль 9) помещается в начале статьи и содержит информацию о результатах описанных исследований.

Основной текст можно разделять на 2 и более подразделов с заголовками, выделенными полужирным шрифтом, пронумерованными арабскими цифрами, как показано в следующей строке.

1. Название раздела

Рисунки и таблицы (черно-белые, контрастные) помещаются в текст после первой ссылки в виде *переносимых объектов* и отдельно нумеруются, при наличии более одного рисунка (таблицы), арабскими цифрами. Рисунок содержит подрисуночную центрированную подпись под иллюстрацией (вне рисунка), как показано на рис. 1.

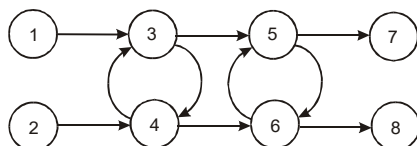


Рис. 1. Граф с контурами

Табличный заголовок располагается справа над таблицей (вне таблицы), что иллюстрируется табл.1. Редакторы: CorelDraw, Table Editor, Excel.

Таблица 1

Шаг i	1	2	3	4	5	6
Ф1(1,3)	1	2	2	4	6	1

Формулы нумеруются при наличии ссылок на них в рукописи. Формулы, символы, переменные, встречающиеся в тексте, должны быть набраны как объекты Microsoft Equation. Рекомендуются высота формульных кеглей: переменная — 10 пунктов, индекс — 8, над- и подиндекс — 8, основной (индексный) математический символ — 12(10):

$$F_{i+i} = \sum_{i=1}^k F_j^i - \prod_{j=1}^{1+h} P_{R_{j+i}} + F^{j-1} + X^{\sum n^k}. \quad (1)$$

Формат переменных (желательно не курсивом — без наклона) в тексте и формулах должен быть идентичным. В тексте над- и подиндексы составляют 70 % от высоты кегля, которые рекомендуются опускать (поднимать) на 17 (33) % относительно основной строки.

Литература (включает опубликованные источники, на которые имеются ссылки в тексте, заключенные в квадратные скобки) печатается без отступа, кегль 9 пунктов.

Образец окончания текста рукописи (литература, сведения об авторах, реферат) представлен ниже.

Литература: 1. *Фамилия И.О.* Название книги. Город: Издательство, 1900. 000 с. 2. *Название сборника /* Под ред. И.О. *Фамилия.* Город: Издательство, 1900. 000 с. 3. *Фамилия И.О.* Название статьи // Название журнала. Название серии. 1997. Т. 00, № 00. С. 00-00.

Поступила в редколлегию 00.00.00

Рецензент: должность, ученая степень, Фамилия, И.О.

Фамилия, имя, отчество, ученая степень, звание, должность и место работы. Научные интересы. Увлечения и хобби. Адрес, контактные телефоны.

Рефераты представляются на украинском и английском языках.

УДК 000.000.00

Назва статті /Ініціали. Прізвище // **Радіоелектроніка та інформатика.** 2000. № 00. С. 00-00.

Текст реферату.

Табл. 00. Лл. 00. Бібліогр.: 00 назв.

UDC 000.000.00

Title of paper /Initials. Surname // **Radioelektronika i informatika.** 2000. N 00. P. 000-000.

Text.

Tab. 00. Fig. 00. Ref.: 00 items.

Представление материалов

Рукопись, рефераты, сведения об авторах — в одном файле, *поименованном фамилией автора*, на дискете 3,5 дюйма. Твердая копия материалов — для граждан Украины — в одном экземпляре: рукопись, подписанная авторами, рефераты, акт экспертизы, внешняя рецензия, подписанная доктором наук, заявление на имя главного редактора со сведениями об авторах.

Адрес редакции: Украина, 61166, Харьков, пр. Ленина, 14, ХНУРЭ, комната 321, тел. 70-21-326, e-mail: ri@kture.kharkov.ua; hahanov@kture.kharkov.ua. <http://www.ewdtest.com/ri>

Рекомендовано Ученым советом Харьковского национального университета радиоэлектроники (протокол № 4 от 27.12.2015)

Підписано до друку 27.12.2015. Формат 60×84^{1/8}.

Умов. друк. арк. 10,8. Зам. № б/н. Тираж 300 прим. Ціна договірна.

Віддруковано у СПД ФО Степанов В.В.

61168, Харків, Акад. Павлова, 311.