МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 3, № 4

Volume 3, No. 4

Одеса – 2013
Odesa – 2013

Журнал внесений до переліку наукових фахових видань України
(технічні науки)
згідно наказу Міністерства освіти і науки України № 463 від 25.04.2013 р.

Виходить 4 рази на рік

Заснований Одеським національним політехнічним університетом у 2011 році

Свідоцтво про державну реєстрацію КВ № 17610 - 6460Р від 04.04.2011р.

Published 4 times a year

Founded by Odessa National Polytechnic University in 2011

Certificate of State Registration КВ № 17610 - 6460P of 04.04.2011

Друкується за рішенням редакційної колегії та Вченої ради Одеського національного політехнічного університету

Оригінал-макет виготовлено редакцією журналу

Адреса редакції: просп. Шевченка, 1, Одеса, 65044, Україна
Телефон: +38 048 734 8506
Web: http://immm.opu.ua E-mail: immm.ukraine@gmail.com

Editorial address: 1 Shevchenko Ave., Odessa, 65044, Ukraine
Tel.: +38 048 734 8506
Web: http://immm.opu.ua E-mail: immm.ukraine@gmail.com

ЗМІСТ / CONTENTS

ТЕХНОЛОГІЇ КОМПОЗИЦІЙНО-СТРУКТУРНОГО МОДЕЛЮВАННЯ ДИСТАНЦІЙНОГО НАВЧАННЯ А.Я. Мушак	299	TECHNOLOGY COMPOSITION AND STRUCTURAL SIMULATION DISTANCE LEARNING Mushak A.
АНАЛІТИЧНІ ЗАЛЕЖНОСТІ ПРИСКОРЕНОГО ОБЧИСЛЕННЯ ЕЛЕМЕНТІВ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ ДЛЯ МОЖЛИВОСТІ ПОБУДОВИ МЕТОДІВ АВТЕНТИФІКАЦІЇ ТА ЦИФРОВОГО ПІДПИСУВАННЯ Ю.Є. Яремчук	306	ANALYTIC DEPENDENCES OF FAST COMPUTATION OF THE TERMS OF RECURRENT SEQUENCES TO BE USED IN THE DEVELOPMENT OF AUTHENTICATION AND DIGITAL SIGNATURE TECHNIQUES Yaremchuk Yu.
ІМОВІРНІСНІ МЕТОДИ КЕРУВАННЯ ПЕРЕДАВАННЯМ В РАДІОМЕРЕЖІ М.П. Карпінський, О.Г. Корченко, С.В. Райба	314	PROBABILISTIC METHODS OF CONTROLLING EMISSIONS IN THE RADIO NETWORK Karpinski M., Korchenko O., Rajba S.
МЕТОД ОЦІНКИ ВЕЛИЧИНИ ПРИХОВАНОЇ ПРОПУСКНОЇ СПРОМОЖНОСТІ КАНАЛУ, СФОРМОВАНОГО МЕТОДОМ МОДИФІКАЦІЇ НАЙМЕНШОГО ЗНАЧУЩОГО БІТА І.І. Бобок	323	A TECHNIQUE TO ESTIMATE A STEGANOGRAPHIC CAPACITY OF A STEGO CHANNEL FORMED WITH LSB MODIFICATION APPROACH Bobok I.
ДІАГНОСТУВАННЯ СКЛАДНИХ ТЕХНІЧНИХ СИСТЕМ З ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ Л.С. Ломакіна, В.П. Губернаторов	331	STRUCTURAL TESTING OF SOFTWARE SYSTEMS BASED ON COMPUTER ALGEBRA ELEMENTS Lomakina L., Gubernatorov V.

МЕТОД МОДЕЛЮВАННЯ ДІЯЛЬНОСТІ СУБ'ЄКТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З ВИКОРИСТАННЯМ ОПЕРАТОРІВ, ЩО ДІЮТЬ В ОНТОЛОГІЯХ ПРЕДМЕТНИХ ОБЛАСТЕЙ
А.А. Шиян
342
A TECHNIQUE TO MODEL THE ACTIVITIES OF INFORMATION SECURITY SUBJECTS INVOLVING THE APPLICATION OF OPERATORS ACTING IN DOMAIN ONTOLOGIES
Shiyan A.

СТІЙКЕ СТЕГАНОПЕРЕТВОРЕННЯ В ПРОСТОРОВІЙ ОБЛАСТІ ЗОБРАЖЕННЯ-КОНТЕЙНЕРА
В.М. Рудницький, О.В. Костирка
353
ROBUST STEGANO TRANSFORMATION IN SPATIAL DOMAIN OF COVER IMAGE
Rudnitsky V., Kostyrka O.

МЕТОД ЗАХИСТУ QR-КОДУ З ВИКОРИСТАННЯМ ЦИФРОВОГО ВОДЯНОГО ЗНАКУ
О.В. Наріманова, Д.М. Семенченко
361
DIGITAL WATERMARKING APPROACH FOR QR-CODE PROTECTION
Narimanova O., Semenchenko D.

МЕТОД ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ В АПАРАТНІ КОНТЕЙНЕРИ З LUT-ОРІЄНТОВАНОЮ АРХІТЕКТУРОЮ
К.В. Защолкін, О.М. Іванова
369
METHOD OF EMBEDDING OF DIGITAL WATERMARKS IN HARDWARE CONTAINERS WITH LUT-ORIENTED ARCHITECTURE
Zashcholkin K., Ivanova O.

УДК 681.3

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 4, pp. 299-305

ТЕХНОЛОГІЇ КОМПОЗИЦІЙНО-СТРУКТУРНОГО МОДЕЛЮВАННЯ ДИСТАНЦІЙНОГО НАВЧАННЯ

А.Я. Мушак

Тернопільський національний економічний університет,
вул. Львівська, 11, Тернопіль, 46020, Україна; e-mail: andriy_mushak@hotmail.com

Пропонується використання елементів композиційно-структурного моделювання для вирішення задач побудови інтерактивних дистанційних мультимедійних програм навчального призначення, які функціонують в середовищі Інтернет. Побудована математична модель навчальної системи з алгоритмом знаходження розв'язків задач при побудові навчальних програм за КСМ-технологією дозволяє реалізувати методику послуговування засобами інтерактивної мультимедіа в дистанційному навчанні. Запропонований підхід до створення курсів дистанційного навчання підвищує технологічність процесів навчання. На основі запропонованого підходу реалізовано ряд курсів дистанційного навчання.

Ключові слова: дистанційне навчання, композиційно-структурне моделювання, мультимедійні програми навчального призначення, прикладна програмна система

Вступ

Розвиток інформаційного суспільства характеризується підвищеними вимогами до рівня освіченості кожного його члена. Оскільки освіта створює фундамент розвитку будь-якої держави, то вона належить до стратегічно найважливіших напрямків впровадження телекомунікаційних та інформаційних технологій в Україні. Поступовий перехід до високоінтелектуального виробництва, невпинний розвиток інформаційних технологій, який супроводжується впровадженням їх у повсякденність і, загалом, зростання темпу життя вимагає від кожної особистості постійного вдосконалення набутого рівня знань та оволодіння кардинально новими знаннями. Іншими словами, мова йде про необхідність навчання протягом усього життя.

Для розв'язання окресленої глобальної задачі прийнятливими є всі доступні засоби. Маємо на увазі як традиційні, так і новітні форми навчання [1–4]. Серед останніх чільне місце належить дистанційному навчанню через глобальні комп'ютерні мережі, оскільки воно має ряд істотних переваг в контексті сьогоднішньої ситуації порівняно із традиційним:

- забезпечує індивідуальний вибір траєкторії навчання: режиму, часу й швидкості;
- забезпечує постійний доступ студентів до навчальних матеріалів;
- забезпечує постійний контакт з викладачем: студент може в будь-який момент звернутися до викладача за допомогою;
- дає можливість залучати закордонних викладачів. Використовуючи мережу Інтернет, вони можуть навчати одночасно всіх бажаючих з різних країн світу. Викладачам не потрібно переїжджати з країни в країну для проведення лекцій;
- забезпечує постійне спілкування між студентами з метою як обговорення поточних питань в ході опрацювання навчального матеріалу, так і для контактування за взаємними інтересами;

- привносить економічний ефект – збільшення кількості студентів не вимагає суттєвих додаткових витрат. У даному реченні й далі, під словом „студент” слід розуміти кожного, хто навчається за програмою дистанційного курсу (наприклад, сюди відносяться учні середніх шкіл, студенти вузів, особи, які проходять перекваліфікацію, підвищують свій рівень знань тощо).

На сьогоднішній день технології дистанційного навчання знаходяться в стадії інтенсивного розвитку. Вагомий внесок у дослідження методології побудови інтерактивних дистанційних мультимедійних програм навчального призначення, вклали вітчизняні та зарубіжні вчені: О.М. Довгялло, В.Н. Кухаренко, М.І. Жалдак, В.В. Лапінський, В.М. Томашевський, П. Коммерс та інші [2–7], яким належить ряд важливих результатів, що стосуються розробки моделей, методів та технологій дистанційного навчання, проте значна кількість проблемних питань все ще потребує вирішення.

Ключовою задачею, яку вирішують сьогодні, є створення методології, яка б містила, з одного боку, методи підвищення технологічності при моделюванні процесів дистанційного навчання, а з іншого – методи дослідження та аналізу ефективності розглядуваного виду навчання.

У роботах [8, 9] пропонуються моделі та методика, які, в цілому, дозволяють говорити про створення елементів методології побудови курсів дистанційного навчання (КДН). Саме в цьому, а також у можливості використання в рамках запропонованого підходу різних технологій проектування та створення програмного забезпечення (в тому числі об’єктно-орієнтованих) і полягає актуальність дослідження.

Мета та задачі дослідження

Мета дослідження – розробка елементів методології побудови інтерактивних дистанційних мультимедійних програм навчального призначення.

Відповідно до поставленої мети в статті ставляться й вирішуються такі задачі:

- розглянути засади технології композиційно-структурного моделювання;
- побудувати математичну модель навчаючої системи;
- дослідити застосування елементів технології композиційно-структурного моделювання (КСМ-технології) в КДН;
- реалізувати методику послуговування засобами інтерактивної мультимедіа в дистанційному навчанні.

Елементи технології композиційно-структурного моделювання

Розглянемо елементи КСМ-технології з метою використання деяких з них для побудови КДН [10, 11]. Ця технологія дозволяє збільшити продуктивність праці розробників прикладних програмних систем (ППС) (що до них відносять і програми навчального призначення), покращити якість та надійність таких систем шляхом вироблення уніфікованих механізмів, моделей мов, методологій побудови ППС.

Монолітний спосіб проектування прикладних програм, а відтак, і наступного їх програмування, характерний для програмного забезпечення 1-го покоління. Складність і зростаюча вартість ППС дозволяє зробити висновок про недосконаліть цього способу.

Технологічнішим принципом програмування є модульність, при якій програма проектується як деякий ланцюжок складових частин («цеглинок»), що одержали назву модулів. Кожна з таких «цеглинок» виступає як окремна програмна одиниця; її проектують автономно, автономно програмують і тестують, використовують у найрізноманітніших програмах, як складову частину, коли тільки за своїм

функціональним призначенням модуль відповідає потребам. Модульність забезпечує структурну адаптацію алгоритму до розв'язуваної задачі, до нього можна підключати нові «цеглинки», змінювати та поновлювати старі аж до конструювання цілком нового алгоритму.

Розглянуті концептуальні основи макромодульного програмування, а саме, опис синтаксичних моделей мов макромодульного середовища програмування та опис верифікації композиційних схем доцільно використовувати для досягнення поставлених цілей.

При побудові КДН за КСМ-технологією виникає ряд оптимізаційних проблем, в цілому характерних для різних стадій розробки ППС. Зокрема, проблема вибору оптимального алгоритму в заданій множині конкуруючих алгоритмів при різних практично важливих припущеннях про властивості останніх може бути сформульована таким чином.

Нехай для розв'язання задачі $z_j \in Z$ визначена множина алгоритмів $A_j \in A$, за допомогою яких ця задача може бути розв'язана. Алгоритмам $A_{ji} \in A$ поставлена у відповідність послідовність характеризуючих їх параметрів $\alpha_{ji} = \{\alpha_{ji}^k : k = 1,\ldots,q\}$. У множині A_j потрібно вибрати алгоритм A_{je} такий, щоб

$$\phi(\alpha_{je}, \gamma_{je}) = ext_i \cdot \phi(\alpha_{ji}, \gamma_{ji})$$

при деяких обмеженнях на α_{ji}.

Ця задача в загальному випадку є складною задачею багатокритеріальної оптимізації і з урахуванням потреб практики побудови КДН може набувати (прирівнюванням окремих параметрів a_k до нуля) різних часткових формулювань типу:

- серед усіх алгоритмів A знайти хоча б один алгоритм, за допомогою якого можна розв'язати дану задачу;
- у множині алгоритмів A знайти найефективніший за якимось одним показником, наприклад, за швидкодією для розв'язування даної задачі та інше.

Практичний інтерес викликає пошук такого алгоритму, всі показники якого найближче відповідали б вимогам користувача при розв'язуванні даної задачі.

Застосування елементів КСМ-технології для дистанційного навчання

Демонстрацією застосування елементів КСМ-технології в КДН може бути, зокрема, низка прикладів послуговування розглядуваною технологією для реалізації навчальних завдань.

Побудована математична модель навчаючої системи шляхом введення так званих функцій розширення $G_{\langle x^*, y^* \rangle}$ в просторі станів, визначенні операцій їх суми та добутку

$$G_{\langle x^*, y^* \rangle} + H_{\langle u^*, v^* \rangle}$$

$$G_{\langle x^*, y^* \rangle} \cdot H_{\langle u^*, v^* \rangle}$$

та складної функції $R_{\langle r,s \rangle}(x)$, яка задається рекурсивною схемою:

$$R_{\langle r,s\rangle}(x)=G_{\langle x^*,y^*\rangle}(x)\,|\,R_{\langle r,s\rangle}(x)+H_{\langle u^*,v^*\rangle}\,|R_{\langle r,s\rangle}(x)\cdot H_{\langle u^*,v^*\rangle}\,|\,H_{\langle u^*,v^*\rangle}\cdot R_{\langle r,s\rangle}(x).$$

Задачею на математичній моделі *C* називається пара станів $\langle x_0, y_0\rangle$.

Складна функція $R_{\langle r,s\rangle}(x)$ називається розв'язком задачі $\langle x_0, y_0\rangle$ на моделі *C*, якщо виконуються такі умови:

1) x_0 належить області визначення функції $R_{\langle r,s\rangle}(x)$, тобто $x_0 \in Z=\{z: z\ge r\}$.

2) $R_{\langle r,s\rangle}(x_0)\ge y_0$.

Показано, що для того, щоб функція $R_{\langle r,s\rangle}(x)$ була розв'язком задачі $\langle x_0, y_0\rangle$, необхідно і достатньо, щоб виконувалась умова $x_0 \ge y_0^{\bar{s}} \vee r$.

Алгоритм побудови розв'язку задачі $\langle x_0, y_0\rangle$ на моделі *C* зводиться до виконання такої послідовності кроків:

1) покласти $W_1=\left\{G^1_{\langle x(j),y(j)\rangle}(x): G^1_{\langle x(j),y(j)\rangle}(x)\in\Im, x(j)\le x_0, j=1,\ldots,m_1\right\}$;

2) нехай $G^1_{\langle x(j),y(j)\rangle}(x)=\left(\sum_{j=1}^{m_1} G^1_{\langle x(j),y(j)\rangle}\right)(x)$ і $d_1=G^1_{\langle x,y\rangle}(x_0)$, де

$$x=\bigvee_{j=1}^{m_1} x(j),\quad y=\bigvee_{j=1}^{m_1} y(j);$$

3) організувати ітераційний процес побудови множин W_i таким чином:

$$W_i=\left\{G^i_{\langle x(j),y(j)\rangle}(x): G^i_{\langle x(j),y(j)\rangle}(x)\in\Im\setminus\bigcup_{l=1}^{i-1}W_l, x(j)\le d_{i-1}, j=1,\ldots,m_1\right\},$$

$$G^i_{\langle x,y\rangle}(x)=\left(\sum_{j=1}^{m_1} G^i_{\langle x(j),y(j)\rangle}\right)(x)\ \text{і}\ d_i=G^i_{\langle x,y\rangle}(d_{i-1}),\ x=\bigvee_{j=1}^{m_i} x(j),\ y=\bigvee_{j=1}^{m_i} y(j);$$

4) ітераційний процес зупиняється за умовою $W_i=\varnothing$;

5) якщо $W_i=\varnothing$ на *k+1* кроці ітераційного процесу, то покласти

$$R_{\langle r,s\rangle}(x)=\left(\prod_{i=1}^{k} G^i_{\langle x,y\rangle}\right)(x).$$

Твердження і наведений алгоритм дозволяють строго розв'язувати задачі контролю правильності виконання завдань, зокрема побудови графіків функцій. Це досягається шляхом визначення умов, при яких заданий графік можна побудувати, а також усіх можливих способів побудови графіка, які одержуємо як різні (відносно комутативності) розв'язки задачі на формальній моделі.

Опишемо деталі програмної реалізації одного з прикладів – побудови графіків функцій. Суть цього завдання полягає у наданні можливості студентові вправлятися у побудові графіків таких функцій, які є композицією інших (простіших функцій). Очевидним є те, що собою представлятимуть модулі для даної задачі в контексті КСМ-технології – це програми, які реалізують побудову графіка тієї чи іншої простої функції або ж їх композиції. До модулів відноситимемо й програму, що дозволяє відображати графіки як набори пікселів, а також подає координатну площину із необхідною інфраструктурою.

Шукане програмове забезпечення написане мовою Java. Кожен модуль програмної системи – це аплет. Для спрощення роботи послуговувалися інтегрованим середовищем програмування – JBuilder 5 Personal.

Особлива увага приділяється організації програмового коду. Зокрема, враховуючи те, що модулі не є статичними одиницями, зазначено нюанси передачі даних між ними в ході застосування інтерфейсу `AppletContent`. Відомо, що взаємодія між аплетами, розташованими на одній HTML-сторінці, передбачає лише звертання із одного з аплетів (аплета-клієнта) до методу, означеного в іншому аплеті (аплеті-сервері). В нашому випадку аплетом-сервером є аплет «Координатна площина»; решта аплетів – аплети-клієнти. У кожному із аплетів-клієнтів є звертання до методу

```
AddPoint (int Value_Of_Function, int red_Ingrad, int green_Ingrad,
int blue_Ingrad)
```

аплета-сервера. Це реалізується за допомогою контексту аплета.

```
appletServer=getAppletContext().getApplet("CoordinatePlane");
((Applet1) appletServer).AddPoint(y,red_Ingradient,
green_Ingradient,blue_Ingradient);
```

Метод `AddPoint` додає у масив значень функції нову точку. Вищенаведений фрагмент лістингу стверджує, що даний метод параметризований, передається не тільки значення функції, але й значення трьох величин типу `int` – складових кольору, що ним відображатиметься графік. Після закінчення формування масиву значень виконується метод `paint()`, що є перекритий нами. Завдяки цьому висвітлюється новий графік. Побудова графіків функцій вигляду $y=-f(x)$, $y=f(|x|)$, $y=|f(x)|$, $y=|f(|x|)|$ та $y=f_1(x)+f_2(x)$ передбачає отримання у відповідний аплет одного чи двох масивів

```
(Value_Of_Function_Array_Second[])

(Value_Of_Function_Array_First[], Value_Of_Function_Array_Second[])
```

значень функції задля наступної його (їх) обробки. Для цього в аплеті «Координатна площина» визначені нижченаведені методи.

```
public int[] get_Value_Of_Function_Array_Second() {
return Value_Of_Function_Array_Second;
}
public int[] get_Value_Of_Function_Array_First() {
return Value_Of_Function_Array_First;
}
```

Природа дії цих методів тривіальна; вони повертають масиви значень функцій. Далі, використовуючи контекст аплета, зчитуються ці дані, наприклад,

```
appletServer=getAppletContext().getApplet("CoordinatePlane");
Value_Of_Function_Array_Local=((Applet1)
appletServer).get_Value_Of_Function_Array_Second();
```

після чого відбувається обробка масиву `Value_Of_Function_Array_Local`.

Практична реалізація завершується розглядом реалізації інтерактивності в КДН «Розміщення продуктивних сил України», який використовувався для навчання студентів у Міжнародному університеті фінансів. Побудовано «Курс комунікаційних та

інформаційних технологій», «Інтерактивна навчальна програма для викладачів з використанням телематики в дистанційному навчанні» та інші.

Зазначено, зокрема, як і якими засобами інтерактивної мультимедіа представлений лекційний матеріал курсу, як організований контроль отриманих студентом знань та в чому полягають особливості дизайну курсу.

Висновки

Застосовуючи методику використання засобів інтерактивної мультимедіа в КДН, розроблено підхід щодо використання КСМ-технології при розробці фрагментів КДН і запропонована математична модель навчаючої системи з алгоритмом знаходження розв'язків задач при побудові навчаючих програм за КСМ-технологією.

Розроблений підхід до побудови інтерактивних програм навчального призначення за допомогою КСМ-технології продемонстрований на конкретному прикладі застосування КСМ-технології в курсах дистанційного навчання. Розв'язано ряд задач, що виникають в процесі навчання, зокрема в ході побудови графіків елементарних функцій.

Підходи до моделювання різних процесів дистанційного навчання можуть бути основою інструментального середовища підтримки побудови курсів дистанційного навчання з урахуванням усього комплексу методологічних проблем, які при цьому виникають.

Список літератури

1. Белов, В.Н. Принципы организации и результаты экспериментального апробирования пакета подпрограмм, ориентированных на изготовление диалоговых обучающих программ / В.Н. Белов, А.М. Довгялло // Управляющие системы и машины. — 1978. — № 1. — С. 41–47.
2. Довгялло, А.М. Обучающие системы нового поколения / А.М. Довгялло, Е.Л. Ющенко / Управляющие системы и машины. — 1988. — № 1. — С. 83–86.
3. Кухаренко, В.М. Дистанційне навчання: умови застосування. Дистанційний курс [Текст] : навч. посібник / В.М. Кухаренко, О.В. Рибалко, Н.Г. Сиротенко; Харківський політехнічний ін-т, нац. техн. ун-т. — Х. : НТУ «ХПІ», 2001. — 320 с.
4. Кухаренко, В.Н. Дистанційне навчання: Умови застосування. Дистанційний курс [Текст] / В.М. Кухаренко; За ред. В.М. Кухаренка. — Х. : Торсінг, 2002. — 320 с.
5. Томашевський, В.М. Моделювання систем [Текст] : підруч. для студ. вищ. навч. закл., які навч. за напрямами «Комп'ютерні науки», «Комп'ютеризовані системи, автоматика і управління», «Комп'ютерна інженерія», «Прикладна математика» / В.М. Томашевський; Ред. М.З. Згуровський. — К. : BHV, 2005. — 349 с.
6. Информационные и коммуникационные технологии для среднего образования. Специализированный учебный курс / П. Коммерс, М. Семерлинг. — М. : Изд. Дом «Обучение-Сервис», 2005. — 128 с.
7. Мушак ,А. Дистанційне навчання: від побудови моделей до генерації програмного коду / А. Мушак, О. Провотар // Вісник Тернопільського національного технічного університету. — 2003. — № 1. — С. 107–115.
8. Мушак, А.Я. Комп'ютерне моделювання процесів дистанційного навчання в Інтернет-технологіях [Текст] : автореф. дис... канд. техн. наук: 01.05.02 / Мушак Андрій Ярославович ; НАН України, Ін-т кібернетики ім. В. М. Глушкова. — К., 2004. — 20 с.
9. Мушак, А. Методологія використання інтерактивної мультимедіа в дистанційному навчанні / А. Мушак // Тези доповідей Міжнародної науково-практичної конференції «Проблеми впровадження інформаційних технологій в економіці та бізнесі». — Ірпінь, 2000. — С. 319–320.
10. Мушак, А. Использование коммуникационных и информационных технологий преподавателями / А. Мушак // Материалы VII Международной конференции по дистанционному образованию «Дистанционное образование: открытые и виртуальные среды». — М., 1999. — С. 190–197.

11. Mushak, A. Using the interactive multimedia in distance course «Communication and information technologies (CIT-course)» // Proc. Seminar about Computers in School POŠKOLE'99. — Lázně Sedmihorky (Czech Republic), 1999. — PP. 119–121.

ТЕХНОЛОГИИ КОМПОЗИЦИОННО-СТРУКТУРНОГО МОДЕЛИРОВАНИЯ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

А.Я. Мушак

Тернопольский национальный экономический университет,
ул. Львовская, 11, Тернополь, 46020, Украина; e-mail: andriy_mushak@hotmail.com

Предлагается использование элементов композиционно-структурного моделирования для решения задач построения интерактивных дистанционных мультимедийных программ учебного назначения, функционирующих в среде Интернет. Построенная математическая модель обучающей системы с алгоритмом нахождения решений задач при построении учебных программ по КСМ-технологии позволяет реализовать методику использования средств интерактивной мультимедиа в дистанционном обучении. Предложенный подход к созданию курсов дистанционного обучения повышает технологичность процессов обучения. На основе предложенного подхода реализован ряд курсов дистанционного обучения.

Ключевые слова: дистанционное обучение, композиционно-структурное моделирование, мультимедийные программы учебного назначения, прикладная программная система

TECHNOLOGY COMPOSITION AND STRUCTURAL SIMULATION DISTANCE LEARNING

Andriy Y. Mushak

Ternopil National Economic University,
11 Lvivska str, Ternopil, 46020, Ukraine; e-mail: andriy_mushak@hotmail.com

Proposed is to use the elements of compositional and structural modeling (KSM) to solve the problems related to the development of web-based interactive multimedia software applications for distance learning and training. When developing learning and training software with KSM approach, the mathematical model of learning and training system with problem solution finding algorithm developed makes it possible to implement a methodology of using interactive multimedia means in distant learning and training. The approach proposed to develop distance learning and training courses increases the technological flexibility of learning and training processes. Based on the approach proposed, a number of learning and training courses has been already developed.

Keywords: distance learning, compositional and structural modeling, multimedia programs for educational purposes, the application software system

УДК 511.216

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 4, pp. 306-313

АНАЛІТИЧНІ ЗАЛЕЖНОСТІ ПРИСКОРЕНОГО ОБЧИСЛЕННЯ ЕЛЕМЕНТІВ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ ДЛЯ МОЖЛИВОСТІ ПОБУДОВИ МЕТОДІВ АВТЕНТИФІКАЦІЇ ТА ЦИФРОВОГО ПІДПИСУВАННЯ

Ю.Є. Яремчук

Вінницький національний технічний університет,
вул. Хмельницьке шосе, 95, Вінниця, 21021, Україна; e-mail: yurevyar@vntu.net

Проведено дослідження рекурентних V_k –послідовностей та отримано аналітичні залежності прискореного обчислення елементів цієї послідовності. Встановлено властивості обчислення елементів $v_{-n+m,k}$ та $v_{-n-m,k}$. Це дозволило розширити математичний апарат рекурентних V_k –послідовностей щодо можливості побудови асиметричних криптографічних методів різного призначення, зокрема методів автентифікації та цифрового підписування.

Ключові слова: рекурентні послідовності, аналітичні залежності, криптографія, автентифікація, цифрове підписування

Вступ

Рекурентні послідовності в загальному вигляді породжуються таким співвідношенням [1]:

$$u_n = a_1 \cdot u_{n-1} + a_2 \cdot u_{n-2} + \ldots + a_k \cdot u_{n-k},$$

де

$a_1, a_2, \ldots, a_k$ — коефіцієнти,

k — порядок послідовності, виходячи з початкових елементів $u_0, u_1, \ldots, u_k$.

Прикладом рекурентної послідовності є відома послідовність Фібоначчі [2], для якої

$$u_n = u_{n-1} + u_{n-2},$$

з початковими елементами $u_0 = 1$ та $u_1 = 1$.

В [3] розглянуто математичний апарат рекурентних V_k – та U_k –послідовностей, в яких початкові елементи пов’язані з коефіцієнтами рекурентного співвідношення. Використовуючи цей апарат, було запропоновано методи асиметричного шифрування інформації, які забезпечили прискорення обчислень у порівнянні з відомими аналогами.

В [3] було запропоновано ідею використання математичного апарату рекурентних V_k– та U_k–послідовностей для побудови асиметричних криптографічних методів різного призначення, як то розподілу секретних ключів, автентифікації та цифрового підписування. Для цього отримано аналітичні залежності для V_k–послідовності, що забезпечують можливість прискореного обчислення елементів $v_{n+m,k}$ та $v_{n-m,k}$ цієї послідовності для цілих додатних n, m та k. На основі цих залежностей в [3] було представлено методи асиметричного шифрування інформації, що базуються на V_k– та U_k–послідовностях.

Однак, для побудови асиметричних криптографічних методів автентифікації сторін взаємодії та цифрового підписування отриманих залежностей недостатньо, оскільки ці криптографічні призначення використовують більш складні криптографічні перетворення, ніж при шифруванні. Тому для розширення можливості побудови асиметричних криптографічних методів різного призначення виникає необхідність отримання аналітичних залежностей прискореного обчислення елементів $v_{-n+m,k}$ та $v_{-n-m,k}$.

Мета роботи

Дослідження рекурентних V_k–послідовностей щодо отримання аналітичних залежностей прискореного обчислення елементів $v_{-n+m,k}$ та $v_{-n-m,k}$.

Постановка задач досліджень

Розглянути математичний апарат рекурентних V_k–послідовностей, встановити і довести аналітичні залежності прискореного обчислення елементів $v_{-n+m,k}$ та $v_{-n-m,k}$ для цієї послідовності.

Дослідження можливості отримання аналітичних залежностей прискореного обчислення елементів $v_{-n+m,k}$ та $v_{-n-m,k}$ для V_k–послідовності

V_k–послідовність [3] складається з V_k^+– та V_k^-–послідовності.

V_k^+–послідовність визначається як послідовність чисел, що обчислюються за формулою

$$v_{n,k} = g_k \cdot v_{n-1,k} + g_1 \cdot v_{n-k,k} \qquad (1)$$

при початкових значеннях $v_{0,k} = 1$, $v_{1,k} = g_2$ для $k = 2$; $v_{0,k} = v_{1,k} = \ldots = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$ для $k > 2$; де g_1, g_k — цілі числа; n і k — цілі додатні числа.

Формула (1) дозволяє отримувати елементи послідовності для зростаючих n, починаючи з $n = 0$. Зворотна процедура обчислення елементів послідовності для спадних n, починаючи з деякого значення $n = l$, буде здійснюватись таким чином

$$v_{n,k} = \frac{v_{n+k,k} - g_k \cdot v_{n+k-1,k}}{g_1}. \qquad (2)$$

Формула (2) дозволяє обчислювати елементи V_k^+–послідовності, тобто елементи $v_{n,k}$ з додатними значеннями індексу для спадних n. Обчислення за формулою (2) може продовжуватись і для від'ємних значень індексу. В такому випадку обчислення елементів $v_{-n,k}$, теж для спадних n, буде здійснюватись за такою формулою

$$v_{-n,k} = \frac{v_{-n+k,k} - g_k \cdot v_{-n+k-1,k}}{g_1}. \qquad (3)$$

Тобто існує два виду послідовностей: перший вид послідовності формується для додатних значень індексу, тобто елементів $v_{n,k}$, за формулою (1); другий вид послідовності формується для від'ємних значень індексу, тобто елементів $v_{-n,k}$, за формулою (3).

Другий вид послідовності – це V_k^-–послідовність, яку визначимо як послідовність чисел, що обчислюються за формулою (3) для від'ємних значень індексів, тобто елементів $v_{-n,k}$, де n і k – цілі додатні числа, при початкових значеннях $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$ для $k = 2$; $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$, $v_{-3,k} = v_{-4,k} = \ldots = v_{-k,k} = 0$ для $k > 2$.

Тоді формула (1), яка дозволяє обчислювати елементи $v_{n,k}$ послідовності V_k^+ з додатними значеннями індексу для зростаючих n, для обчислення елементів $v_{-n,k}$ послідовності V_k^- з від'ємними значеннями індексу, теж для зростаючих n, буде мати такий вигляд

$$v_{-n,k} = g_k \cdot v_{-n-1,k} + g_1 \cdot v_{-n-k,k}. \qquad (4)$$

Теорема 1. Для будь-яких цілих додатних n, m та k

$$v_{-n+m,k} = v_{m+(k-2),k} \cdot v_{-n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot v_{-n-k+i,k}. \qquad (5)$$

Доведення. Проведемо доведення аналітичної залежності (5) індукцією по m.

Оскільки V_k^+–послідовність приймає різні початкові значення для $k = 2$ та $k > 2$, тому основу індукції доведемо окремо для обох цих випадків.

Спочатку доведемо основу індукції для $k = 2$.

В такому випадку аналітична залежність (5) буде мати вигляд

$$v_{-n+m,2} = v_{m,2} \cdot v_{-n,2} + g_1 \cdot v_{m-1,k} \cdot v_{-n-1,k}, \qquad (6)$$

а формула (4) запишіться як $v_{-n,2} = g_2 \cdot v_{-n-1,2} + g_1 \cdot v_{-n-2,2}$.

Покажемо, що (6) виконується для m, що дорівнюють 1 і 2.

$$v_{-n+1,2} = v_{1,2}v_{-n,2} + g_1 v_{0,k} v_{-n-1,2} = g_2 v_{-n,2} + g_1 v_{-n-1,2} = g_2 v_{(-n-1)+1,2} + g_1 v_{(-n-2)-1,2} = v_{-n+1,2}.$$

$$v_{-n+2,2} = v_{2,2}v_{-n,2} + g_1 v_{1,k}v_{-n-1,2}.$$

З (1) $v_{2,2} = g_2 v_{1,2} + g_1 v_{0,2} = g_2^2 + g_1$. Враховуючи це,

$$v_{-n+2,2} = \left(g_2^2 + g_1\right)v_{-n,2} + g_1 g_2 v_{-n-1,2} = g_2^2 v_{-n,2} + g_1 v_{-n,2} + g_1 g_2 v_{-n-1,2} =$$

$$= g_2\left(g_2 v_{-n,2} + g_1 v_{-n-1,2}\right) + g_1 v_{-n,2} = g_2 v_{-n+1,2} + g_1 v_{-n,2} = g_2 v_{(-n-1)+2,2} + g_1 v_{(-n-2)+2,2} = v_{-n+2,2}.$$

Таким чином, основу індукції для $k = 2$ доведено.

Доведемо тепер основу індукції для $k > 2$.

Покажемо, що (5) виконується для m, які дорівнюють 1, 2 , 3, . . . , k

$$v_{-n+1,k} = v_{k-1,k}v_{-n,k} + g_1 v_{k-2,k}v_{-n-k+1,k} + g_1 v_{k-3,k}v_{-n-k+2,k} + \ldots + g_1 v_{0,k}v_{-n-1,k}.$$

Враховуючи значення початкових елементів V_k^+–послідовності, отримаємо $v_{-n+1,k} = g_k v_{-n,k} + g_1 v_{-n-k+1,k}$.

Якщо записати це як $v_{(-n)+1,k} = g_k v_{(-n-1)+1,k} + g_1 v_{(-n-k)+1,k}$, то з (4) видно, що аналітична залежність (5) виконується для $m = 1$.

Аналогічно знайдемо тепер $v_{-n+2,k}$.

$$v_{-n+2,k} = v_{k,k}v_{-n,k} + g_1 v_{k-1,k}v_{-n-k+1,k} + g_1 v_{k-2,k}v_{-n-k+2,k} + g_1 v_{k-3,k}v_{-n-k+3,k} + \ldots + g_1 v_{1,k}v_{-n-1,k}.$$

Виходячи з (1), $v_{k,k} = g_k v_{k-1,k} + g_1 v_{0,k} = g_k v_{k-1,k}$. Враховуючи це, а також значення початкових елементів V_k^+–послідовності, отримаємо

$$v_{-n+2,k} = g_k v_{k-1,k}v_{-n,k} + g_1 v_{k-1,k}v_{-n-k+1,k} + g_1 v_{k-2,k}v_{-n-k+2,k} =$$

$$= v_{k-1,k}\left(g_k v_{-n,k} + g_1 v_{-n-k+1,k}\right) + g_1 v_{-n-k+2,k} =$$

$$= g_k v_{-n+1,k} + g_1 v_{-n-k+2,k} = g_k v_{(-n-1)+2,k} + g_1 v_{(-n-k)+2,k}.$$

Враховуючи (4), переконуємось, що останній вираз дорівнює $v_{-n+2,k}$, тобто аналітична залежність (5) виконується і для $m = 2$.

Роблячи таким же чином, знайдемо $v_{-n+3,k}$.

$$v_{-n+3,k} = v_{k+1,k}v_{-n,k} + g_1 v_{k,k}v_{-n-k+1,k} + g_1 v_{k-1,k}v_{-n-k+2,k} + g_1 v_{k-2,k}v_{-n-k+3,k} +$$

$$+ g_1 v_{k-3,k}v_{-n-k+4,k} + \ldots + g_1 v_{2,k}v_{-n-1,k} =$$

$$= \left(g_k v_{k,k} + g_1 v_{1,k}\right)v_{-n,k} + g_1 v_{k,k}v_{-n-k+1,k} + g_1 v_{k-1,k}v_{-n-k+2,k} + g_1 v_{-n-k+3,k} =$$

$$= v_{k,k}\left(g_k v_{-n,k} + g_1 v_{-n-k+1,k}\right) + g_1 v_{k-1,k}v_{-n-k+2,k} + g_1 v_{-n-k+3,k} =$$

$$= v_{k,k}v_{-n+1,k} + g_1 v_{k-1,k}v_{-n-k+2,k} + g_1 v_{-n-k+3,k} =$$

$$= \left(g_k v_{k-1,k} + g_1 v_{0,k}\right) v_{-n+1,k} + g_1 v_{k-1,k} v_{-n-k+2,k} + g_1 v_{-n-k+3,k} =$$

$$= v_{k-1,k}\left(g_k v_{-n+1,k} + g_1 v_{-n-k+2,k}\right) + g_1 v_{-n-k+3,k} =$$

$$= g_k v_{-n+2,k} + g_1 v_{-n-k+3,k} = g_k v_{(-n-1)+3,k} + g_1 v_{(-n-k)+3,k} = v_{-n+3,k}$$

. . .

$$v_{-n+k,k} = v_{2k-2,k} v_{-n,k} + g_1 v_{2k-3,k} v_{-n-k+1,k} + g_1 v_{2k-4,k} v_{-n-k+2,k} +$$

$$+ g_1 v_{2k-5,k} v_{-n-k+3,k} + \ldots + g_1 v_{k,k} v_{-n-2,k} + g_1 v_{k-1,k} v_{-n-1,k} =$$

$$= \left(g_k v_{2k-3,k} + g_1 v_{k-2,k}\right) v_{-n,k} + g_1 v_{2k-3,k} v_{-n-k+1,k} + g_1 v_{2k-4,k} v_{-n-k+2,k} +$$

$$+ g_1 v_{2k-5,k} v_{-n-k+3,k} + \ldots + g_1 v_{k,k} v_{-n-2,k} + g_1 v_{k-1,k} v_{-n-1,k} =$$

$$= v_{2k-3,k}\left(g_k v_{-n,k} + g_1 v_{-n-k+1,k}\right) + g_1 v_{2k-4,k} v_{-n-k+2,k} +$$

$$+ g_1 v_{2k-5,k} v_{-n-k+3,k} + \ldots + g_1 v_{k,k} v_{-n-2,k} + g_1 v_{k-1,k} v_{-n-1,k} =$$

$$= v_{2k-3,k} v_{-n+1,k} + g_1 v_{2k-4,k} v_{-n-k+2,k} + g_1 v_{2k-5,k} v_{-n-k+3,k} + \ldots + g_1 v_{k,k} v_{-n-2,k} + g_1 v_{k-1,k} v_{-n-1,k} =$$

$$= \left(g_k v_{2k-4,k} + g_1 v_{k-3,k}\right) v_{-n+1,k} + g_1 v_{2k-4,k} v_{-n-k+2,k} +$$

$$+ g_1 v_{2k-5,k} v_{-n-k+3,k} + \ldots + g_1 v_{k,k} v_{-n-2,k} + g_1 v_{k-1,k} v_{-n-1,k} =$$

$$= v_{2k-4,k}\left(g_k v_{-n+1,k} + g_1 v_{-n-k+2,k}\right) + g_1 v_{2k-5,k} v_{-n-k+3,k} + \ldots + g_1 v_{k,k} v_{-n-2,k} + g_1 v_{k-1,k} v_{-n-1,k} =$$

$$= v_{2k-4,k} v_{-n+2,k} + g_1 v_{2k-5,k} v_{-n-k+3,k} + \ldots + g_{1,k} v_{k,k} v_{-n-2,k} + g_1 v_{k-1,k} v_{-n-1,k} = \ldots =$$

$$= v_{k-1,k} v_{-n+k-1,k} + g_1 v_{k-2,k} v_{-n,k} = g_k v_{-n+k-1,k} + g_1 v_{-n,k} .$$

Таким чином основу індукції для $k > 2$ доведено.

Нехай аналітична залежність (5) виконується для $m-k$, $m-k+1$, . . . , $m-1$. Покажемо, що вона виконується для m.

$$v_{-n+m,k} = g_k v_{-n+m-1,k} + g_1 v_{-n+m-k,k} =$$

$$= g_k v_{m-1+(k-2),k} v_{-n,k} + g_1 g_k \sum_{i=1}^{k-1} v_{m-1+(k-2)-i,k} v_{-n-k+i,k} +$$

$$+ g_1 v_{m-k+(k-2),k} v_{-n,k} + g_1^2 \sum_{i=1}^{k-1} v_{m-k+(k-2)-i,k} v_{-n-k+i,k} =$$

$$= g_k v_{m-1+(k-2),k} v_{-n,k} + g_1 g_k v_{m-1+(k-2)-1,k} v_{-n-k+1,k} +$$

$$+ g_1 g_k v_{m-1+(k-2)-2,k} v_{-n-k+2,k} + \ldots + g_1 g_k v_{m-1+(k-2)-(k-1),k} v_{-n-1,k} +$$

$$+ g_1 v_{m-k+(k-2),k} v_{-n,k} + g_1^2 v_{m-k+(k-2)-1,k} v_{-n-k+1,k} +$$

$$+ g_1^2 v_{m-k+(k-2)-2,k} v_{-n-k+2,k} + \ldots + g_1^2 v_{m-k+(k-2)-(k-1),k} v_{-n-1,k} =$$

$$= \left(g_k v_{m-1+(k-2),k} + g_1 v_{m-k+(k-2),k}\right) v_{-n,k} + g_1 \left(g_k v_{m-1+(k-2)-1,k} + g_1 v_{m-k+(k-2)-1,k}\right) v_{-n-k+1,k} +$$

$$+ g_1 \left(g_k v_{m-1+(k-2)-2,k} + g_1 v_{m-k+(k-2)-2,k}\right) v_{-n-k+2,k} + \ldots +$$

$$+ g_1 \left(g_k v_{m-1+(k-2)-(k-1),k} + g_1 v_{m-k+(k-2)-(k-1),k}\right) v_{-n-1,k} =$$

$$= v_{m+(k-2),k} v_{-n,k} + g_1 v_{m+(k-2)-1,k} v_{-n-k+1,k} + g_1 v_{m+(k-2)-2,k} v_{-n-k+2,k} + \ldots + g_1 v_{m+(k-2)-(k-1),k} v_{-n-1,k} =$$

$$= v_{m+(k-2),k} v_{-n,k} + g_1 \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} v_{-n-k+i,k} .$$

Теорему доведено.

Теорема 2. Для будь-яких цілих додатних n, m та k

$$v_{-n-m,k} = v_{-m+(k-2),k} \cdot v_{-n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{-m+(k-2)-i,k} \cdot v_{-n-k+i,k} . \qquad (7)$$

Доведення. Проведемо доведення аналітичної залежності (7) індукцією по m. Покажемо, що (7) виконується для m, які дорівнюють 1, 2 , 3, . . . , k.

$$v_{-n-1,k} = v_{k-3,k} v_{-n,k} + g_1 v_{k-4,k} v_{-n-k+1,k} + \ldots + g_1 v_{-1,k} v_{-n-2,k} + g_1 v_{-2,k} v_{-n-1,k} .$$

Враховуючи значення початкових елементів, отримаємо

$$v_{-n-1,k} = g_1 g_1^{-1} v_{-n-1,k} = v_{-n-1,k} .$$

Знайдемо тепер $v_{-n-2,k}$

$$v_{-n-2,k} = v_{k-4,k} v_{-n,k} + g_1 v_{k-5,k} v_{-n-k+1,k} + \ldots +$$

$$+ g_1 v_{-1,k} v_{-n-3,k} + g_1 v_{-2,k} v_{-n-2,k} + g_1 v_{-3,k} v_{-n-1,k} = g_1 v_{-2,k} v_{-n-2,k} = v_{-n-2,k}$$

. . .

$$v_{-n-k,k} = v_{-2,k} v_{-n,k} + g_1 v_{-3,k} v_{-n-k+1,k} + \ldots + g_1 v_{-k,k} v_{-n-2,k} + g_1 v_{-k-1,k} v_{-n-1,k} =$$

$$= v_{-2,k} v_{-n,k} + g_1 v_{-k-1,k} v_{-n-1,k} = g_1^{-1} v_{-n,k} + g_1 \left(-g_k g_1^{-2}\right) v_{-n-1,k} = \frac{v_{-n,k} - g_k v_{-n-1,k}}{g_1} = v_{-n-k,k} .$$

Нехай залежність (7) виконується для $m+1$, $m+2$, . . . , $m+k$. Покажемо, що вона виконується для m.

$$v_{-n-m,k} = g_k v_{-n-m-1,k} + g_1 v_{-n-m-k,k} =$$

$$= g_k v_{-m-1+(k-2),k} v_{-n,k} + g_1 g_k \sum_{i=1}^{k-1} v_{-m-1+(k-2)-i,k} v_{-n-k+i,k} +$$

$$+ g_1 v_{-m-k+(k-2),k} v_{-n,k} + g_1^2 \sum_{i=1}^{k-1} v_{-m-k+(k-2)-i,k} v_{-n-k+i,k} =$$

$$= g_k v_{-m-1+(k-2),k} v_{-n,k} + g_1 g_k v_{-m-1+(k-2)-1,k} v_{-n-k+1,k} +$$

$$+ g_1 g_k v_{-m-1+(k-2)-2,k} v_{-n-k+2,k} + \ldots + g_1 g_k v_{-m-1+(k-2)-(k-1),k} v_{-n-1,k} +$$

$$+ g_1 v_{-m-k+(k-2),k} v_{-n,k} + g_1^2 v_{-m-k+(k-2)-1,k} v_{-n-k+1,k} +$$

$$+ g_1^2 v_{-m-k+(k-2)-1,k} v_{-n-k+1,k} + \ldots + g_1^2 v_{-m-k-1,k} v_{-n-1,k} =$$

$$= \left(g_k v_{-m-1+(k-2),k} + g_1 v_{-m-k+(k-2),k}\right) v_{-n,k} +$$

$$+ g_1 \left(g_k v_{-m-1+(k-2)-1,k} + g_1 v_{-m-k+(k-2)-1,k}\right) v_{-n-k+1,k} +$$

$$+ g_1 \left(g_k v_{-m-1+(k-2)-2,k} + g_1 v_{-m-k+(k-2)-2,k}\right) v_{-n-k+2,k} + \ldots +$$

$$+ g_1 \left(g_k v_{-m-1+(k-2)-(k-1),k} + g_1 v_{-m-k+(k-2)-(k-1),k}\right) v_{-n-1,k} =$$

$$= v_{-m+(k-2),k} v_{-n,k} + g_1 v_{-m+(k-2)-1,k} v_{-n-k+1,k} +$$

$$+ g_1 v_{-m+(k-2)-2,k} v_{-n-k+2,k} + \ldots + g_1 v_{-m+(k-2)-(k-1),k} v_{-n-1,k} =$$

$$= v_{-m+(k-2),k} v_{-n,k} + g_1 \sum_{i=1}^{k-1} v_{-m+(k-2)-i,k} v_{-n-k+i,k} \,.$$

Це і вимагалося довести.

В окремому випадку, коли $m = n$ аналітична залежність (7) буде мати такий вигляд

$$v_{-2n,k} = v_{-n+(k-2),k} \cdot v_{-n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{-n+(k-2)-i,k} \cdot v_{-n-k+i,k} \,. \qquad (8)$$

Висновки

Проведено дослідження рекурентної V_k –послідовності, що складається з двох послідовностей V_k^+ і V_k^-. Отримано властивості, що дозволяють здійснювати прискорене обчислення елементів цієї послідовності, а саме елементів $v_{-n+m,k}$ та $v_{-n-m,k}$.

Отримані властивості дозволили розширити математичний апарат рекурентних V_k –послідовностей щодо можливості побудови асиметричних криптографічних методів різного призначення, зокрема методів автентифікації та цифрового підписування.

Список літератури

1. Маркушевич, А.И. Возвратные последовательности [Текст] : научно-популярная литература / А.И. Маркушевич. — 3-е изд. — М. : Физ.-мат. лит.: Наука, 1983. — 48 с.
2. Воробьев, Н.Н. Числа Фибоначчи [Текст] / Н.Н. Воробьев. — 6-е изд., доп. — М. : Наука, 1992. — 192 с.
3. Яремчук, Ю.Є. Криптографічні методи та засоби шифрування інформації на основі рекурентних послідовностей [Текст] : монографія / Ю.Є. Яремчук. — Вінниця : Книга-Вега, 2002. — 136 с.

АНАЛИТИЧЕСКИЕ ЗАВИСИМОСТИ УСКОРЕННОГО ВЫЧИСЛЕНИЯ ЭЛЕМЕНТОВ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ ВОЗМОЖНОСТИ ПОСТРОЕНИЯ МЕТОДОВ АУТЕНТИФИКАЦИИ И ЦИФРОВОГО ПОДПИСЫВАНИЯ

Ю.Е. Яремчук

Винницкий национальный технический университет,
ул. Хмельницкое шоссе, 95, Винница, 21021, Украина; e-mail: yurevyar@vntu.net

Проведено исследование рекуррентных V_k –последовательностей и получены аналитические зависимости ускоренного вычисления элементов этой последовательности. Установлены свойства вычисления элементов $v_{-n+m,k}$ и $v_{-n-m,k}$. Это позволило расширить математический аппарат рекуррентных V_k –последовательностей для возможности построения асимметричных криптографических методов различного назначения, в частности методов аутентификации и цифрового подписания.

Ключевые слова: рекуррентные последовательности, аналитические зависимости, криптография, аутентификация, цифровое подписание

ANALYTIC DEPENDENCES OF FAST COMPUTATION OF THE TERMS OF RECURRENT SEQUENCES TO BE USED IN THE DEVELOPMENT OF AUTHENTICATION AND DIGITAL SIGNATURE TECHNIQUES

Yuri E. Yaremchuk

Vinnytsia National Technical University,
95 Khmelnytske shose, Vinnytsia, 21021, Ukraine; e-mail: yurevyar@vntu.net

Recurrent V_k sequences were investigated and analytic dependences related to fast computation of the terms of such a sequence obtained. The features of computation of $v_{-n+m,k}$ and $v_{-n-m,k}$ terms were established. This made it possible to expand the mathematical apparatus for recurrent V_k sequences that may be used to develop asymmetric cryptographic techniques of various purposes, including authentication and digital signature techniques.

Keywords: recurrent sequences, analytical dependences, cryptography, authentication, digital signature

Mathematics Subject Classification (2010) 68M10

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 4, pp. 314-322

PROBABILISTIC METHODS OF CONTROLLING EMISSIONS IN THE RADIO NETWORK

Mykola P. Karpinski[1], Oleksandr G. Korchenko[2], Stanisław W. Rajba[1]

[1] University of Bielsko-Biala,
ul. Willowa, 2, 43-309 Bielsko-Biala, Poland; e-mail: rajbas@ath.bielsko.pl
[2] National Aviation University,
1 Kosmonavta Komarova Ave., Kyiv, 03680, Ukraine

This paper presents a method of probabilistic radio transmission control in wireless sensor networks (WSN). Specified probability of collision-free conditions in the network transmission of the single-hop type. We propose the concept of WSN with random moments of time-signal emissions with a one-way transmission using one radio frequency. We use Poisson Arrivals See Time Average (PASTA) for modeling probability of a collision during the transmission of the radio network to control the correct network operation. The proposed model WSN network access allows the improvement of the reliability and security of information.
Key words: Wireless Sensor Network, Poisson Arrivals See Time Averages (PASTA system), probability of collision, random control

Problem formulation

In the paper we present problems of radio communications for wireless measurement networks. We analyze the random access control for wireless measurement nodes by examining the conditions of communication, depending on their number, average working time of transmission based on the previously proposed algorithm which uses a Poisson stream. In particular, we estimate probabilities of the determined number of times messages by nodes that are in a collision during communication based on the number of nodes and other network communication parameters. We estimate both unconditional and conditional probability on the assumption of a given number of sensor transmissions. It also provides an estimation of the expected number of nodes that are in collision and the variance. Proposed probabilistic model can increase the reliability of the network and increase the security of the information.

Evaluation of the recent publications in explored issue

Wireless sensor networks create a new quality in modern systems, acquisition and transfer of information (Wireless Sensor Network – WSN). Implementation of WSN puts an entirely new requirements for the radio communication and control processes, which manage to meet the increasingly sophisticated technologies [1]. The use of radio communications in the network-type convergecast is much more difficult than in a well operated radio broadcasting systems (broadcasting, television, satellite GPS, etc.) and conciliation point-to-point (cellular telephone). The main difficulty lies in the organization of radio traffic which is represented by the controlled access to the transmission medium which in other terms represents the surrounding space. In the surrounding area, an active space in the radio communication is defined by the value of the electric field which produces a transmitting device at a given point of space. There can be only one sender at a particular frequency. As

we know from Maxwell's equations [2]. In vacuum by physical constants permittivity of vacuum $\varepsilon_0 = 8.854 \cdot 10^{-12}$ F/m and the magnetic permeability of vacuum $\mu_0 = 4\pi \cdot 10^{-7}$ H/m) defines the vacuum as a transmission medium impedance $Z_0 = \sqrt{\frac{\mu_0}{\varepsilon_0}} = 377\Omega$. In the terrestrial conditions of the troposphere, the situation is quite similar, but each object field and the Earth itself has a very different electrical and magnetic parameters. This results in significantly different impedances of these centers and their contact with the air comes to the many reflections of radio waves. Reflections considering additionally the principle of Huygens created another problem in the radio transmission – the multipath transmission and thus it created a problem of the multi-way loss. In the air we observe a large heterogeneity due to the different temperatures of the different air, water vapor content, rain, snow, pollination layers, the state of the air ionization which constitutes the source of refraction and transmission path of the increased attenuation [1]. Designing radio communication types, these phenomena must always be taken into account. In case of wireless network design aggregation of all these phenomena effectively impedes proper communication and discussion in case of a success or a failure of the radio transmission. The fundamental problem in WSN network concerns the controlling of the network access to the information mouth (sink), so that the transmission medium is occupied at a certain frequency and at a given point of time by only one sender [3]. In an environment covered by a wireless network must be developed ways to control access of each node – network components that information seamlessly redirected to the mouth (sink) [4–7]. It should be noted that the correct reception depends not only on the resolution of the network itself, but also on external influence of other radio communication types. The subject of this paper concerns the issue of controlling the node access to the base station in the single-hop type wireless networks [8] applying random methods.

This applies in particular to the organization and process control of the radio emission with an aim to obtain data on the deliberate quality level under all relevant physical conditions of the wireless network work [9].The paper [10] presents a random access algorithm for a class of wireless network measurement and the analysis of working conditions. The concept of the convergecast networks (sink) (e.g., wireless sensor network (WSN)) involves the fact that the information sources distributed in space (fixed and mobile), which are considerably numerous, communicate with the information directly to the base station (the mouth of the information) [11]. These are networks of single-hop. Networks of the single-hop is a traditional star topology in which each link can be implemented duplex or Simple, depending on the needs and dispose the number of required frequency channels (frequency dispose). If the network is organized in a way that it is capable to provide information through other nodes, somewhat indirectly, than the networks are multi-hop. Network of the multi-hop architecture is the most common type mesh [12, 13]. Network architecture of the multi-hop is more complex. It is also a sophisticated hardware and requires complex control algorithms. However, it has many advantages over a solution of the single-hop. For example, the possibility of reconfiguration in case of a failure or unavailability of certain nodes, allows the range enlargement within the same low-power transmitting nodes [14]. It is assumed that the various communication nodes (associated with the sensors) can move in a field study of the physical effects and are controlled by sensors (they are mobile). This means that it will require a dynamic reorganization of the network architecture.

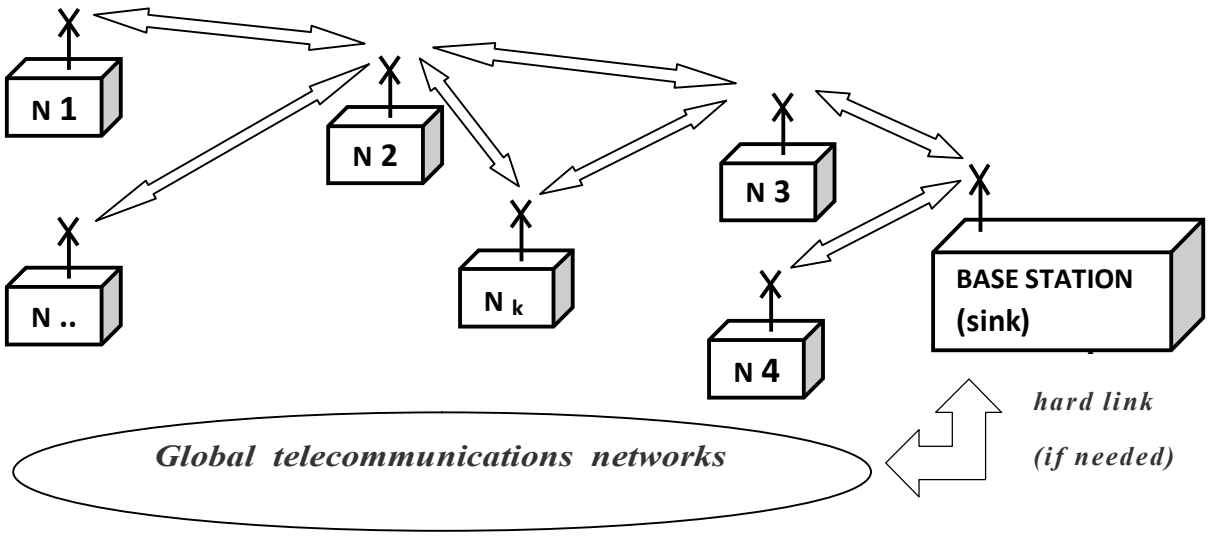


Fig. 1. Wireless network multi-hop

The WSN network conditions limiting the power supply and energy supply sources capacity constitute the primary problem of determining the solutions further consequences [15]. For this reason, frequent solution is the multi-hop topology (retransmission from node to node until the sink), than the single-hop requires more energy for the radio transmission. The multi-hop network requires more complex communication algorithms. Low level of radiated power, can be an advantage on the one hand, but on the other hand it also creates communication problems. Limitations of the power supply require incorporation mechanisms for "savings" that allow the user the possibility of a longer «life» at the expense of reducing the network bandwidth, or increasing the transmission delay [16, 17]. WSN design in terms of access control nodes to the mouth of the data (sink) requires the following conditions [6–8, 15]:

- Bands and frequency communication;
- Hardware limits;
- Restrictions on the external (environmental);
- The demand for power supply (e.g. for communication and data processing);
- Scalability;
- Range of fault tolerance.

Characteristic features of the networks topology WSN in the access control

It is assumed that the various communication nodes (associated with the sensors) that can move in a field study of the physical effects are controlled by the sensors. Thus, the mobility of nodes is assumed, which often entails changes in the network configuration, and in particular, changes in the conditions required for the propagation of electromagnetic waves. These requirements impose very significant and needed characteristics of the wireless network nodes [3] as follows: algorithms and protocols must possess the ability to self-organization. This means that the node must be equipped with the hardware in the processor, which will implement very complex algorithms, often operating under changing environmental conditions of measurement [18–21]. The following is a random solution to control access to the network architecture of the single-hop assumption implementing the structural simplicity of nodes and limiting the solution to use only one frequency channel [11]. The solution for many applications, WSN has many desirable advantages. Theoretical principles of the random access control model.

Probabilistic network model

We consider a network consisting of n sensors which are able to send information about the measured physical magnitude on one selected radio frequency to the receiving base, quite independently of each other. Duration of communication protocol is t_p, the sensors send the information to the receiving point in randomly selected moments, every T s. at a average.

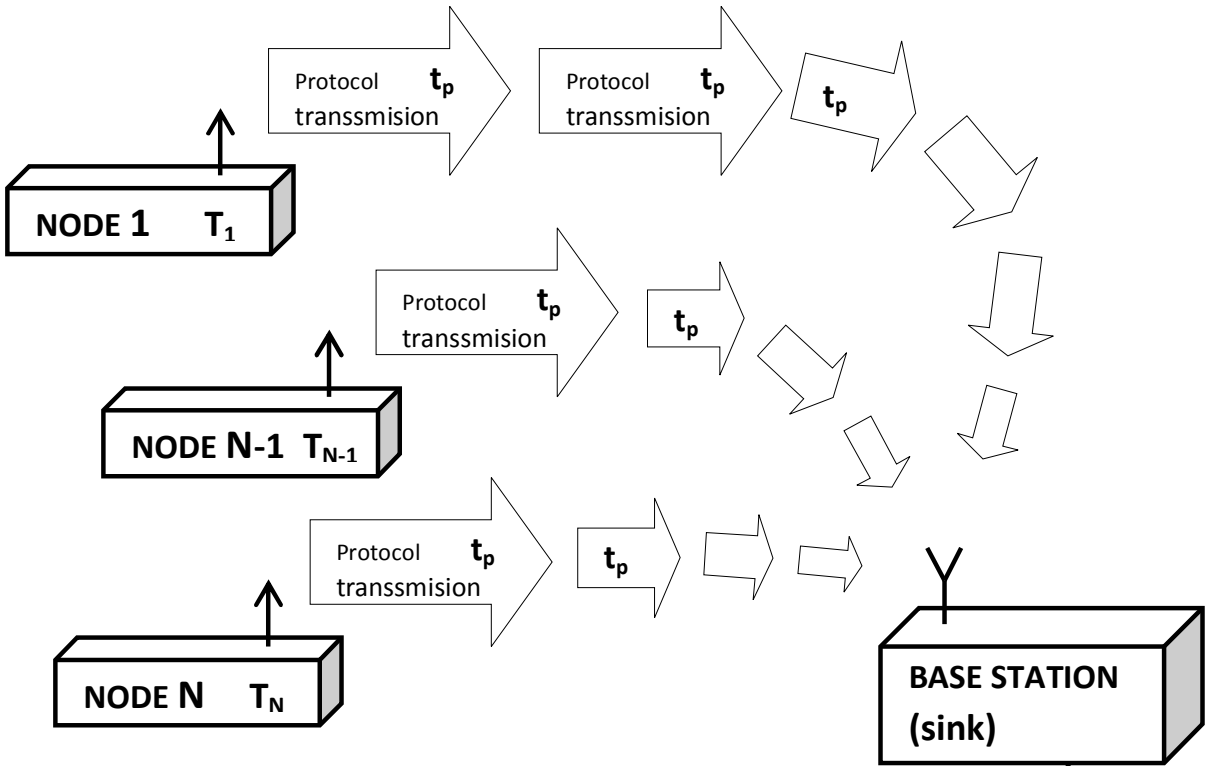


Fig. 2. Model analyzed single-hop network with one-way transmission

Beginning and cessation of transmission of a particular sensor takes place in random moments of time but these moments are relatively rare. It is a one-way transmission, i.e. from sensors to the receiving base. The sensors are completely independent from each other and their on or off state is of no influence on the operation of the network. All the sensor- senders or a part of them may be mobile provided that their senders have been left within the radio range of the receiving base. If one or more senders start sending while protocol transmission of t_p time is going on from another sensor, then such a situation is called collision. Collision excludes the possibility of the correct receiving of information by the receiving base. Such a disturbed signal is ignored. The receiving base rejects the erroneous message and waits for a retransmission to be made after the average time T. We must accept a certain loss of information in exchange for simplicity in respect of both system and equipment.

We used in modeling our wireless network a Poisson process. Poisson process is the stochastic process in which events occur continuously and independently of one another. Mathematically the process N is described by the so called counter process N_t or $N(t)$(see [22], and [10, 11]) of rate $\lambda > 0$. The counter tells the number of events that have occurred in the interval $[0, t]$ $(t \geq 0)$. N has independent increments (the number of occurrences counted in disjoint intervals are independent from each other), such that $N(t) - N(s)$ has the Poisson ($\lambda(t-s)$) distribution, for $t \geq s \geq 0$, $j = 0,1,2,\ldots$,

$$P\{N(t)-N(s)=j\}=e^{-\lambda(t-s)}\frac{[\lambda(t-s)]^j}{j!}. \tag{1}$$

A counting process has two corresponding random sequences, the sequence of count times (T_j) and the sequence of inter count times (U_j), such that $U_1=T_1$ and $U_j=T_j-T_{j-1}$, for $j\geq 2$. It is well known (see [22]) that N is a Poisson process with the rate $\lambda>0$ if and only if the inter count times $U_1,U_2,...$are mutually independent and each is exponentially distributed with parameter λ (mean $1/\lambda$).

Let us state our main assumptions. There are n identical sensors observing a dynamical system and reporting to a central location over the wireless sensor network with one radio channel. For simplicity, we assume our sensor network to be a single hop network with the star topology. We also assume that every node (sender-sensor, shortly sensor) has always packet ready for transmission. We assume that sensors send probe packets at Poissonian times. The average time between sending (the wake-up- times) of a sensor is T (the epoch period), and the duration of the on-time is t_p (the awake interval). Assume that the wake-up-times corresponding to sensors are independent from each other. Let N be the Poisson process representing the time counter of sending sensors. Let $T_1,T_2,\ldots$ be the sending times (the wake-up- times) of sensors, $U_1,U_2,\ldots$ the inter sending times. Then the average time between sending of sensors is T/n, the average number of sending sensors in the time interval of T length equals to n. We say that a collision occurs in the time interval of t_p length, if at least two sensors start sending within this interval. We say that a collision occurs in time interval s, if there exist at least two sensors which start sending within this interval with the difference between the beginning of their sending time not exceeding the value of t_p. Then the Poisson process N has the rate $\lambda=n/T$. By (1)

$$P(N_t=j)=e^{-\lambda t}\frac{[\lambda t]^j}{j!}(j=0,1,\ldots). \tag{2}$$

In [11, 23] we give the theorem on the probability of collisions in the interval of s length in the case $s>t_p$. In the following theorem we give the lower and upper estimations of the conditional probability of the number sensor transmissions in collision in the interval of s length, assuming that the number of sensor transmissions that have occurred in the interval of s length $(s>t_p)$ equals j. Let Y_s be the number sensor transmissions in collision, in the interval of s length.

Theorem 1. Let $s>t_p$. Then we have

$$\left(j\frac{t_p}{s}\right)^{\kappa-1}\left(1-j\frac{t_p}{s}\right)^{j-\kappa}\leq P(Y_s=\kappa/N(s)=j)\leq\left(j\frac{t_p}{s}\right)^{\left[\frac{\kappa+1}{2}\right]}\left(1-\frac{t_p}{s}\right)^{j-\left[\frac{\kappa+1}{2}\right]}. \tag{3}$$

Proof: Let $2\leq i_2,\ i_3,\ .....,\ i_j\leq j$, be such that $U_{i_2}\leq U_{i_3}\leq\ldots\leq U_{i_j}$. Since $Y_s=\kappa$, there exists $\left[\frac{\kappa+1}{2}\right]\leq k\leq\kappa-1$, such that $U_{i_{k+1}}<t_p\leq U_{i_{k+2}}$. Consequently, we obtain that

$$P(U_2<t_p,U_3<t_p,...,U_\kappa<t_p,U_{\kappa+1}\geq t_p,...,U_j\geq t_p)\leq P(Y_s=\kappa/N(s)=j)\leq$$

$$\le P\left(U_2 < t_p,\ ...,\ U_{\left[\frac{\kappa+1}{2}\right]+1} < t_p, U_{\left[\frac{\kappa+1}{2}\right]+2} \ge t_p, ..., U_j \ge t_p\right).$$

This implies (3).

In the next theorem we estimate the unconditional probability of the number sensor transmissions in collision in the interval of s length $(s > t_p)$.

Theorem 2. Let $s > t_p$. Then we have

$$\sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \frac{\left(n\frac{s}{T}\right)^j}{j!}\left(j\frac{t_p}{s}\right)^{\kappa-1}\left(1-j\frac{t_p}{s}\right)^{j-\kappa} \le P(Y_s=\kappa) \le \sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \frac{\left(n\frac{s}{T}\right)^j}{j!}\left(j\frac{t_p}{s}\right)^{\left[\frac{\kappa+1}{2}\right]}\left(1-\frac{t_p}{s}\right)^{j-\left[\frac{\kappa+1}{2}\right]}.$$

In the next theorem we give estimations of the expected value and the variance, respectively.

Theorem 3. Let $s > t_p$. Then we have

$$\sum_{\kappa=2}^{\infty}\kappa\sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \frac{\left(n\frac{s}{T}\right)^j}{j!}\left(j\frac{t_p}{s}\right)^{\kappa-1}\left(1-j\frac{t_p}{s}\right)^{j-\kappa} \le EY_s \le \sum_{\kappa=2}^{\infty}\kappa\sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \frac{\left(n\frac{s}{T}\right)^j}{j!}\left(j\frac{t_p}{s}\right)^{\left[\frac{\kappa+1}{2}\right]}\left(1-\frac{t_p}{s}\right)^{j-\left[\frac{\kappa+1}{2}\right]},$$

$$\sum_{\kappa=2}^{\infty}\kappa^2\sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \frac{\left(n\frac{s}{T}\right)^j}{j!}\left(j\frac{t_p}{s}\right)^{\kappa-1}\left(1-j\frac{t_p}{s}\right)^{j-\kappa} - \left[\sum_{\kappa=2}^{\infty}\kappa\sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \frac{\left(n\frac{s}{T}\right)^j}{j!}\left(j\frac{t_p}{s}\right)^{\left[\frac{\kappa+1}{2}\right]}\left(1-\frac{t_p}{s}\right)^{j-\left[\frac{\kappa+1}{2}\right]}\right]^2 \le$$

$$\le D^2(Y_s) \le \sum_{\kappa=2}^{\infty}\kappa^2\sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \frac{\left(n\frac{s}{T}\right)^j}{j!}\left(j\frac{t_p}{s}\right)^{\left[\frac{\kappa+1}{2}\right]}\left(1-\frac{t_p}{s}\right)^{j-\left[\frac{\kappa+1}{2}\right]} - \left[\sum_{\kappa=2}^{\infty}\kappa\sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \frac{\left(n\frac{s}{T}\right)^j}{j!}\left(j\frac{t_p}{s}\right)^{\kappa-1}\left(1-j\frac{t_p}{s}\right)^{j-\kappa}\right]^2.$$

Below we give an example of calculating estimates of the expected value (the lower and upper) for a wireless network with random access, where the average transmission time is $T = 10$ s, the number of nodes is $n = 5$ and the observation time is $s = 180$ s.

Namely: $3.1985376 \cdot 10^{-5} \le EY_S \le 3.1986410 \cdot 10^{-5}$.

The calculation shows that there is approximately 3.1986 collisions at 10^5 intervals of length s in which the phenomenon has been studied. As seen in these conditions, the network will work very well. For the same sample network parameters were calculated upper and lower estimation of the variance: $6.39705 \cdot 10^{-5} \le D^2(Y_S) \le 6.39746 \cdot 10^{-5}$.

It is easy to see from both the estimation of the expected value and variance, the difference between the lower and upper estimate is low, they differ only in fifth place significant digits. So I can tell from the error estimates in the examples is small, the order of 10^{-9}. Calculating the standard deviation (dispersion) $D(Y_S)$ as $D(Y_S) = \sqrt{D^2(Y_S)}$ and then by calculating the coefficient of variation (i.e. dispersion-to-mean ratio) as $DMR(Y_S) = \frac{D(Y_S)}{EY_S}$, we obtain:

$$\frac{D_L}{E_U} \le \frac{D(Y_S)}{EY_S} \le \frac{D_U}{E_L},$$

where

D_L — lower estimate of the standard deviation,

D_U — upper estimate of the standard deviation,

E_L — lower estimate of the expected value,

E_U — upper estimate of the expected value.

All the above estimates upper and lower expected value and variance are given in Theorem 4. For the given example, we obtain the following estimates of value $DMR(Y_S)$: $1.99993 \le DMR(Y_S) \le 2.00012$. Coefficient of variation is around 2, the standard deviation of radio collisions occurring is very small, about two times higher than the expected value, which is very small (approximately $3.198 \cdot 10^{-5}$). This result fully confirms the assumption of random network control algorithm.

Conclusions

In summary it can be said that a significant simplification of the nodes structure (simplex transmission on one frequency), the simplification algorithm simplifies handling radio traffic. Moreover, communication protocols and reduced energy consumption of nodes (node extends the lifespan of the network) have a significant impact on the improving of the network reliability, as well as significantly increase the security of the information transmitted on the network. Further research concerning the number of nodes that are in collision in WSN with the random access networks will be conducted in the networks with the nodes division into groups comprising different average time between transmissions.

References

1. Курітник, І.П. Безпровідна трансляція інформації [Текст] / Ігор Петро Курітник, Микола Карпінський ; пер. з пол. магістра Володимира Карпінського та магістра Уляни Яциковської. — Т. : Крок, 2010. — 376 с.
2. Zahn, M. Pole elektromagnetyczne / M. Zahn, P. Stasiak, A. Bechler. — Warszawa: PWN, 1989. — 782 s.
3. Akyildiz, I.F. Wireless sensor networks: a survey / I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci // Computer networks. — 2002. — Vol. 38, Iss. 4. — PP. 393–422.
4. Culler, D. Guest Editors' Introduction: Overview of Sensor Networks / D. Culler, D. Estrin, M. Srivastava // Computer. — 2004. — Vol. 37, No. 8. — PP. 41–49.
5. Gupta, P. The capacity of wireless networks / P. Gupta, P.R. Kumar // IEEE Transactions on Information Theory. — 2000. — Vol. 46, Iss. 2. — PP. 388–404.
6. Xue, G. On current areas of interest in wireless sensor networks designs / G. Xue, H. Hassanein // Computer Communications. — 2006. — Vol. 29, Iss. 4. — PP. 409-412.
7. Misra, S. Algorithmic and theoretical aspects of wireless ad hoc and sensor networks / S. Misra, S.C. Misra, I. Woungang // Computer Communications. — 2008. — Vol. 31, Iss. 4. — PP. 655–658.
8. Chatzigiannakis, I. Efficient data propagation strategies in wireless sensor networks using a single mobile sink / I. Chatzigiannakis, A. Kinalis, S. Nikoletseas // Computer Communications. — 2008. — Vol. 31, Iss. 5. — PP. 896–914.
9. Кравчук, С.О. Модель прямого каналу системи широкосмугового доступу з диференційованими послугами гарантованої передачі / С.О. Кравчук // Наукові вісті НТУУ «КПІ». — 2008. — № 1. — С. 5–12.
10. Rajba, S. Wireless sensor convergecast based on random operations procedure / S. Rajba, T. Rajba // Pomiary, Automatyka, Kontrola. — 2010. — R. 56, Nr. 3. — PP. 255–258.

11. Rajba, S. Wireless sensor network with random sending / S. Rajba, T. Rajba // Knowledge in Telecommunication Technologies and Optics: Proceedings of the 11th International Conference : KTTO 2011 : June 22-24, 2011, Szczyrk, Poland. — 2011. — PP. 170–175.
12. Joo, C. Performance of Random Access Scheduling Schemes in Multi-Hop Wireless Networks / C. Joo, N.B. Shroff // Proceedings of Fortieth Asilomar Conference on Signals, Systems and Computers, 2006. ACSSC'06. — 2006. — PP. 1937–1941.
13. Rajba, P. Efektywne szukanie stacji w sieciach o topologii kraty / P. Rajba // Przegląd Elektrotechniczny. — 2009. — R. 85, Nr. 4. — PP. 108–115.
14. Brzezinski, A. Enabling Distributed Throughput Maximization in Wireless Mesh Networks: A Partitioning Approach / A. Brzezinski, G. Zussman, E. Modiano // MobiCom'06 Proceedings of the 12th annual international conference on Mobile computing and networking, September 23-26, 2006, Los Angeles, California, USA. — 2006. — PP. 26–37.
15. Zorzi, M. Error Control and Energy Consumption in Communications for Nomadic Computing / M. Zorzi, R.R. Rao // IEEE Transactions on Computers. — 1997. — Vol. 46, No. 3. — PP. 279–289.
16. Pemmaraju, S.V. Energy conservation via domatic partitions / S.V. Pemmaraju, I.A. Pirwani // Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing, MobiHoc'06. — 2006. — PP 143–154.
17. Chen, B. Span: An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks / B. Chen, K. Jamieson, H. Balakrishnan, R. Morris // Wireless Networks. — 2002. — Vol. 8, Iss. 5. — PP. 481–494.
18. Jurdziński, T. Probabilistic Algorithms for the Wake-Up Problem in Single-Hop Radio Networks / T. Jurdziński, G. Stachowiak // Theory of Computing Systems. — 2005. — Vol. 38, Iss. 3. — PP. 347–367.
19. Kumar, V.S.A. Algorithmic Aspects of Capacity in Wireless Networks / V.S.A. Kumar, M.V. Marathe, S. Parthasarathy, A. Srinivasan // Proceedings of the 2005 ACM SIGMETRICS international conference on Measurement and modeling of computer systems. — New York, 2005. — PP. 133–144.
20. Liu, B. On the Capacity of Hybrid Wireless Networks / B. Liu, Z. Liu, D. Towsley // Proceedings of the Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'03). — 2003. — Vol. 2. — PP. 1543–1552.
21. Wattenhofer, H. Algorithms for Wireless Sensor Networks (Tutorial) / H. Wattenhofer // Lecture Notes in Computer Science. — 2006. — Vol. 3868. — P. 2.
22. Feller, W. Wstęp do rachunku prawdopodobieństwa / W. Feller, R. Bartoszyński, B. Bielecki. — Warszawa: Państwowe Wydawnictwo Naukowe, 2006. — 456 p.
23. Rajba, S. The probability of collisions in Wireless Sensor Network with random sending / S. Rajba, T. Rajba // Przegląd Elektrotechniczny. — 2012. — Nr 9a. — PP. 243–246.

ІМОВІРНІСНІ МЕТОДИ КЕРУВАННЯ ПЕРЕДАВАННЯМ В РАДІОМЕРЕЖІ

М.П. Карпінський[1], О.Г. Корченко[2], С.В. Райба[1]

[1] University of Bielsko-Biala,
ul. Willowa, 2, 43-309 Bielsko-Biala, Poland; e-mail: rajbas@ath.bielsko.pl
[2] Національний авіаційний університет,
просп. Космонавта Комарова, 1, Київ, 03680, Україна

У статті представлено імовірнісне керування радіопередачею в безпровідних сенсорних мережах (БСМ). Визначено імовірність стану без колізій в мережевій передачі одновузлового типу. Нами запропоновано концепцію БСМ з випадковими моментами передавання сигналів часу з односторонньою передачею, застосовуючи одну радіочастоту. Нами використовується середнє значення за час спостереження надходження пуассонівського потоку (PASTA) для моделювання імовірності появи колізії під час передавання в радіомережі з метою контролю правильності роботи мережі. Запропонована модель мережевого доступу дозволяє підвищити надійність і безпеку інформації.

Ключові слова: безпровідна сенсорна мережа, середнє значення за час спостереження надходження пуассонівського потоку (система PASTA), імовірність появи колізії, випадкове керування

ВЕРОЯТНОСТНЫЕ МЕТОДЫ УПРАВЛЕНИЯ ПЕРЕДАЧЕЙ В РАДИОСЕТИ

Н.П. Карпинский[1], А.Г. Корченко[2], С.В. Райба[1]

[1] University of Bielsko-Biala,
ul. Willowa, 2, 43-309 Bielsko-Biala, Poland; e-mail: rajbas@ath.bielsko.pl
[2] Национальный авиационный университет,
просп. Космонавта Комарова, 1, Киев, 03680, Украина

В статье представлено вероятностное управление радиопередачей в беспроводных сенсорных сетях (БСС). Определена вероятность состояния без коллизий в сетевой передаче одноузлового типа. Предложена концепция БСС со случайными моментами передачи сигналов времени с односторонней передачей, используя одну радиочастоту. В работе используется среднее значение за время наблюдения поступления пуассоновского потока (PASTA) для моделирования вероятности появления коллизии во время передачи в радиосети с целью контроля корректной работы сети. Предложенная модель сетевого доступа позволяет повысить надежность и защиту информации.

Ключевые слова: беспроводная сенсорная сеть, среднее значение за время наблюдения поступления пуассоновского потока (система PASTA), вероятность появления коллизии, случайное управление

Mathematics Subject Classification (2010) 94A60

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 4, pp. 323-330

A TECHNIQUE TO ESTIMATE A STEGANOGRAPHIC CAPACITY OF A STEGO CHANNEL FORMED WITH LSB MODIFICATION APPROACH

Ivan I. Bobok

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: onu_metal@ukr.net

A polynomial technique for estimating a steganographic capacity (SC) of a stego channel formed with least-significant-bit (LSB) modification approach was developed within the framework of steganalysis efficiency-improvement job based on general approach to analysis of the status and performance of information systems. Digital images of lossy compression formats were used as cover objects. The technique developed is important to implement decoding of additional data embedded in a cover object. With respect to stego transformation with LSB approach, a relationship between the rate-of-change of smallest singular values of image blocks (i.e., submatrices) and SC value was established. It was empirically established that the absolute error of SC obtained by the developed technique is essentially independent of its true value, but dependent on the number of stego messages (images) subjected to analysis.

Keywords: steganalysis, steganographic capacity, singular values, digital image, matrix

Introduction

The state-of-art steganography, recent scientific activity in this area, and publications of some results in open-access sources have boosted the chance of various anti-state and terrorist structures to implement the new developments. Therefore, the issues related to increase in efficacy of steganalysis are of supreme importance [1, 2].

The main problems of steganalysis are:

- Detection of steganographically embedded data, and, if detected;
- Decoding the data embedded inside a cover object.

Currently, the first of these two problems remains the most important, and, when developing the techniques to solve it, a special attention is given to minimization of type-I errors [3].

Today, when organizing a stego communication channel, the most widely used approach is that of LSB modification [1]. However, in current use, it involves some specificity as follows: embedding additional data (AD) in a cover object is often implemented with a low steganographic capacity (SC) [1, 2], thus hampering detection of AD with steganalysis algorithms.

In [4], the author presented a steganalysis technique to detect the embedded data produced with LSB approach, that technique being efficient also for low SC. Digital images (DI) of lossy compression formats were used as cover objects. The basic idea of the technique developed based on general approach to analysis of the status and performance of information systems [4] involves estimating the rate-of- change of two smallest singular values (SVs) of blocks (submatrices) of DI under test, these smallest SVs obtained as a result of standard decomposition [5]. The conclusion of the presence or absence of embedded AD is made after comparison of the argument of the histogram of angular factors interpolating the 7^{th} and 8^{th} SVs of all DI blocks in which the global histogram maximum is achieved, with an

experimentally set threshold value. Such use of the technique ensures effective detection of the result of stego embedding with LSB approach [3]; however, to perform decoding operations, it is important to estimate the SC value of a stego channel used for transfer of AI.

Therefore, development of a technique to estimate a steganographic capacity of a least-significant-bit approach with the performed stego transformation is deemed appropriate for organization of steganalysis process.

Aim of the Work and Problem Setting-up

The *aim* of the research is to develop a technique to estimate a steganographic capacity of a stego channel formed with least-significant-bit (LSB) modification approach based on the earlier developed steganalysis technique, by estimating the rate-of-change of two smallest SVs of DI blocks obtained with standard DI matrix decomposition. To accomplish the purpose, the following *problems* are to be solved:

- Establishing qualititative features of SVs of stego message (SM) blocks with increase in SC value;
- Establishing quantitative features of SVs of stego message (SM) blocks with increase in SC value;
- Ensuring a low computational complexity for the technique developed to estimate a steganographic capacity of stego communication channel, and
- Guaranteeing efficient work of the technique developed regardless of the real value of SC when embedding AI with the LSB approach.

Main Body

Let us review characteristic features of changes for the smallest SVs of blocks of lossy compressed (LC) cover objects (digital images) within the process of stego transformation (ST).

Comparison of properties of SVs of blocks of lossy and lossless compressed cover objects makes it possible to foresee the behaviour pattern of properties of SVs of blocks (i.e., submatrices) of LC cover objects within the course of ST. Presence of non-zero SVs within the submatrix is indicative of the submatrix degeneracy (linear dependence of its row vectors (column vectors)). If the smallest SVs are non-zero, but close to zero (as it is often observed in the DI fully restored after compression), the submatrix, being not degenerative, but badly conditioned, contains row (or column) vectors that are close to being linear dependent, e.g., the angle between some row (or column) vectors can be not equal, but close to zero. Any disturbance (in particular, ST), will change these angles in some way. However, apparently, the possibility that the angle will become equal to zero, thus leading to the increase in the number of zero SVs, is much lower than that the angle would remain non-zero after disturbance. Besides, due to specificity of the problem concerned, all row (or column) vectors of 8×8 blocks are geometrically located in the first coordinate orthant of R^8 vector space, and, in the main, no disturbance can lead them beyond the limits of this orthant. Therefore, if the close-to-zero angle between row (or column) vectors of the matrix is disturbed, the possibility of increase in value of the angle is higher, than that of decrease. In order to test the proposed hypothesis, we performed a computing experiment involving 250 JPEG DIs. The experiment was performed as follows. Each DI was decomposed into 8×8 blocks in a standard way. Block columns were normalized. For each normalized B block, an 8x8 $\overline{B}$ matrix was calculated with $\overline{b}_{ij}, i, j = \overline{1,8}$ elements equal to the scalar product of i^{th} and j^{th} columns of B matrix (i.e., cosine of the angle between i^{th} and j^{th} columns). Blocks, where corresponding $\overline{B}$ matrix contained close-to-one (>0.999) elements, were marked, and their

total number for the each DI was counted. Furthermore, in marked blocks, the indices of close-to-linearly-dependent columns were saved. With the noise (Gaussian noise with zero expectation value and different variances) superimposed on the image, the matrix was decomposed into blocks again, and the whole above-mentioned procedure was repeated for them. The experiment results showed the following. The number of blocks for which $\overline{B}$ matrix contained close-to-one elements did not increase in 83% of DIs tested. At the stage of verification of the marked blocks, non-increase of the corresponding $\overline{B}$ elements (increase of the angle between column vectors of B) was registered in 93% of all close-to-linear-dependent columns found at the first stage.

The experiment, in case of disturbance, confirmed an increase in the degree of non-singularity of the corresponding block for DI of lossy-compressed format (LCF), decrease of its condition number, increase of deviation-from-zero value for the smallest SVs of the block, thus confirming that, as a result of ST, a block of LC cover object will be «losing» LCF properties of SVs, and «acquiring» those of lossless-compressed format (LLCF) [6].

Therefore, qualitative results of ST of LC cover objects with LSB approach will be as follows:

- Decrease in the quantity of non-zero SVs in blocks compared to LC cover-object blocks, and, the higher is SC of the organized stego channel, the greater will be this decrease, and,
- With the increase of SC, the behavior pattern of SVs of SS blocks will be more and more «matching» to that of SVs for lossless-compressed DI; in particular, for the majority of blocks, the rate of change for the smallest SVs will increase.

Thus, increase in the rate-of-change of the lowest SVs for the overwhelming majority of image submatrices comparing with the corresponding characteristic of LC cover object states that the ST procedure has been held, and the rate-of-change of the lowest SVs itself appears to be that very characteristic of disturbance of image parameters that allows not only to determine the presence of ST [3, 4, 6] results, but also to estimate the SC value.

Let us perform a detailed analysis of the parameters of stego message vs. the value of SC of a channel.

As it follows from above, ST will result in a decrease in number of degenerated blocks when compared to that of LC cover object, and, the higher is SC, the greater will be the number of degenerated blocks [7]. Using estimation of the number of non-degenerated DI blocks as a basis for conclusion on the presence/absence of AI in DI in actual practice causes difficulties due to availability of a vast number of LC cover objects with ≈100% percentage of the blocks not involving zero SVs. This results in great computational complexity in obtaining a threshold value of this number in order to separate the cover image from SM.

Let us review a relationship between the average rate-of-change for the smallest SVs of DI matrix blocks and SC. This relationship is reflected by the plot built according to the results of the computing experiment performed in *MathWorks* MATLAB environment with 500 DIs from the NRCS database [8], the latter being traditional one to test algorithms dealing with images; here the lowest SC was 1/20 bit per pixel (or 5%) (Fig. 1).

The results obtained fully quantitatively confirm the qualitative statement that, with the increase in SC, the behavior of SVs of blocks belonging to SM «tends to» match to that of SVs of lossless-compressed DI. This fact is reflected in strictly monotomic increase of the rate-of-change of smallest SVs with the increase of SC, and the average rate-of-change V vs. steganographic capacity S characteristic is practically linear (Figure 1) and can be approximated by the following relationship:

$$V \approx 0.004 \cdot S + 0.346. \qquad (1)$$

This fact provides a possibility in principle for the following:

- Estimating quantitatively the average rate-of-change for the arbitrary SC within 5 to 100% range based on the plot obtained, and
- Estimating the SC value from average rate-of-change of the smallest SVs of the blocks, when developing SM with LSB approach, thus increasing efficiency of AI decoding (if required).

The results received can have practical importance when not one, but a set of DIs received during stego channel work with maintained SC undergo steganalysis. That is the basis for the *SPS* technique used to estimate SC of the stego channel organized with the help of LSB approach. The main steps are as follows:

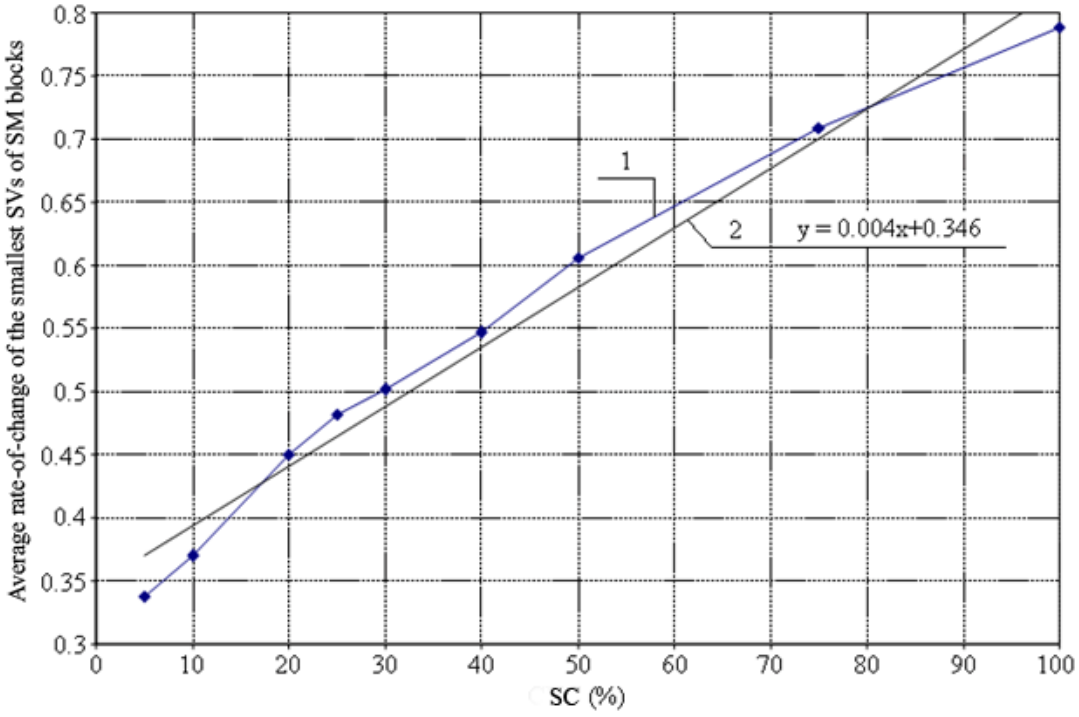


Fig. 1. Average rate-of-change of the smallest SVs of SM blocks vs. SC characteristic: 1 – interpolation spline of degree 1; 2 – linear approximation

Let F_i, $i=\overline{1,n}$ be the matrices of DIs under analysis, received from the same stego channel (it is supposed that stego messages were formed with the same SC).

Step 1. Decompose matrices F_i, $i=\overline{1,n}$ of digital images under analysis into 8×8 blocks (sumbatrices) B_j, $j=\overline{1,N}$, where N is the total number of the blocks obtained.

Step 2. For each of thus B_j, $j=\overline{1,N}$ submatrices obtained:

2.1. Determine the set of singular values as follows: $\sigma_1^{(j)} \geq ... \geq \sigma_8^{(j)} \geq 0$;

2.2. For $\sigma_7^{(j)}, \sigma_8^{(j)}$ determine angular factor $k^{(j)}$ of interpolating polynomial of degree 1.

Step 3. Determine V, the average rate-of-change of the smallest SVs of SM blocks of DIs under analysis:

$$V = \frac{\sum_{j=1}^{N} k^{(j)}}{N}; \tag{2}$$

Step 4. Estimate the SC value in accordance with (1) and using the result of (2):

$$S \approx \frac{V - 0.346}{0.004}. \tag{3}$$

The value of SC obtained in step 4 with formula (3) is approximate. Let us perform a computational experiment to test the technique developed. For this purpose, let us form an I set of DIs (cover objects) from 500 images taken from NCRS base. With this done, let us use LSB approach to form I_1, I_2, I_3, I_4, I_5 sets by stego transformation of the images from I set with steganographic capacity equal to 10, 30, 50, 70, and 90%, respectively. In order to determine the steganographic capacity used during the development of stego messages incorporated into proper sets, let us subject each of I_1, I_2, I_3, I_4, I_5 sets to analysis with SPS method. The test results are given in Table 1.

Table 1.

Results of tests of SPS method

The set under test		I_1	I_2	I_3	I_4	I_5
True value of SC (%)		10	30	50	70	90
SC value obtained/absolute error (%)	for complete set (500 DIs)	5/5	33/3	55/5	72/2	86/4
	for subset (400 DIs)	7/3	34/4	56/6	73/3	86/4
	for subset (300 DIs)	5/5	35/5	55/5	76/6	84/6
	for subset (200 DIs)	4/6	37/7	57/7	78/8	81/9
Average error value		4.75	4.75	5.5	4.75	5.5

As our computational experiment shows, when estimating steganographic capacity with SPS technique, the average of Δ (absolute error) practically does not depend on the true value of SC (including small SC values), but depends on K number of digital images subjected to analysis: the average of Δ (absolute error) denoted hereinafter by Δ_S, is increased with decrease in K (Fig. 2), which is natural if one takes into account the way in which relationship (1) was obtained.

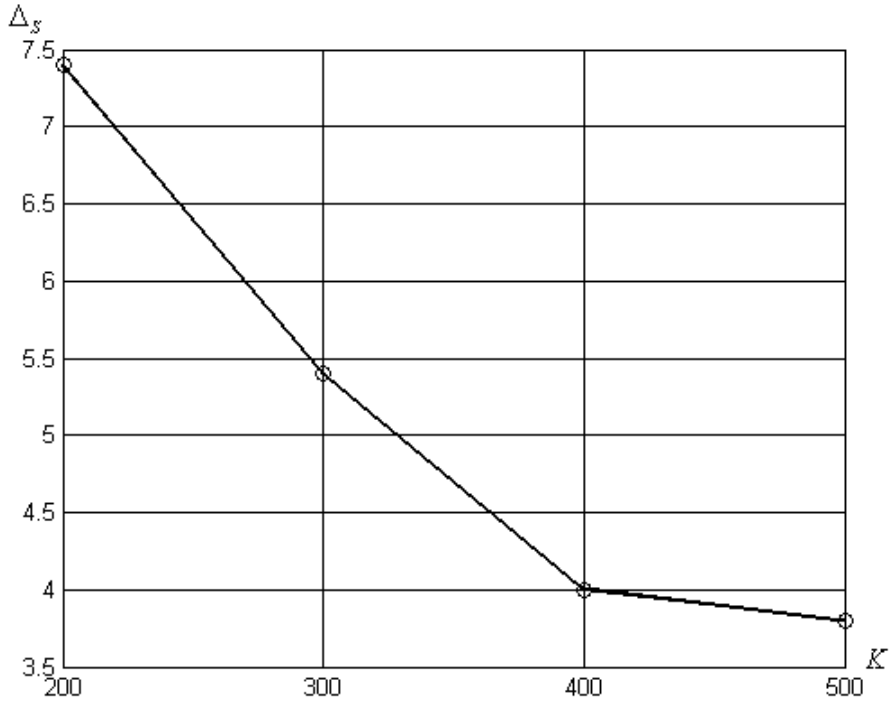


Fig. 2. Average absolute value of steganographic capacity determined with *SPS* method vs. Number of digital images subjected to analysis

Note. The computational complexity of *SPS* technique developed to estimate SC of the stego channel by analysis of a set comprising K number of $n \times n$-pixel digital images (with this channel organized by means of LSB modification approach) is determined by a number of blocks (i.e., submatrices) obtained by standard matrix decomposition. When it concerns one digital image, the computational complexity equals to $\underline{O}\left(n^2\right)$. Therefore, the resultant computational complexity of *SPS* technique is determined as $K \cdot \underline{O}\left(n^2\right)$.

Conclusions

In this work, a polynomial (of degree 2) technique for estimating a steganographic capacity of a stego channel formed with LSB approach was developed based on general approach to analysis of the status and performance of information systems. Digital images of lossy compression formats were used as cover objects.

During the performance of this work:

1) It was established that strictly monotomic increase of the rate-of-change of smallest singular values with the increase of SC is the qualititative feature of the two smallest singular values of blocks (i.e., submatrices) of a digital image. This fact supports the following hypothesis: with the increase of SC, the behavior pattern of SVs of SS blocks will be more and more «matching» to that of SVs for lossless-compressed DI.

2) With respect to stego transformation with LSB approach, a quantitative correspondence relationship between the rate-of-change of smallest singular values of digital image blocks (i.e., submatrices) and SC value was established.

3) It was empirically established that the absolute error of SC obtained by *SPS* technique is essentially independent of its true value, but dependent on the number of stego messages subjected to analysis.

4) It was established that the absolute error of result obtained by *SPS* technique is dependent on the K number of stego messages obtained with the same SC and subjected to analysis: the more is K number, the less is the error of estimated SC.

References

1. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.
2. Стеганография, цифровые водяные знаки и стеганоанализ : [монография] / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. — М.: Вузовская книга, 2009. — 220 с.
3. Бобок, И.И. Использование метода анализа ROC-кривых для комплексной оценки эффективности стеганоаналитического метода / И.И. Бобок // Інформатика та математичні методи в моделюванні. — 2012. — Том 2, №3. — С. 221–230.
4. Бобок, И.И. Стеганоаналитический метод для цифрового сигнала-контейнера, хранящегося в формате с потерями / И.И. Бобок // Сучасний захист інформації. — 2011. — №2. — С. 50–60.
5. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. — М. : Техносфера, 2006. — 1070 с.
6. Бобок, И.И. Детектирование наличия возмущений матрицы цифрового изображения как составная часть стеганоанализа / И.И. Бобок // Вісник Східноукраїнського національного університету ім. В. Даля. — 2011. — № 7(161). — С. 32–41.
7. Бобок, И.И. Стеганоанализ как частный случай анализа информационной системы / И.И. Бобок, А.А. Кобозева // Сучасна спеціальна техніка. — 2011. — № 2. — С. 21–34.
8. NRCS Photo Gallery: *[Електронний ресурс]* // United States Department of Agriculture. Washington, USA. Режим доступа: http://photogallery.nrcs.usda.gov (Дата обращения: 26.07.2012).

МЕТОД ОЦІНКИ ВЕЛИЧИНИ ПРИХОВАНОЇ ПРОПУСКНОЇ СПРОМОЖНОСТІ КАНАЛУ, СФОРМОВАНОГО МЕТОДОМ МОДИФІКАЦІЇ НАЙМЕНШОГО ЗНАЧУЩОГО БІТА

І.І. Бобок

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: onu_metal@ukr.net

У рамках підвищення ефективності стеганоаналізу на основі загального підходу до аналізу стану й технології функціонування інформаційних систем розроблений поліноміальний метод оцінки величини прихованої пропускної спроможності (ППС) каналу зв'язку, організованого за допомогою методу модифікації найменшого значущого біта (LSB-методу). Як контейнери використовувалися цифрові зображення у форматах із втратами. Розроблений метод є важливим при організації декодування вбудованої в контейнер додаткової інформації. Отриманий закон кількісної залежності середньої швидкості зміни найменших сингулярних чисел блоків матриці зображення від величини ППС при організації стеганоперетворення LSB-методом. Емпірично встановлено, що абсолютна похибка одержуваного розробленим методом значення ППС практично не залежить від її дійсного значення, а визначається кількістю зображень-стеганоповідомлень, що аналізуються.

Ключові слова: стеганоаналіз, прихована пропускна спроможність, сингулярні числа, цифрове зображення, матриця

МЕТОД ОЦЕНКИ ВЕЛИЧИНЫ СКРЫТОЙ ПРОПУСКНОЙ СПОСОБНОСТИ КАНАЛА, СФОРМИРОВАННОГО МЕТОДОМ МОДИФИКАЦИИ НАИМЕНЬШЕГО ЗНАЧАЩЕГО БИТА

И.И. Бобок

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: onu_metal@ukr.net

В рамках повышения эффективности стеганоанализа на основе общего подхода к анализу состояния и технологии функционирования информационных систем разработан полиномиальный метод оценки величины скрытой пропускной способности (СПС) канала связи, организованного при помощи метода модификации наименьшего значащего бита (LSB-метода). В качестве контейнеров использовались цифровые изображения в форматах с потерями. Разработанный метод является важным при организации декодирования внедренной в контейнер дополнительной информации. Получен закон количественной зависимости средней скорости изменения наименьших сингулярных чисел блоков матрицы изображения от величины СПС при организации стеганопреобразования LSB-методом. Эмпирически установлено, что абсолютная погрешность получаемого разработанным методом значения СПС практически не зависит от ее истинного значения, а определяется количеством изображений-стеганосообщений, которые подвергаются анализу.

Ключевые слова: стеганоанализ, скрытая пропускная способность, сингулярные числа, цифровое изображение, матрица

УДК 519.682.5

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 4, pp. 331-341

ДИАГНОСТИРОВАНИЕ СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Л.С. Ломакина, В.П. Губернаторов

Нижегородский государственный технический университет им. Р.Е. Алексеева,
ул. Минина, 24, Нижний Новгород, 603950, Российская Федерация; e-mail: llomakina@list.ru

Рассмотрена задача оптимального диагностирования сложных технических систем. Для решения задачи разработана модификация эволюционно-генетического алгоритма. Выполнено сравнение разработанной модификации с алгоритмами, основанными на концепциях динамического программирования и имитации отжига.

Ключевые слова: техническое диагностирование, эволюционно-генетический алгоритм, метод имитации отжига, динамическое программирование

Введение

Современные сложные технические системы решают задачи, требующие высокого уровня надёжности их функционирования. Одним из методов обеспечения надёжности является диагностирование систем на заданном наборе тестов. Выполнение каждого теста связано с затратой материальных ресурсов, поэтому при необходимости диагностирования, возникает задача построения оптимальной тестовой последовательности, обеспечивающей минимум затрат на определение заданного числа отказов технической системы.

Данной проблеме посвящено большое количество работ отечественных и зарубежных авторов: Г.Ф. Верзаков, П.П. Пархоменко, В.И. Сагунов, А.Ю. Арженеко, Д.В. Сперанский, В.В. Сапожников, М.А. Владимиров, J. Wegener, J. Ribero, A. Arcury, J. Shiozaky, и др. На основании обзора литературных источников можно сделать вывод, что рассматриваемая задача является комбинаторной и может быть решена с помощью известных методов дискретной оптимизации [1], однако при диагностировании сложных систем эти методы не всегда практически реализуемы, так как требуют трудоёмких вычислений. Когда использование точных методов оптимизации становится невозможным, практическую значимость приобретает приближённый подход. В ряде работ предлагается использовать метаэвристические алгоритмы: имитацию отжига, моделирование муравьиной колонии и восхождение к экстремуму, однако рассмотренные методы носят частный характер, поэтому актуальной является разработка нового эффективного метода диагностирования сложных систем, основанного на применении обобщенной модели и современных приближённых методов оптимизации.

Предлагается модификация эволюционно-генетического алгоритма, адаптированная для решения задачи построения оптимальной тестовой последовательности и выполняется сравнение предложенной модификации с другими известными методами.

Базовая модель сложной системы

Для разработки обобщенного метода оптимального диагностирования сложных технических систем в качестве базовой модели будём использовать графо-матричную модель.

Пусть T — множество тестов, разработанных для проверки диагностируемой системы. Каждый тест $t_i \in T$ позволяет определить работоспособность и может быть представлен в виде множества $\{(X_a, Y_d, Z_d)_g\}$, где X_a — определённое воздействие на систему, Y_d — ожидаемая реакция на это воздействие, Z_d — контрольная точка, на которой производится сравнение с Y_d реакции объекта на воздействие X_a.

Представим сложную техническую систему в виде ориентированного графа $G(B,U)$ с N вершинами. Обозначим B — множество вершин графа, U — множество рёбер графа. Если можно выделить конструктивные или функциональные блоки объекта, вершины графа соответствуют структурным блокам системы, а рёбра графа – связям между блоками. Если выделить блоки затруднительно – вершины графа соответствуют параметрам системы, а рёбра графа – причинно-следственным связям между параметрами.

Далее будем рассматривать граф блочной структуры, для графа причинно-следственных связей моделирование осуществляется аналогично.

Пронумеруем блоки объекта, диагностирования и разметим вершины графа $G(B,U)$ соответствующими номерами $\{1,\ldots,N\}$. Отметим на графе контрольные точки, соответствующие тестам $t_i \in T$. Контрольные точки представляются в виде разметки рёбер графа $G(B,U)$. Ребро $U_\gamma = (B_\alpha, B_\beta)$ размечено контрольной точкой Z_γ, тогда и только тогда, когда при выполнении одного из тестов $t_i \in T$ осуществляется оценка диагностического параметра Y_γ, являющегося выходным для блока B_α и входным для блока B_β.

На графе $G(B,U)$ тест t_i изображается в виде множества контрольных пар вершин (B_δ, B_γ), где B_δ — вершина, соответствующая блоку, на вход которого подаётся входной сигнал X_{ag}; B_γ — вершина, из которой выходит дуга **U**, соответствующая контрольной точке Z_{dg}. Тест t_i контролирует состояние блока B_j тогда и только тогда, когда в графе $G(B,U)$ существует хотя бы один путь из вершины B_δ в вершину B_γ, проходящий через вершину B_γ (рис. 1).

Каждый элементарный тест позволяет установить исправность или неисправность группы из k контролируемых блоков. Остальные $(N-k)$ блоков остаются непроверенными.

Если число блоков диагностируемой системы N, тест $t_i \in T$ может быть представлен в виде N-мерного вектора V_i. Ненулевое значение j-й компоненты вектора V_i означает, что j-й блок системы контролируется данным тестом и является исправным, если результат теста положительный. Нулевые значения компонент вектора V_i соответствует блокам, неконтролируемым элементарным тестом t_i. При положительном результате теста и неисправном состоянии всей исследуемой системы в целом формулируется вывод о том, что неисправен, по меньшей мере, один из $(N-k)$ неконтролируемых блоков.

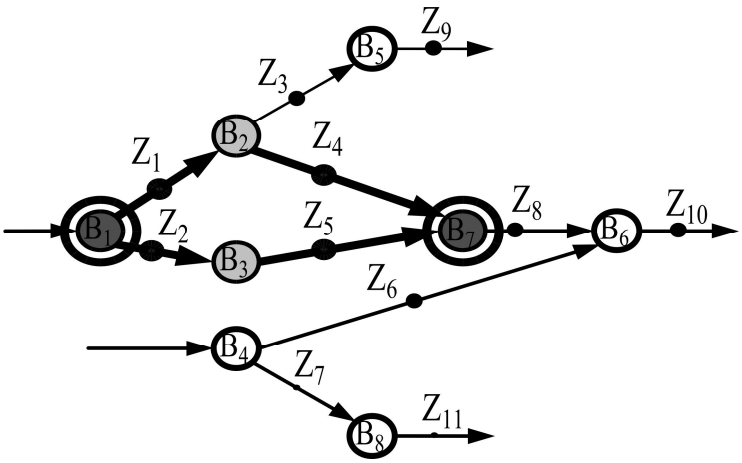
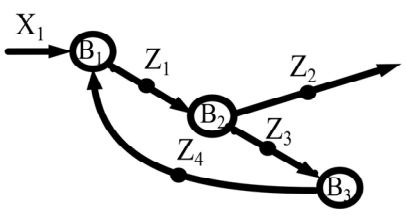


Рис. 1. Представление теста $t_i = \{(X_1, Y_8, Z_8)\} \longrightarrow \{(B_1; B_7)\}$ на графе сложной системы

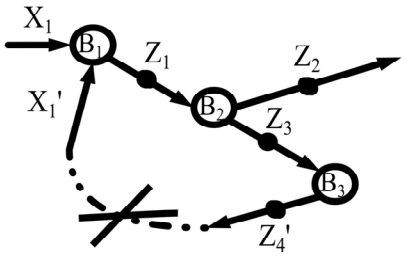
Положим, что $|T| = M$, и на основе модели теста построим модель сложной системы в виде матрицы идентификации. Матрица идентификации – это прямоугольная матрица $A_{M\times N} = \|a_{ij}\|$ столбцам, которой соответствуют блоки исследуемой системы B_j, а строкам тесты t_i.

Если два или более столбца в матрице A совпадают, то неисправности в соответствующих им блоках являются неразличимыми (рис. 2(а)). Описанная ситуация может возникнуть из-за ориентированных циклов в графе $G(B,U)$. Данные циклы свидетельствуют о наличии обратных связей между блоками исследуемой системы. Для возможности обнаружения неисправности данных блоков, необходимо вводить контролируемые разрывы в контуры обратных связей (рис. 2(б)).



	B_1	B_2	B_3
t_1	1	1	1
t_2	1	1	1
t_3	1	1	1
t_4	1	1	1

а



	B_1	B_2	B_3
t_1	1	0	0
t_2	1	1	0
t_3	1	1	0
t_4	1	1	1

б

Рис. 2. Введение контролируемых разрывов в граф исследуемой системы для идентификации состояния блоков, входящих в конуры обратных связей

Выбранная модель представляет информацию о структуре системы, возможных неисправностях, разработанных тестах и стоимости их исполнения. Данная модель позволяет представить тестовую последовательность в виде нагруженного дерева поиска $S = s(\tau \subseteq T)$, листьями которого являются номера неисправных блоков системы $i \in [1, N]$, а каждой внутренней вершине соответствует тест из некоторого подмножества τ множества тестов $T = \{t_1 ... t_M\}$.

При известной стоимости выполнения каждого теста $C(t_i \in T) = C_i$ и вероятности неисправности каждого блока $P(B_i, i \in [1, N]) = P_i$ можно вычислить стоимость исполнения тестовой последовательности:

$$C(S) = \sum_{z \in Z \subseteq N} C(B_z) P(B_z), \tag{1}$$

где

Z — множество блоков диагностируемой системы, состояния которых могут быть идентифицированы путём выполнения последовательности S;

$C(B_z)$ — стоимость идентификации состояния блока z, определяемая как суммарная стоимость тестов, принадлежащих пути от корня дерева S до листа B_z.

В качестве глубины диагностирования системы, достигаемой при исполнении тестовой последовательности S, рассматривается величина:

$$\phi(S) = \frac{\sum_{z \in Z \subseteq N} P(B_z)}{\sum_{i \in N} P(B_i)}, \tag{2}$$

где Z — множество блоков диагностируемой системы, состояния которых могут быть идентифицированы путём выполнения последовательности S.

Постановка задачи: найти тестовую последовательность $S = s(\tau \subseteq T)$, позволяющую минимизировать целевую функцию $C(S)$, при условии $\phi(S) = \phi_0$.

Алгоритмы построения оптимальных тестовых последовательностей

Для решения поставленной задачи построим модификацию классического эволюционно-генетического алгоритма [2], в качестве альтернативных методов решения для последующего сравнения рассмотрим алгоритмы на основе концепций имитации отжига и динамического программирования.

Модификация эволюционно-генетического алгоритма (ЭГА)

Формально эволюционно-генетический алгоритм можно определить следующим образом:

$$ЭГА = (P^0, K, \lambda, L, Sl, R, f, k), \tag{3}$$

где

$P^0 = \{x_1^0, x_2^0, ... x_\lambda^0\}$ — начальная популяция;

x_γ — потенциальное решение задачи, представленное в виде хромосомы;

λ — размер популяции;

K — биективное отображение множества допустимых решений во множество хромосом, определяющее способ кодирования;

L — длина хромосомы;

Sl — операторы селекции;

R — операторы рекомбинации;

$f = f(x)$ — функция приспособленности (целевая функция для эволюционной оптимизации);

k — критерий останова.

Модификация эволюционно-генетического алгоритма заключается в выборе параметров (3), согласно условиям поставленной задачи.

Рассмотрим в качестве генома популяции множество номеров тестов $J = \{1,2,\ldots, j,\ldots, M\}$. *Допустимой хромосомой* будем считать любую перестановку из элементов этого множества.

Тест, соответствующий первому гену x_0^γ, становится корнем дерева тестовой последовательности, при этом множество всех блоков исследуемой системы разбивается на классы $\{B_1^0, B_2^0, \ldots, B_j^0, \ldots, B_H^0\}$, и образуется H ветвей дерева, по которым расположены подозрительные на неисправность блоки диагностируемого объекта. Просматриваются все ветви, тест, соответствующий следующему гену x_1^γ, добавляется к ветви j только в том случае, если он позволяет выполнить дальнейшее разбиение подмножества B_j^0 на классы $\{B_1^1, B_2^1, \ldots, B_j^1, \ldots, B_H^1\}$. Затем, операция повторяется для тестов, соответствующих оставшимся генам $x_2^\gamma, \ldots, x_k^\gamma, \ldots, x_M^\gamma$.

Процесс прекращается при условии:

$$\left(\forall (i,j): \left|B_j^i\right| = 1\right) \vee \left(\phi(S_\gamma) = \phi_0\right) \vee (k = M). \qquad (4)$$

Предложенный метод кодирования позволяет получать хромосомы одинаковой длины $L = M$ и использовать не декодируемую часть хромосомы, как дополнительное средство выхода из локальных оптимумов.

В качестве операторов R из различных операторов кроссинговера и мутации были выбраны *жадный и упорядоченный операторы кроссинговера*. Совместное применение выбранных операторов позволяет *комбинировать случайный и направленный поиск* (рис. 3) и обеспечивает достаточное условие выхода из локальных оптимумов:

$$\forall \gamma : p\left(x_\gamma : x_\gamma \xrightarrow{K} \left(S_\gamma \in U\right)\right) \neq 0, \qquad (5)$$

где

U — множество тестовых последовательностей, удовлетворяющих условиям задачи;

$p(x_\gamma)$ — вероятность появления хромосомы x_γ после применения генетических операторов R.

Для ускорения выхода из локальных оптимумов предлагается использовать адаптивную поисковую стратегию. При схождении популяции вторые операнды операторов R генерируются случайно, а не выбираются из текущей популяции. При длительном нахождении в состоянии схождения к популяции применяется оператор геноцида. Предложенная поисковая стратегия основана на принципе *элитизма,* позволяет ускорить выход локальных оптимумов и обеспечивает более быстрое схождение по сравнению с классическими ЭГА, использующими кроссинговер и мутацию (рис. 4).

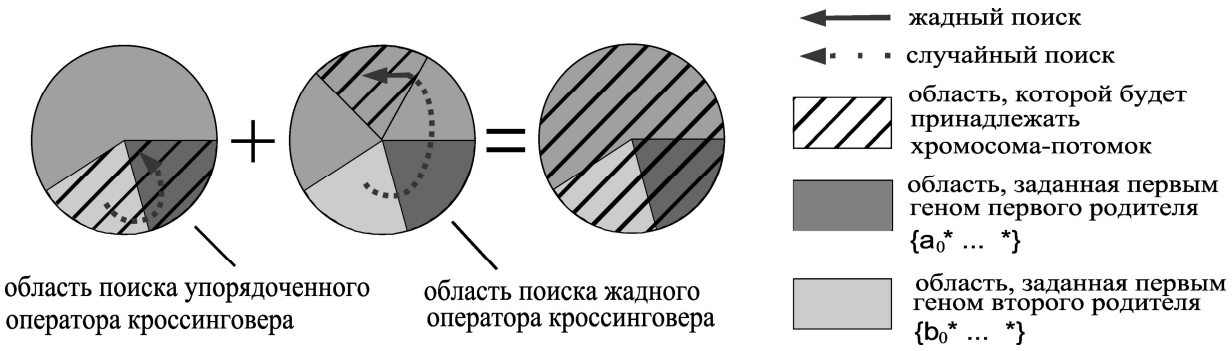


Рис. 3. Область эволюционно-генетического поиска при совместном применении жадного и упорядоченного операторов кроссинговера

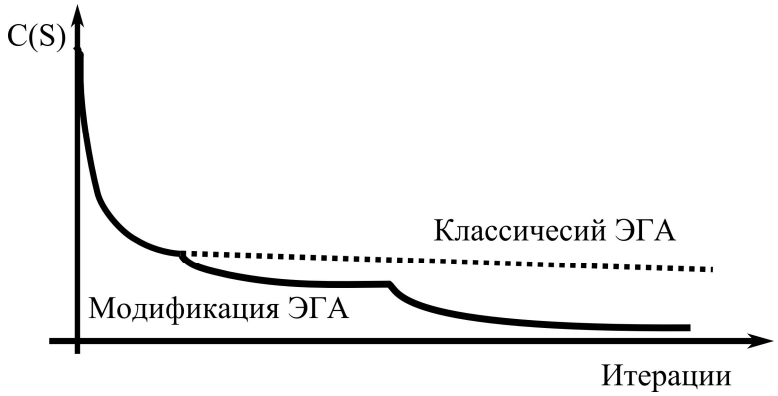


Рис. 4. График схождения разработанной модификации и классического ЭГА

В качестве оператора Sl предлагается использовать простую элитную селекцию на основе сравнения значений функции приспособленности $f(x)=C(s)$, а начальную популяцию P^0 формировать путём применения фрактального оператора кроссинговера к двум случайно сгенерированным решениям. Такой подход позволит эффективно использовать жадный оператор кроссинговера на первой итерации алгоритма, обеспечивать уникальность начальных решений и автоматически определять размер родительской популяции, как функцию от числа строк матрицы идентификации – M. Останов будем осуществлять при достижении желаемого значения целевой функции $C(S)$ либо по истечении заданного числа итераций.

Имитация отжига (ИО)

Метод имитации отжига является одним из наиболее эффективных методов случайного поиска решения широкого спектра задач. В работе [3] указывается, что на большинстве задач метод имитации отжига не проигрывает эволюционно-генетическим алгоритмам, а на многих оказывается эффективнее. Основным преимуществом метода имитации отжига является возможность выхода из локальных оптимумов. Это достигается за счет принятия решений не только в сторону улучшения, но и в сторону ухудшения целевой функции в зависимости от температуры отжига Δ, моделируемого процесса закалки.

Общая схема алгоритма имитации отжига.

1) Выбирается температура отжига в виде дискретного отрезка $[\Delta_o,...\Delta_n]$, устанавливается текущая температура $\Delta' = \Delta_i$, $i = n$.

2) Выбирается начальное решение x_o, оно становится текущим $x' = x_o$.

3) С помощью преобразования θ получается решение-кандидат $x'' = \theta(x')$.

4) Вероятность, с которой решение $x'' = \theta(x')$ станет текущим, равна $P(x', x'')$, где P — распределение Гиббса:

$$P(x', x'' \mid x') = \begin{cases} 1 & \text{при } f(x'') \le f(x') \\ e^{\lambda} & \text{при } f(x'') > f(x') \end{cases}, \qquad \lambda = -\frac{f(x'') - f(x')}{\Delta'}, \tag{6}$$

где $f(x)$ — значение целевой функции, соответствующее решению x.

5) Понижаем температуру $i = i - 1$, $\Delta' = \Delta_i$.

6) Процесс прекращается при $\Delta' = \Delta_0$, в противном случае переходим к шагу 3.

В начале поиска температура имеет наибольшие значения, и величина e^{λ} близка к единице, поэтому велика вероятность выбора решения с худшим значением целевой функции $f(x)$. При высоких температурах Δ_i, $i > n/2$ решение $x'' = \theta(x')$ может быть выбрано текущим при $f(x'') > f(x')$, что может привести к попаданию в локальный оптимум при дальнейшем уменьшении температуры. Чтобы избежать описанной ситуации, предлагается на каждой итерации алгоритма сохранять наилучшее из найденных решений.

Динамическое программирование (ДП)

Метод подробно рассмотрен в работе [2]. Для построения оптимальной тестовой последовательности используется уравнение Беллмана вида:

$$C_{opt}(k_{\beta x}, T_{\beta x}) = C_{opt}(S_{\beta x}) = \min_i \left(C(t_i \in T_{\beta x}) + \sum_j P_j \cdot C_{opt}(k_{jh}; T_{jh}) \right),$$

$$P_j = \frac{\sum_{Б_y \in k_{jh}} P(B_y)}{\sum_{Б_z \in k_{\beta x}} P(B_z)}, \tag{7}$$

где

$(k_{\alpha h}; T_{\alpha h})$ — ситуация α, порядка $h = | k_{\alpha h} |$;

$T_{\alpha h} \subseteq T$ — множество тестов, позволяющих выполнить дальнейшее разбиение подмножества $k_{\alpha h} \in K$;

K — Совокупность подмножеств блоков B^i, соответствующих всевозможным сочетаниям тестов из T;

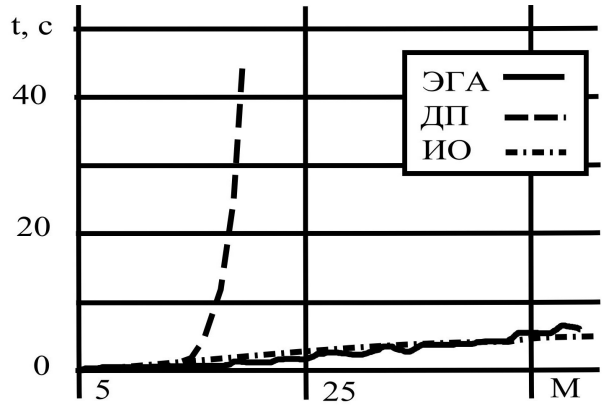
t_i — тест из множества $T_{\beta x}$;

k_{jh} — подмножества, на которые t_i разбивает множество $k_{\beta x}$;

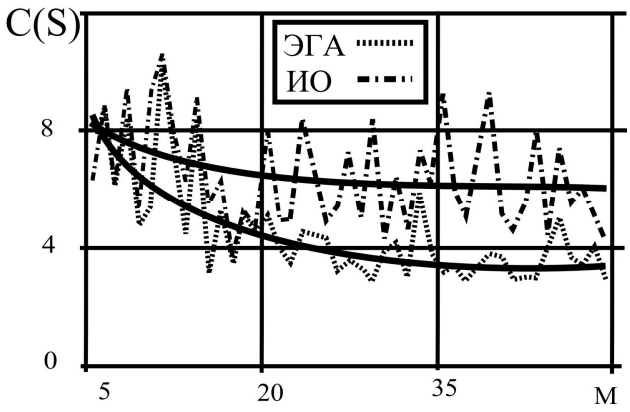
P_j — условная вероятность наличия неисправности в блоках $B_y \in k_{jh}$.

Вычислительный эксперимент

Рассмотрим оценки вычислительной сложности (рис. 5(а)) и сходимости (рис. 5(б)) разработанной модификации ЭГА, ДП и ИО. Модификации ЭГА обладает квадратичной сложностью от числа разработанных тестов M и линейной относительно числа блоков системы N. Возможно снижение сложности до $O(M^2/K)$ при использовании K параллельных вычислителей. Сложность ДП экспоненциальная относительно M и линейная относительно N. ИО имеет линейную сложностью относительно M и N. Сравнение целевой функции оптимальной тестовой последовательности, получаемой в результате применения модификации ЭГА и ИО, позволяет сделать вывод, что ЭГА эффективнее ИО.



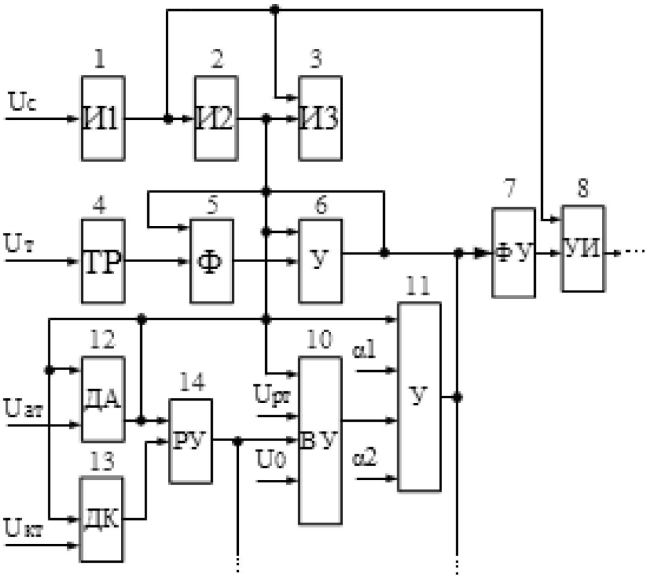
а



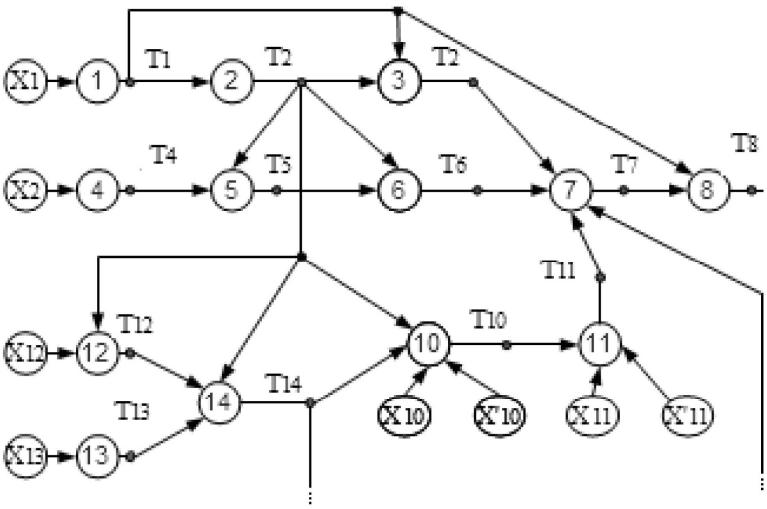
б

Рис. 5. а – оценка времени работы ЭГА, ДП, ИО от числа тестов M; б – сравнение значения целевой функции оптимального решения для ИО и ЭГА

В качестве примера рассмотрен автоматизированный электропривод [4], функциональная схема которого изображена на рис. 6(а), граф на рис. 6(б), матрица идентификации на рис. 6(в). Точками контроля являются выходы функциональных блоков. Для каждого блока устанавливаются зависимости между входными и выходными сигналами, а также допустимые диапазоны этих сигналов. Функциональный блок считается дефектным, если при допустимых входных сигналах на выходе данного блока наблюдается недопустимый сигнал. Стоимость тестов соответствует временным затратам на отключение и подключение измерительной аппаратуры. Вероятности неисправностей блоков выбираются, исходя из насыщенности данных блоков элементами.



а



б

Тесты	Блоки элементов						С(Т)
	Б1	Б2	Б3	Б4		Б48	
Т1	1	0	0	0		0	0,04
Т2	1	1	0	0		0	0,02
Т3	1	1	1	0		0	0,01
Т48	1	1	0	0		1	0,03
Р(Б)	0,04	0,06	0,04	0,01		0,18	

в

Рис. 6. Модель автоматизированного электропривода

С помощью предложенных в работе алгоритмов были получены результаты, представленные в таблице. Для ДП результат получить не удалось, так как исполнение алгоритма потребовало более 2 Гб ОЗУ.

Таблица 1.

Результаты экспериментов

	$C(S)$	t, с
ДП	-	>7200
ЭГА	28.4	10
ИО	31.7	15

Результаты вычислительных экспериментов показали, что предложенный подход позволяет использовать возможности современных вычислительных систем и может эффективно применяться для оптимизации числа контрольных точек при проектировании сложных технических систем, либо для минимизации затрат на тестирование в процессе их эксплуатации.

Выводы

1) Разработана модификация ЭГА, для решения задачи построения оптимальных тестовых последовательностей, отличающаяся от существующих: способами кодирования решений и построения целевой функции; использованием специальными генетических операторов. Модификация позволяет рассматривать тестовые последовательности различной длины, учитывать заданную глубину диагностирования и может применяться при неполном или избыточном наборе тестов.

2) Рассмотрены альтернативные методы решения поставленной задачи на основе концепции динамического программирования и метода имитации отжига.

3) Экспериментально получены оценки сходимости и вычислительной сложности, позволяющие сделать вывод об эффективности предложенной модификации ЭГА, по сравнению с другими известными алгоритмами.

4) На основе предложенной модификации разработан новый метод оценки оптимального решения, позволяющий решить задачу диагностирования с наименьшим использованием вычислительных ресурсов, по сравнению с другими известными методами.

Список литературы

1. Сигал, И.Х. Введение в прикладное дискретное программирование: модели и вычислительные алгоритмы [Текст] : учеб. для студ. вузов, обуч. по напр. и спец. «Прикладная математика и информатика» / И.Х. Сигал, А.П. Иванова. — Изд. 2-е, испр. и доп. — М. : Физматлит, 2007. — 304 с.
2. Ломакина, Л.С. Модификация эволюционно-генетического алгоритма для эффективного диагностирования сложных систем / Л.С. Ломакина, В.П. Губернаторов // Системы управления и информационные технологии. — 2013. — Т. 53, № 3. — С. 59–64.
3. Inber, L. Genetic Algorithms and Very Fast Simulated Reannealing: A comparison / L. Inber, B. Rosen // Mathematical and Computer Modelling. — 1992. — Vol. 16, Iss. 11. — PP. 87–100.
4. Осипов, О.И. Техническая диагностика автоматизированных электроприводов : научное издание / О.И. Осипов, Ю.С. Усынин. — М. : Энергоатомиздат, 1991. — 160 с.

ДІАГНОСТУВАННЯ СКЛАДНИХ ТЕХНІЧНИХ СИСТЕМ З ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Л.С. Ломакіна, В.П. Губернаторов

Нижегородський державний технічний університет ім. Р.Є. Алексєєв,
вул. Мініна, 24, Нижній Новгород, 603950, Російська Федерація; e-mail: llomakina@list.ru

Розглянуто задачу оптимального діагностування складних технічних систем. Для вирішення завдання розроблена модифікація еволюційно-генетичного алгоритму. Виконано порівняння розробленої модифікації з алгоритмами, заснованими на концепціях динамічного програмування та імітації відпалу.
Ключові слова: технічне діагностування, еволюційно-генетичний алгоритм, метод імітації відпалу, динамічне програмування

STRUCTURAL TESTING OF SOFTWARE SYSTEMS BASED ON COMPUTER ALGEBRA ELEMENTS

Lyubov S. Lomakina, Vladimir P. Gubernatorov

Nizhny Novgorod State Technical University n.a. R.E. Alekseev,
24 Minina str., Nizhny Novgorod, 603950, Russian Federation; e-mail: llomakina@list.ru

The problem of complex technical systems optimal diagnosis is concerned. The evolutionary algorithm modification for optimal diagnosis is proposed. The proposed approach is compared with the simulated annealing and dynamic programming methods.
Keywords: technical diagnosis, evolutionary algorithm, simulated annealing, dynamic programming

УДК 004.056:159.95

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 4, pp. 342-352

МЕТОД МОДЕЛЮВАННЯ ДІЯЛЬНОСТІ СУБ'ЄКТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З ВИКОРИСТАННЯМ ОПЕРАТОРІВ, ЩО ДІЮТЬ В ОНТОЛОГІЯХ ПРЕДМЕТНИХ ОБЛАСТЕЙ

А.А. Шиян

Вінницький національний технічний університет,
вул. Хмельницьке шосе, 95, Вінниця, 21021, Україна; e-mail: aa_shiyan@mail.ru

В статті розроблено математичний апарат та метод моделювання діяльності суб'єктів інформаційної безпеки, який базується на використанні множини операторів, що діють в спеціальним чином структурованих онтологіях предметних областей, навантажених ціллю. Доведено, що довільний оператор можна звести до певної сукупності двокомпонентних операторів, дія яких зв'язує дві компоненти онтології, одну до, а другу після здійснення діяльності. Наведено ряд прикладів застосування розробленого методу до моделювання суб'єктів інформаційної безпеки.

Ключові слова: інформаційна безпека, метод, онтологія, діяльність, предметна область, суб'єкт

Вступ

Інформаційна безпека – це захищеність інформації та інфраструктури, яка її підтримує, від випадкових або навмисних впливів природного чи штучного характеру, які можуть завдати неприйнятної шкоди суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації та підтримуючій інфраструктурі [1]. В [1, 2] показано, що сьогодні існує велика кількість визначень терміну «інформація», – але всі вони включають в себе, явно чи неявно, те, що тільки *суб'єкт* може як створити, так і користуватися інформацією.

Для суб'єкта характерно, що він має *внутрішні* степені свободи, які й надають йому можливість займати *активну* позицію в інформаційних відносинах. Проявляється це, наприклад, через постановку цілей, вибору однієї/декількох із множини можливих альтернатив, прояв індивідуальних переваг суб'єкта тощо.

На сьогодні в якості суб'єкту можуть виступати тільки люди, - окрема людина, їх структуровані чи неструктуровані об'єднання, суспільні інститути, суспільство в цілому та держава.

Таким чином, дослідження ролі суб'єктів в інформаційних відносинах, аналіз їх характеристик в різних умовах є важливим напрямком наукових досліджень у сфері інформаційної безпеки та її практичних застосувань.

Аналіз літератури та постановка задачі.

Існує багато підходів до опису основного суб'єкту інформаційної безпеки – людини [1, 2]. Умовно їх можна розділити на два великих класи. До першого можна віднести опис суб'єкта в рамках переважно психологічних перемінних [2]. Другий

підхід базується на використанні характеристик суб'єкту, які описують його діяльність [1]. Слід відмітити, що для практичних потреб використовують, як правило, змішані підходи, які описують і психологічні, і діяльні класи.

В [3, 4] розроблено підхід до опису суб'єкта діяльності, який використовує спеціальним чином структурований інформаційний простір задачі. Для цього вся сукупність даних розбивається спеціальним чином, *універсальним* для кожної задачі, на вісім класів (1), які не перетинаються між собою.

$$I_b = \sum_k \oplus I_b^k, \quad \forall k, m : I_k \cap I_m = 0, \tag{1}$$

де

I_b — інформаційний простір задачі *до* здійснення діяльності,

I_b^k — k-та компонента відповідного інформаційного простору,

$k = 1,...,8$ — нумерація компонент інформаційного простору задачі.

Індексами b та a позначаються інформаційні простори задачі *до* та *після* здійснення діяльності людиною.

Схематично метод розбиття множини даних (характеристик) про предметну область онтології на класи-компоненти (тобто алгоритм виділення компонент інформації із даного загального опису) [3, 4] можна представити таблицею 1.

Таблиця 1.

Опис компонент онтології (як інформаційного простору задачі для заданої цілі)

Дані про предметну область онтології	дані про клас подібних об'єктів (узагальнюючі компоненти інформації)	опорні елементи класу (структура, топологія)	Статичність, незмінність	Ст-С
			Динамічність, мінливість	Ст-Д
		границя між даним класом і іншими	Статичність, незмінність	Гр-С
			Динамічність, мінливість	Гр-Д
	дані про саме цей об'єкт (деталізуючі компоненти інформації)	сам об'єкт як одиничний і унікальний	Статичність, незмінність	Об-С
			Динамічність, мінливість	Об-Д
		зв'язки цього об'єкту з іншими конкретними, подібними до нього	Статичність, незмінність	Зв-С
			Динамічність, мінливість	Зв-Д

Можна показати, що побудований за алгоритмом табл. 1 інформаційний простір задачі є онтологією [5]. Але, на відміну від існуючого підходу до визначення онтологій, інформаційний простір є такою онтологію предметної області, яка відповідає *конкретній та фіксованій* цілі діяльності. Такі онтології будемо називати онтологіями, навантаженими ціллю.

Із використанням онтологій предметних областей, навантажених ціллю діяльності, наявність діяльності визначається за досить простим алгоритмом. Спочатку будуємо онтології (інформаційні простори) I_b перед та I_a після здійснення суб'єктом діяльності. Якщо після діяльності спостерігаються зміни в компонентах інформації, які

становлять базис онтології (інформаційного простору), – то вважається, що діяльність над розглянутою системою була здійснена.

Застосування такого підходу до задач інформаційної безпеки дозволяє використовувати лише об'єктивні характеристики та параметри. Важливою перевагою є те, що при цьому в рамках єдиного методу описувати діяльність всіх суб'єктів інформаційної безпеки – і окремих людей, і їх об'єднань: підприємств, суспільних інститутів, суспільства та держави.

Метою статті є розробка методів моделювання діяльності суб'єктів інформаційної безпеки з використанням множини операторів, що діють в онтологіях предметних областей.

Основна частина

Спочатку опишемо математичний апарат, який буде застосовано до опису задач інформаційної безпеки.

В подальшому викладі терміни «інтер'єр» або «інтер'єр діяльності» будуть розглядатися як тотожні терміну «предметна область діяльності».

Визначення 1. Перетворення (зміну) *наповнення* базових компонент онтології (інформаційного простору) будемо називати *діяльністю*.

Розглянемо об'єкт, який здатний здійснити управління в сенсі, описаному вище. Для нього можна дати таке визначення:

Визначення 2. Об'єкт, який сприймає наповнення компонент онтологій, і який здатний трансформувати (змінювати, перетворювати) наповнення компонент онтологій, називається *абстрактним інформаційним автоматом (АІА)*.

Зауваження. Підкреслимо, що АІА оперує, у загальному випадку, двома *різними* онтологіями, навантаженими *однієї й тою ж самою* ціллю діяльності (інформаційними просторами задачі). Першу онтологію він «будує» *перед* прийняттям рішення, і вона для нього *програмуючу роль*. Другу онтологію АІА будує вже *після* здійснення діяльності (наприклад, управляючого впливу), і служить вона для того, щоб визначити, чи досягнута ціль діяльності.

В наведеному визначенні явно виділена здатність АІА до зміни наповнення компонент онтології, – наприклад, до зміни станів і/або процесів у системі. Фактично, АІА розглядається як окремий самостійний об'єкт (певна окрема система), який здатний, у відповідь на вплив зовнішніх чинників, відповідним чином змінювати деякі характеристики зовнішнього по відношенню до себе середовища.

Остаточно, АІА може розглядатися як об'єкт, який має таку структурну будову:

$$< input \mid output > . \qquad (2)$$

Сконструйовані в такий спосіб АІА своїм першим блоком сприймають (засвоюють) наповнення певних компонент онтологій та трансформують їх у компоненти онтологій (загалом кажучи – інші), в рамках яких і можна описати діяльність цього АІА (його «творчість», «керування», управління»). Іншими словами АІА, який побудовано відповідно до такого правила, може розглядатися як об'єкт, який реалізує набір методів (алгоритмів, режимів, способів, технологій) для здійснення діяльності.

Введений вище АІА може розглядатися як оператор, який діє в просторі онтологій предметних областей, навантажених *фіксованою* ціллю.

Для цього, користуючись побудованим базисом онтології, можна записати довільну інформацію про предметну область (інтер'єр) діяльності в такому вигляді

$$I = \sum_{k=1}^{8} I_k \cdot \vec{i}_k , \qquad (3)$$

де

i_k — базисні вектори простору компонент інформації (вони задають просто назви компонент онтології),

I_k — характеристики, які можуть бути віднесені до даної компоненти онтології (тобто наповнення цих компонент інформацією).

Таким чином, співвідношення (3) розуміється в тому сенсі, що I_k являє собою базу даних, яка відноситься до певного заданого класу інформації, яка описує саме цю компоненту онтології діяльності для розглядуваної нами задачі. В цьому сенсі «точка» в онтологічному просторі є сукупністю баз даних, які не перетинаються між собою, і кожна із яких відноситься тільки і тільки до однієї компоненти інформації, – див. (1).

Відмітимо, що I_k не є числом, внаслідок чого операція «покомпонентного додавання» повинна бути визначена як об'єднання двох однорідних (тобто таких, які описують ту ж саму компоненту онтології) баз даних в одну (наприклад, в рамках реляційної моделі даних). «Покомпонентне віднімання» визначається аналогічно. Операція множення на число, яка необхідна для завершення побудови лінійного простору, відповідає зміні масштабу для одиниць вимірювання при описі даних (відмітимо, що в її наявності немає необхідності, і в подальшому вона не використовується). В цьому сенсі запис (3) являє собою певне узагальнення лінійного простору. Підкреслимо, метрика в інформаційному просторі не вводиться, тобто «відстань» між точками в нашому підході не визначається.

Таким чином, діяльність може бути представлена у вигляді оператора G, який перетворює онтологію I_{before}, яка була побудована (задана) перед здійсненням акту діяльності, в онтологію I_{after} для цього ж інтер'єру діяльності, але яка побудована вже після здійснення акту діяльності. Сказане можна записати в такий спосіб:

$$I_{after} = G \cdot I_{before} . \qquad (4)$$

Неважко побачити, що визначений таким чином оператор G має таку властивість: якщо онтологія (інформаційний простір) розбивається на два підпростори I_{b1} і I_{b2}, які не перетинаються, то $G(I_{b1} + I_{b2}) = G(I_{b1}) + G(I_{b2})$. Ця властивість є наслідком тієї обставини, що розв'язання сукупності задач, кожна із яких отримується шляхом декомпозиції основної (складної) задачі на взаємодоповнюючі частини, кожна із яких розв'язується окремо, є рівнозначною розв'язанню початкової складної задачі. Звичайно, це виконано у випадку, коли ефекти синергії та нелінійності відсутні. Але це, власне, й означає, що підпростори I_{b1} і I_{b2} онтології не перетинаються (тобто не мають спільних точок).

Таким чином, якщо інформаційний простір I_{before} розбивається на пряму суму підпросторів (1), то внаслідок цього оператор G діє в такий спосіб:

$$I_a = \sum_k \oplus I_a^k = G\left(\sum_k \oplus I_b^k \right) = \sum_k \oplus G\left(I_b^k\right). \qquad (5)$$

У загальному вигляді із (5) випливає, що оператор G може бути представлений як тензорний оператор, у якого є n «нижніх» і m «верхніх» індексів. При цьому, в силу

наявності в онтології базису із восьма компонент, кількість як «верхніх», так і «нижніх» компонентів у тензора G_n^m обмежена 8: $n, m \le 8$.

Умовимося для простоти запису, що «нижні» компоненти відповідають компонентам інформації для інформаційного простору I_{before}, а «верхні» – відповідно для I_{after}.

Застосовуючи «умову Ейнштейна» про те, що за повторюваним індексах здійснюється сумація, (4) може бути переписане у такому вигляді.

$$I_a^{k1,k2,\dots} = G_{s1,s2,\dots}^{k1,k2,\dots} \cdot I_b^{s1,s2,\dots}. \qquad (6)$$

Використовуючи властивість (1) і (5), приходимо до висновку, що дія будь-якого тензорного оператора G_n^m виражається через дію суми $\max\{n, m\}$ квазілінійних операторів, які мають вигляд g_k^i.

Це твердження може бути сформульоване у вигляді такої теореми.

Теорема 1. Для здійснення будь-якої діяльності необхідно та достатньо наявності тільки таких AIA, які програмуються всього однією компонентою онтології I_{before} і діяльність яких виражається також у зміні всього однієї компоненти із онтології I_{after} (тобто результуюча зміна при переході від I_{before} до I_{after} полягає в зміні в онтології I_{after} всього однієї компоненти в порівнянні із онтологією I_{before}).

Доведення. Справедливість цієї теореми ґрунтується на тій обставині, що онтологія являє собою повний простір даних (відомостей, характеристик, параметрів тощо), які відносяться до розглянутої нами задачі.

У цьому сенсі будь-який оператор AIA: $I_{before} \to I_{after}$ діє як автоморфізм, тобто, по суті, не змінює нашої онтології: змінюється тільки «наповненість» її координат, тобто чисельні (або інші) значення її компонент. Для інших «двокомпонентних» AIA результат дії «попереднього» AIA є програмуючою онтологією. Ланцюжок можна продовжувати доти, поки це необхідно.

Достатність теореми випливає із тієї обставини, що, порівнюючи тільки «початкову» і «кінцевий» онтології між собою, ми не зможемо визначити, чи було управління здійснене оператором G_n^m, чи воно було здійснено сукупністю послідовно застосованих «двокомпонентних» операторів g_k^i. •

Символом «•» буде в статті позначатися закінчення доведення чи прикладу.

Іншими словами, ми можемо «замінити» одне управління, яке ґрунтується на сукупності компонент із онтології на суму послідовно застосовуваних актів діяльності, кожен із яких «задіює» усього одну компоненту із онтології I_{before} і результат застосування якого виражаємося в зміні всього однієї компоненти із онтології I_{after}. Це «майже очевидне» твердження являє собою, по суті, стандартний метод «розбиття» складної задачі на послідовні етапи. Як правило, досить часто таке розбиття на послідовні етапи здійснюється суб'єктом діяльності «навіть не замислюючись», як «очевидне».

Таким чином, в силу теореми 1, кожен оператор, який відповідає AIA, може бути виражений як сума певних «бінарних» операторів, що зв'язують між собою всього дві компоненти онтології: одну із простору I_{before}, а іншу – із простору I_{after}. Математично це можна записати таким чином.

$$g_{(n)}^{(m)} = \sum_{k=1}^{\max(n,m)} g_{(k)_i}^{\ j} . \qquad (7)$$

Неважко побачити, що для введених операторів g_k^i будуть справедливі такі теореми.

Теорема 2. Оператор g_k^i має властивість бути комутативним $g_k^i + g_p^l = g_p^l + g_k^i$ та асоціативним $g_1 + (g_2 + g_3) = (g_1 + g_2) + g_3$.

Доведення випливає із властивостей операторів g_k^i.

Теорема 3. Загальна кількість операторів g_k^i становить 64 різних варіантів.

Доведення. Бінарний оператор g_k^i може мати лише одну із восьми компонент з інформаційного простору I_{before} і лише одну із восьми компонент із інформаційного простору I_{after}. Кількість різних можливих варіантів становить 8×8=64. •

Наведемо ряд прикладів, які описують застосування операторів g_k^i для опису діяльності, включаючи діяльність в сфері розв'язання задач інформаційної безпеки. Відмітимо, що наведений вище метод моделювання діяльності, в його *практичному* застосуванні, відповідає переліку спеціальним чином структурованих *функціональних обов'язків*, які повинен виконувати суб'єкт діяльності.

Приклад 1. Розглянемо відцентровий (рос. центробежный) регулятор, прикладом якого є регулятор Уатта. З точки зору введених вище АІА він являє собою управління, яке влаштоване за таким алгоритмом.

$$< процес \mid стан > \qquad (8)$$

Звичайно, при цьому розглядається цілком певна характеристика об'єкту, який підлягає управлінню. Регулятор відслідковує певну характеристику об'єкту, після чого здійснює свою діяльність таким чином, щоб досягти її незмінності – тобто щоб досягти певного стану (заданого для цієї характеристики). •

Приклад 2. Іншим прикладом слугує регулятор, який не допускає, наприклад, флаттер (сукупність самозбуджених незатухаючих крутильних та згинальних коливань конструкцій літака, що призводять до його руйнування). В цьому випадку АІА, який здійснює діяльність, влаштовано «навпаки».

$$< стан \mid процес > \qquad (9)$$

В цьому випадку також розглядається цілком певна характеристика об'єкту, який підлягає управлінню.

Регулятор (9) відслідковує набір цілком *значень* (тобто *станів*) певних характеристик об'єкту, що управляється. А його діяльність полягає в започаткуванні *процесів*, які направлені на *зміну* «критичних» для об'єкту значень тих же самих характеристик.

Цікаво, що за аналогічним алгоритмом (9) також можна описати цілий клас регуляторів, які мають своєю ціллю недопущення параметричного резонансу елементів конструкції об'єкту (наприклад, які відповідають так званим «язикам Арнольда»). •

Підкреслимо, що в прикладах 1 та 2 розглядалися такі АІА, для яких інші полюси дихотомій компонент інформаційного простору є *однаковими*.

Приклад 3. В загальному вигляді *негативний* зворотній зв'язок задається виразом (8). Але, на відміну від попередніх прикладів, в ньому вже можуть використовуватися *декілька* компонент інформаційного простору задачі. •

Приклад 4. Позитивний зв'язок задається виразом (9), де теж, в загальному випадку, можуть використовуватися декілька компонент інформаційного простору задачі. •

Як видно із прикладів 3 та 4, велика частина стандартних задач загальної теорії управління та кібернетики в цілому допускає використання концепції АІА в якості стандартизованих елементів.

Але предметна область застосування АІА значно ширша, аніж теорія управління та кібернетика. Наведемо приклад, коли АІА можуть бути використані в якості аналога «природної мови» для побудови інтелектуальних систем в інформаційних технологіях.

Розглянемо спеціальний клас АІА – двокомпонентні АІА (скорочено 2АІА), кількість яких є *меншою* за 64, але які дозволяють описати будь-яку діяльність. Дамо для них таке визначення (назви базисних компонент інформації наведено в табл. 1).

Визначення 3. АІА називається двохкомпонентним (2АІА), якщо він задовольняє таким умовам:

1) Кожен 2АІА сприймає тільки одну компоненту інформації і здійснює діяльність теж тільки в рамках однієї компоненти інформації.

2) Для кожного 2АІА одна компонента описує статичність, а інша – динамічність.

3) Для кожного 2АІА одна компонента є узагальнюючою, а інша – деталізуючою.

Коректне визначення 2АІА саме як об'єкта, що реалізує ті або інші режими (типи, способи, алгоритми, методи, шляхи) діяльності, можливе тільки так, як описано вище.

Перша умова відповідає теоремі 1.

Друга умова також є необхідною. Дійсно, якщо допустити, наприклад, що 2АІА і програмуються процесом, і творять також процес, то також не одержимо оптимальної діяльності. По суті, тут також підійде принцип «бритви Оккама»: бо все рівно прийдеться вводити такі 2АІА, які мають вигляд <*стан* | *процес*> – так само як і <*процес* | *стан*>, бо тільки такі «додаткові» 2АІА можуть дозволити нам організувати «спілкування» у середовищі таких 2АІА. Наприклад, це необхідно для того, щоб «ставити завдання» перед такими АІА.

Нарешті, розглянемо третю умова. Припустимо, що ми визначили 2АІА таким чином, щоб одні з них реалізовували діяльність (тобто і програмувалися, і творили) тільки за деталізуючими компонентами, а інші тільки за узагальнюючими. У цьому випадку прийдеться вводити спеціальний новий тип 2АІА, який би «аналізував» ситуацію за допомогою узагальнюючих компонент онтології, – а роздавав би завдання вже для «деталізуючих типів 2АІА». Отже, третя умова також випливає із вимоги оптимальності для управління, реалізованого системою 2АІА («бритва Оккама»: не потрібно множити сутності без необхідності).

Відзначимо також, що при будь-якому іншому визначенні 2АІА їхня кількість буде більшою: отже, введений нами клас 2АІА є в цьому сенсі «мінімально необхідним».

Таким чином, 2АІА перетворює одну компоненту інформації (за допомогою своєї «сприймаючої функції») в іншу (за допомогою своєї «творчої, діяльнісної функції»).

Можна сказати, що,2АІА влаштовані так, що одна з їхніх компонент (будемо для неї також використовувати назву «функція») відповідає узагальненому опису предметної області, а друга її компонента відповідає конкретним одиничним об'єктам, із яких вона складається. Схематично це показано на рис. 1, де через Узаг і Дет позначені узагальнююча та деталізуюча компоненти інформації, відповідно. З рис. 1 видно, що клас 2АІА створює кільця зворотного зв'язку.

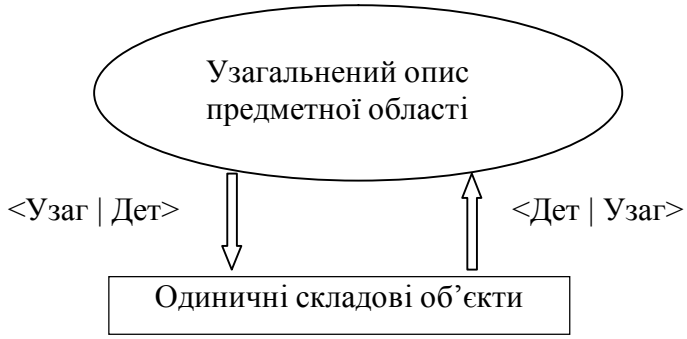


Рис. 1. 2AIA як об’єкти, що здійснюють перетворення компонент інформації в онтології предметної області

Підрахувати кількість різних типів 2AIA можна в такий спосіб. По-перше, у якості «вхідної» компонента може бути обрано будь-яку компоненту онтології. Значить – є вісім різних можливостей. А для другої потрібно відкинути ряд варіантів вибору для компонент онтології. Спочатку потрібно відкинути всі ті компоненти, які описують ту ж саму часову динаміку – тобто чотири компоненти онтології (наприклад, якщо вхідна компонента є статичною, то вихідна компонента інформації не може бути статичною). Далі повинні бути відкинуті компоненти онтології, які описують той же самий рівень, що і для вхідної компоненти онтології (наприклад, якщо вхідна компонента онтології є узагальнюючою – то вихідна компонента онтології узагальнюючої бути не може). Більше обмежень у визначенні 2AIA немає. В результаті залишаються 2 компоненти онтології, які можуть використаними в якості вихідної – за умови, коли вхідна компонента онтології є заданою. Наприклад, якщо вхідна компонента онтології є узагальнюючою та динамічною, то в якості вихідної можна взяти будь-яку компоненту із двох: статичну та деталізуючу (тобто або *Об-С* або *Зв-С*). Разом: вісім можливих варіантів входу помножити на два можливих варіанти виходу матимемо 16 різних типів 2AIA.

Таким чином, приходимо до такої теореми.

Теорема 4. Несуперечлива діяльність в загальному вигляді може бути здійснено сукупністю із 16-ти типів 2AIA, які мають наступний вигляд:

<Ст-С|Зв-Д>, <Ст-С|Об-Д>, <Ст-Д|Зв-С>, <Ст-Д|Об-С>,
<Гр-С|Зв-Д>, <Гр-С|Об-Д>, <Гр-Д|Зв-С>, <Гр-Д|Об-С>,
<Об-С|Ст-Д>, <Об-С|Гр-Д>, <Об-Д|Ст-С>, <Об-Д|Гр-С>,
<Зв-С|Ст-Д>, <Зв-С|Гр-Д>, <Зв-Д|Ст-С>, <Зв-Д|Гр-С>.

При записі типів 2AIA використані найменування компонент інформації, наведені в табл. 1. Перша компонента онтології відповідає входу в 2AIA, тобто опису тієї компоненти онтології, якою цей 2AIA програмується до дії (тобто яку він сприймає), а друга компонента – описує ту компоненту онтології, у рамках якої може бути виражена його діяльність. Нагадаємо, що ці компоненти онтології беруться в різні моменти часу.

Умови Теореми 1 і Теореми 4 приводять до такої теореми.

Теорема 5. Для здійснення довільної управлінської діяльності в довільній предметній області необхідно та достатньо наявності 16-ти типів 2AIA.

Іншими словами, для будь-якого інтер’єру реалізації як завгодно складної та витонченої діяльності необхідно та достатньо мати всього лише такі 16 типів 2AIA, які визначені вище.

Результат нашого розгляду вийшов досить нетривіальним: ми, по суті, побудували класифікацію всіх можливих типів діяльності. Теорема 5 говорить, що «інших типів» бути просто не може. Роз’яснимо це твердження більш докладно. Внаслідок Теореми 1 для здійснення довільно взятої діяльності в предметній області необхідно та достатньо мати набір тільки із *двокомпонентних* AIA. У відповідності із

Теоремою 4 несуперечливе управління можуть здійснювати тільки 16 спеціальним чином сконструйованих типів АІА, які ми позначили як 2АІА. Відмітимо, що в [6] доведено, що 2АІА є детермінованими скінченними автоматами.

В [4] доведено, що *раціональна* діяльність довільної людини повністю описується в рамках одного і тільки одного типу 2АІА.

Наведемо приклади застосування розробленого математичного апарату до задач інформаційної безпеки.

Розглянемо задачі забезпечення інформаційної безпеки держави. Суб'єктами інформаційної безпеки держави є суспільні та державні інститути та структури, угрупування людей, а також окремі індивіди. Опишемо приклади моделей діяльності деяких таких суб'єктів.

Приклад 5. Прокуратура як державний інститут повинна забезпечувати *виконання законів* в державі. Тобто результатом її діяльності повинен бути *стан*, а відслідковувати (програмуватися) вона повинна *відхиленнями* від цього стану, – тобто *процесом*. Таким чином, прокуратура повинна діяти в рамках *негативного* зворотного зв'язку, тобто в рамках формули (8). Більш того: закони формуються в рамках узагальнюючих компонент онтологій, тому програмуватися прокуратура повинна *узагальнюючими* компонентами, а результатом її діяльності є *деталізуючи* компоненти (наприклад, конкретні дії суб'єктів). Подальша деталізація компонент онтологій є неможливою: тут можуть бути різні варіанти. Таким чином, діяльність прокуратури може моделюватися як оператор G у вигляді $<Ст\text{-}Д,\ Гр\text{-}Д|Об\text{-}С,\ Зв\text{-}С>$, або відповідними чотирма відповідними типами 2АІА із теореми 5. Це означає, до речі, що діяльність прокуратури можна повністю звести до діяльності *окремих типів* 2АІА (наприклад, вона може бути здійснена конкретними людьми).

Використання прокуратури як державного інституту в рамках інших компонент онтологій предметної області законодавства буде суперечити її ролі, і приведе до зниження рівня інформаційної безпеки держави. •

Приклад 6. Інститут суду (юстиції) в державі повинен забезпечувати *рівновагу* в суспільстві. Це значить, що повинен програмуватися *станом* суспільства, а результатом його діяльності також повинен бути *стан* (той же, або *інший*). Таким чином, к вигляді оператора G діяльність судової системи записується у вигляді $<Стан|Стан>$.

Виконання такої діяльності неможливо забезпечити однією людиною, і тому в рамках судового процесу обов'язково повинні приймати участь *декілька* людей (звичайно, крім самого порушника закону, – втім, в рамках судового процесу він розглядається не як суб'єкт, а в якості об'єкту для застосування норм права). Власне, *інститут адвокатури* (а також інститут присяжних) виник саме в якості механізму, який призваний забезпечити *виконання діяльності* інститутом суду за допомогою *людей* (кожен із яких має конкретний тип 2АІА).

Так як, відповідно до прикладу 5, інститут прокуратури як учасник судового процесу може бути представлений у вигляді $<Процес|Стан>$, то діяльність інституту адвокатури повинна виглядати як $<Стан|Процес>$, тобто забезпечувати *позитивний* зворотний зв'язок. Таким чином, інститут суду дійсно *здатний забезпечити* встановлення рівноваги в результаті *змагальності* прокуратури та адвокатури.

Відмітимо, що судова система держави може бути використана за двома *різними* каналами. Перший визначається оператором G $<Стан|Стан>$, тобто діяльністю із *збереження* існуючого в суспільстві та державі стану. Цей канал відповідає континуальному (або кодексному) праву, характерному, в тому числі, і для України. Другий канал визначається оператором G, який має вигляд $<Стан\text{-}1|Стан\text{-}2>$, тобто за цих умов діяльність судової системи держави здатна *змінювати* існуючий у суспільстві та державі стан. Цей другий канал відповідає *прецедентній* правовій системі. Короткий історичний огляд формування та порівняння прецедентної та континентальної судових

систем як суспільних інститутів здійснено в [7], де доведено, що *адаптаційні* властивості кращі для прецедентного права. Підкреслено, що на етапі *трансформації* в суспільстві та державі, прецедент не право дозволяє різко *знизити* рівень суспільної напруженості та запобігти революційним виступам населення.

Цікаво, що в Україні Верховний Суд працює *частково* також і в рамках прецедентного права: ряд його рішень можуть бути використані судами нижчої інстанції в якості прецедентів. •

Приклад 7. Законодавча та виконавська системи влади в країні виконують діяльність в рамках оператора G, який має вигляд $<Узаг|Дет>$: вони, виходячи із «інтересів держави», здійснюють діяльність з управління конкретними об'єктами та суб'єктами держави.

Отже, із «трьох гілок влади» в держави дві гілки працюють в одному напрямку: від інтересів держави, якій вони підпорядковують інтереси суб'єктів більш низького рівня ієрархії (підприємств, суспільних груп та окремих індивідів). Судова влада в рамках контингентного права також підпорядковує інтереси громадян інтересам держави.

Таким чином, в ряді держав (в тому числі і в Україні) спостерігається явне домінування держави практично у всіх сторонах життя людей.

Для забезпечення потрібного рівня інформаційної безпеки держави необхідно, щоб в ній цей «перекіс» урівноважувався суспільними інститутами, діяльність яких описується в рамках оператора G $<Дет|Узаг>$. Діяльність цих інститутів полягає в *інформуванні* гілок державної влади щодо явищ та реалій суспільного життя. Фактично, тільки за їх наявності формується *кільце* зворотного зв'язку, яке показано на рис. 1.

Саме таку інформаційну будову мають ЗМІ та громадські організації (включаючи політичні партії). Саме тому в *розвинених* країнах велика увага приділяється тому, щоб ці суспільні інститути були *незалежні* від держави. •

Таким чином, розроблений математичний апарат можна використовувати для аналізу широкого кола задач інформаційної безпеки держави, притому як на макрорівні, так і на рівні забезпечення інформаційно-психологічної безпеки людини, суспільства та держави. При цьому виникає можливість конструювати інформаційні системи, які складаються із суб'єктів інформаційної безпеки, з використанням фрагментів, які описуються відповідними АІА та 2АІА.

Висновки

В статті розроблено математичний апарат та метод моделювання діяльності суб'єктів інформаційної безпеки. Метод моделювання базується на використанні множини операторів, що діють в спеціальним чином структурованих онтологіях предметних областей, навантажених ціллю. Доведено, що довільний оператор можна звести до двокомпонентного, дія якого зв'язує дві компоненти онтології, одну до, а другу після здійснення діяльності. Побудовано множину із мінімальної кількості двокомпонентних абстрактних інформаційних автоматів (2АІА). Наведено ряд прикладів застосування розробленого методу моделювання до опису суб'єктів інформаційної безпеки.

Список літератури

1. Андреєв, В.І. Основи інформаційної безпеки: підручник / В.І. Андреєв, В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест; Держ. ун-т інформ.-комунікац. технологій. — 2-ге вид., доповн. і переробл. — К., 2009. — 293 с.

2. Манойло, А.В. Государственная информационная политика в особых условиях [Текст] : монография / А.В. Манойло. — М. : МИФИ, 2003. — 388 с.
3. Шиян, А. А. Информационное пространство и классификация стратегий управленческой деятельности в теории игр и принятия решений / А.А. Шиян // Інформаційні технології та комп'ютерна інженерія. — 2007. — № 3(10). — С. 131–139.
4. Шиян, А.А. Теоретико-ігровий аналіз раціональної поведінки людини та прийняття рішень в управлінні соціально-економічними системами [Текст] : монографія / А.А. Шиян ; Вінниц. нац. техн. ун-т. — Вінниця : Універсум - Вінниця, 2009. — 404 с.
5. Handbook on Ontologies: International Handbooks on Information Systems / Eds. S. Staab and R. Studer. — 2nd edition. — Berlin : Springer, 2009. — 832 p.
6. Шиян, А.А. Механізм та технології для управління колективом на основі моделі детермінованих скінченних автоматів / А.А. Шиян, Л.О. Нікіфорова, Т.К. Мещерякова // Вісник Хмельницького національного університету. Економічні науки. — 2012. — № 2, Т. 1. — С. 46–49.
7. Шиян, А.А. Управління формуванням ефективних економічних інститутів в умовах України [Текст] : монографія / А.А. Шиян, Л.О. Нікіфорова ; Вінниц. нац. техн. ун-т. — Вінниця : ВНТУ, 2011. — 300 с.

МЕТОД МОДЕЛИРОВАНИЯ ДЕЯТЕЛЬНОСТИ СУБЪЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ ОПЕРАТОРОВ, ДЕЙСТВУЮЩИХ В ОНТОЛОГИЯХ ПРЕДМЕТНЫХ ОБЛАСТЕЙ

А.А. Шиян

Винницкий национальный технический университет,
ул. Хмельницкое шоссе, 95, Винница, 21021, Украина; e-mail: aa_shiyan@mail.ru

В статье разработан математический аппарат и метод моделирования деятельности субъектов информационной безопасности, который базируется на использовании множества операторов, действующих в специальным образом структурированных онтологиях предметных областей, которые нагружены целью. Доказано, что произвольный оператор можно свести к определенной совокупности двокомпонентных операторов, действие которых связывает две компоненты онтологии, одну до, а вторую после осуществления деятельности. Описан ряд примеров применения разработанного метода к моделированию деятельности субъектов информационной безопасности.

Ключевые слова: информационная безопасность, метод, онтология, деятельность, предметная область, субъект

A TECHNIQUE TO MODEL THE ACTIVITIES OF INFORMATION SECURITY SUBJECTS INVOLVING THE APPLICATION OF OPERATORS ACTING IN DOMAIN ONTOLOGIES

Anatoliy A. Shiyan

Vinnytsia National Technical University,
95 Khmelnytske shose, Vinnytsia, 21021, Ukraine; e-mail: aa_shiyan@mail.ru

In this work, a mathematical apparatus for, and a technique to model, information security subjects were developed based on application of operators acting in specially-structured domain ontologies loaded with a target. It was proved, that an arbitrary operator can be reduced to a definite collection of two-component operators, with the action of the latter binding the first and second components of onthology before and after performance of the activity, respectively. Several examples of application of the technique developed to model the activity of information security subjects were given.

Keywords: information security, method, ontology, activity, subject area, subject

УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 4, pp. 353-360

СТІЙКЕ СТЕГАНОПЕРЕТВОРЕННЯ В ПРОСТОРОВІЙ ОБЛАСТІ ЗОБРАЖЕННЯ-КОНТЕЙНЕРА

В.М. Рудницький[1], **О.В. Костирка**[2]

[1] Черкаський державний технологічний університет,
бул. Шевченка, 460, Черкаси, 18006, Україна
[2] Академія пожежної безпеки імені Героїв Чорнобиля ДСНС України,
вул. Онопрієнка, 8, Черкаси, 18034, Україна; e-mail: chaykaov@rambler.ru

У роботі пропонується новий стеганографічний метод, стійкий до збурних дій, який здійснює вбудову додаткової інформації в просторовій області зображення-контейнера. Як збурну дію детально досліджено накладення різних шумів з різними параметрами (гауссівського, мультиплікативного, пуассонівського) на цифрове зображення. В ході дослідження встановлена залежність основного параметра розробленого методу – величини збурення яскравості пікселів блоку контейнера при стеганоперетворенні від розміру блоку.

Ключові слова: стеганографічний метод, цифрове зображення, просторова область зображення, збурна дія, гауссівський шум, мультиплікативний шум, пуассонівський шум

Вступ

Розвиток і вдосконалення комплексної системи захисту інформації сьогодні неможливо без наявності в її складі ефективної стеганографічної системи, що ґрунтується на сучасних стеганографічних алгоритмах [1–3]. Стеганографування може застосовуватися як для прихованої передачі конфіденційних даних, так і для захисту від несанкціонованого використання інформаційного контенту шляхом вбудовування в контейнер цифрових водяних знаків [2]. Найчастіше як контейнер, або основне повідомлення (ОП), сьогодні використовуються цифрові зображення (ЦЗ), файли аудіо й відеоданих [2, 3].

При розробці будь-якого стеганометоду, стеганоалгоритму для прихованої передачі даних до нього висуваються певні вимоги, зокрема:

1) стійкості до стеганоаналізу;
2) стійкості до різного роду збурних дій,
3) забезпечення надійності сприйняття стеганоповідомлення (СП), яке є результатом вбудови додаткової інформації (ДІ) в ОП (ДІ будемо називати результат кодування конфіденційної інформації, що представляє, як правило, бінарну послідовність: $p_1, p_2,..., p_t,\ p_i \in \{0,1\}, i = \overline{1,t}$);
4) забезпечення достатньої прихованої пропускної спроможності стеганографічного каналу зв'язку, що організується [2];
5) малої обчислювальної складності.

У даній роботі як контейнер розглядається ЦЗ.

Вбудова ДІ, або стеганоперетворення (СПР), у загальному випадку може відбуватися як у просторовій області ЦЗ, так і в області перетворення (частотній, області сингулярного розкладання відповідної матриці і т.д.). В [4] показано практично, що просторова область ОП має певні переваги при організації СПР, у порівнянні з областями перетворення контейнера, як з погляду обчислювальної складності

відповідних алгоритмів, так і з погляду обчислювальної похибки, яка впливає на ефективності декодування ДІ. У той же час, в [5, 6] показано, що забезпечення стійкості стеганоалгоритму до збурних дій не залежить безпосередньо від того, у якій області ЦЗ-контейнера відбувається СПР. З врахуванням цього питання розробки стійких до збурних дій стеганометодів і алгоритмів, що працюють у просторовій області ЦЗ-контейнера, є своєчасним і *актуальним*.

Ціль статті й постановка завдань

В [6] отримана достатня умова забезпечення стійкості стеганографічного алгоритму до збурних дій при організації СПР у просторовій області ЦЗ-контейнера, яка зводиться до збурення яскравості пікселів кожного $l \times l$-блоку B ЦЗ-контейнера, отриманого шляхом стандартної розбивки його матриці на блоки, на значення Δb, при цьому

$$|\Delta b| = \left| \frac{\Delta \sigma_1}{l} \right| > \frac{\left\| \Delta \overline{B} \right\|_2}{l}, \qquad (1)$$

де

$\Delta \sigma_1$ — збурення максимального сингулярного числа [7] блока B при СПР,

$\left\| \Delta \overline{B} \right\|_2$ — спектральна норма [7] матриці збурення $\Delta \overline{B}$ відповідного блока $\overline{B}$ СП.

Шляхом варіювання величини Δb буде забезпечуватися стійкість стеганоалгоритмів, що розроблятимуться, до різних конкретних збурних дій.

У зв'язку з цим *метою* роботи є розробка нового стійкого до збурних дій стеганометода, що організує СПР у просторовій області ЦЗ-контейнера на основі отриманої в [6] достатньої умови забезпечення стійкості.

Як збурна дія для конкретного визначення Δb нижче буде розглядатися накладання різних шумів з різними параметрами на ЦЗ.

Для досягнення поставленої мети необхідно розв'язати наступні *задачі*:

1) Отримати оцінки значень $\left\| \Delta \overline{B} \right\|_2$ матриці збурення блоку зображення при накладанні різних найбільш часто використовуваних шумів на ЦЗ: гауссівського, мультиплікативного, пуассонівського;

2) Дослідити залежність $\left\| \Delta \overline{B} \right\|_2$ від розміру блоку l;

3) З урахуванням рішень задач 1, 2 визначити можливі значення Δb коректування яскравості пікселів блоку при СПР для різних l;

4) Отримати рекомендації для розмірів блоку при організації СПР відповідно до отриманої в [6] достатньої умови забезпечення стійкості стеганометоду до збурних дій.

Основна частина

Нехай F, $\overline{F}$ — $m \times m$-матриці ОП, СП відповідно, $p_1, p_2, ..., p_t$ — ДІ, $p_i \in \{0, 1\}, i = \overline{1, t}$. Декодовану ДІ будемо позначати: $\overline{p}_1, \overline{p}_2, ..., \overline{p}_t$, де $\overline{p}_i \in \{0, 1\}, i = \overline{1, t}$. Для кольорового зображення його формальним представленням буде не одна, а три (чотири) матриці. Однак, з врахуванням того, що вбудова ДІ часто відбувається лише в одну матрицю ЦЗ (при моделі RGB – у синю складову, як правило [2]), представлення ОП, СП у вигляді однієї матриці ніяк не обмежує область застосування запропонованого нижче стеганометоду.

Припустимо, що оцінка $\left\|\Delta\overline{B}\right\|_2$ результату передбачуваної збурної дії на блок СП відома. Основні кроки стеганометоду наступні.

Вбудова ДІ.

Крок 1. Матриця F ОП розбивається на $l\times l$-блоки. Кожний блок контейнера використовується для вбудови $k+1$ ($k\geq 0$) біт ДІ.

Крок 2. (*Вбудова ДІ в черговий блок контейнера*). Нехай B — черговий блок ОП, що використовується для СПР, а $p_i,\ldots,p_{i+k}$ — чергові біти ДІ. Вбудова ДІ проводиться шляхом збурення значень яскравості пікселів блоку B на Δb, що задовольняє (1). Кількість різних варіантів коректування яскравості визначається кількістю S різних варіантів упорядкованих бінарних послідовностей $p_i,\ldots,p_{i+k}$:

$$S=2^{k+1}. \qquad (2)$$

(Наприклад, якщо в блок B контейнера вбудовується один біт ДІ p_i ($k=0$), то кількість різних варіантів бінарної послідовності, яка містить один елемент p_i, відповідно до (2) дорівнює 2. Таким чином, при СПР необхідно забезпечити два можливі варіанти коректування значень яскравості пікселів блоку B. Це можна зробити, наприклад, використовуючи як величини збурення $+\Delta b$, $-\Delta b$). Результат – блок $\overline{B}$ СП $\overline{F}$.

У результаті пересилання й/або зберігання СП може зазнати збурень, після яких його матриця, у загальному випадку, буде відрізнятися від $\overline{F}$, а тому далі позначається $\overline{\overline{F}}$.

Декодування ДІ.

Крок 1. Матриці F контейнера в $\overline{\overline{F}}$ можливо збуреного СП розбиваються на $l\times l$-блоки. Кожний блок СП використовується для декодування $k+1$ ($k\geq 0$) біт ДІ.

Крок 2. Нехай $\overline{\overline{B}}$ — черговий блок СП, з якого декодуються біти $p_i,\ldots,p_{i+k}$ ДІ, а B — відповідний йому блок ОП.

2.1. Визначити:

$$\Delta B=\overline{\overline{B}}-B.$$

2.2. Визначити по матриці ΔB значення Δb, відповідно до якого цілком декодувати бінарну послідовність $p_i,\ldots,p_{i+k}$.

Конкретний спосіб реалізації кроків 2 при вбудові й декодуванні ДІ буде визначати конкретний стеганоалгоритм, що реалізує метод.

Ключовим моментом у запропонованому стеганометоді є оцінка значення $\left\|\Delta\overline{B}\right\|_2$ передбачуваної збурної дії, у якості якої в даній роботі розглядається накладання шуму.

Для рішення цієї задачі в середовищі *MathWorks* MATLAB був проведений обчислювальний експеримент, у якому було задіяно 200 кольорових ЦЗ (модель RGB) у форматах як з втратами (JPEG), так і без втрат (TIF) з бази NRCS [8], а також отримані непрофесійними фотографами. В ході експерименту на ЦЗ накладалися різні шуми (гауссівський, мультиплікативний, пуассонівський) з різними параметрами (варіанти значень параметрів шумів підбиралися, по можливості, так, щоб накладання шуму зберігало/не зберігало надійність сприйняття ЦЗ), після чого зображення аналізувалося. Для цього одна з колірних матриць зашумленого ЦЗ й відповідна матриця вхідного зображення аналогічним чином розбивалися на $l\times l$-блоки ($l\in\{4,8,10,12\}$),для кожного з яких визначалася спектральна норма матриці збурення

$\left\|\Delta\overline{B}\right\|_2$, що відбулося в результаті накладання шуму. Для кожного *i*-го ЦЗ, $i=\overline{1,200}$, для аналізованої колірної матриці обчислювалися: максимальне $M^{(i)}$, мінімальне $m^{(i)}$, середнє $S^{(i)}$ значення $\left\|\Delta\overline{B}\right\|_2$ по всім блокам, а також *PSNR* — пікове відношення «сигнал-шум», що отримується в децибелах (dB) і є традиційним при оцінці спотворень ЦЗ [9]:

$$PSNR = 10\cdot\log_{10}\left(255^2\Big/\left(\frac{1}{m^2}\sum_{i,j}\left(F(i,j)-(F+\Delta F)(i,j)\right)^2\right)\right),$$

де $F(i,j),(F+\Delta F)(i,j),\ i,j=\overline{1,n}$, — значення яскравості пікселів вхідного зображення з матрицею F і зашумленого з матрицею $F+\Delta F$ відповідно. Потім по всім ЦЗ обчислювалися середні значення $M^{(i)}$, $m^{(i)}$, $S^{(i)}$ і $PSNR$. Результати експерименту відображені в табл. 1–3 для гауссівського, мультиплікативного й пуассонівського шумів відповідно.

Необхідно відмітити, що оцінка візуального спотворення ЦЗ за допомогою *PSNR* в загальному випадку не є придатною для оцінки надійності сприйняття СП у стеганографії, яка носить суб'єктивний характер [10]. Оскільки основною задачею будь-якого стеганометоду є збереження в секреті наявності таємного каналу передачі інформації, що досягається, у тому числі, і за рахунок забезпечення надійності сприйняття СП, у систему стеганографічної передачі даних включається людина, що вносить додаткові, неподоланні до цього моменту труднощі у процес математичної формалізації забезпечення розглянутої вимоги. У силу цього поряд з *PSNR* оцінка спотворень ЦЗ в роботі проводиться також шляхом суб'єктивного ранжирування, відображенням якого є останні стовпці таблиць 1–3.

Таблиця 1.

Результати накладання на ЦЗ гауссівського шуму з нульовим математичним сподіванням

Дисперсія	*l*	Середні знач-я по всім протестованим ЦЗ				Збереження надійності сприйняття
		$M^{(i)}$	$m^{(i)}$	$S^{(i)}$	*PSNR* (dB)	
0.001	4	46	4	24	30	–
	8	58	21	39		
	10	63	23	44		
	12	67	32	49		
0.0001	4	15	2	8	40	+
	8	19	7	13		
	10	20	8	14		
	12	22	11	16		
0.0005	4	35	3	18	33	±
	8	41	15	27		
	10	45	18	31		
	12	48	23	35		

Таблиця 2.

Результати накладання на ЦЗ мультиплікативного шуму

Дисперсія	l	Середні знач-я по всім протестованим ЦЗ				Збереження надійності сприйняття
		$M^{(i)}$	$m^{(i)}$	$S^{(i)}$	$PSNR$ (dB)	
0.00005	4	8	1	2	49	+
	8	10	1	4		
	10	12	2	5		
	12	13	3	6		
0.0001	4	11	1	3	46	±
	8	15	2	6		
	10	17	2	7		
	12	18	3	8		
0.001	4	35	2	9	37	–
	8	42	4	15		
	10	53	4	17		
	12	57	5	21		

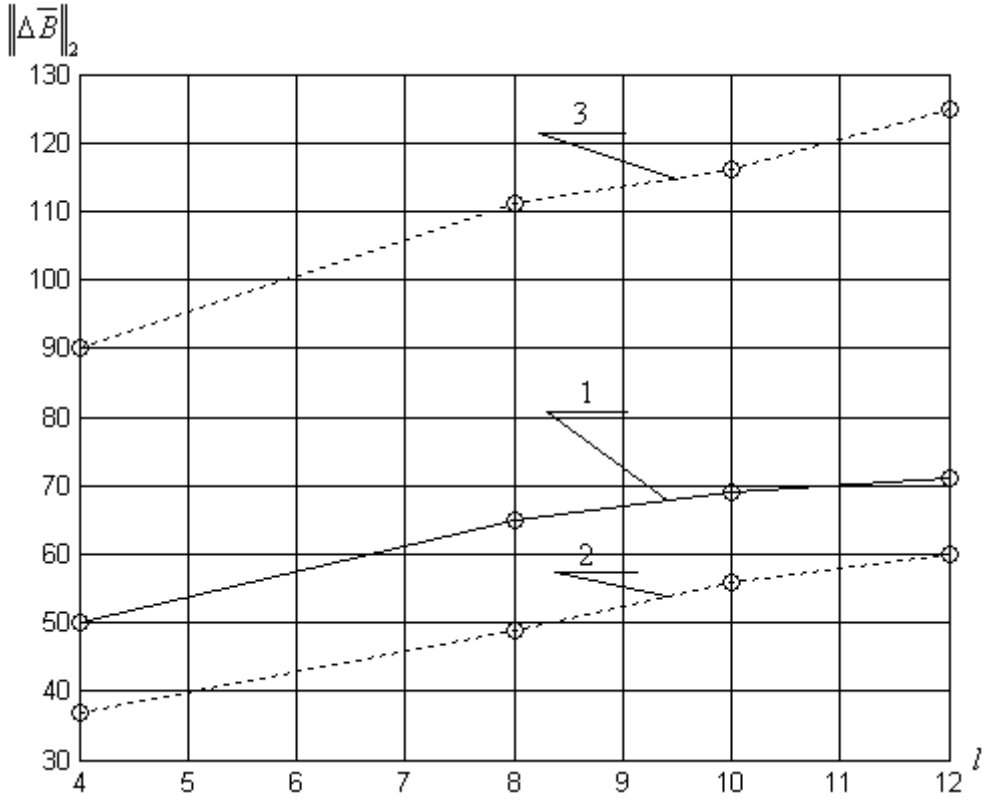
Таблиця 3.

Результати накладання на ЦЗ пуассонівського шуму

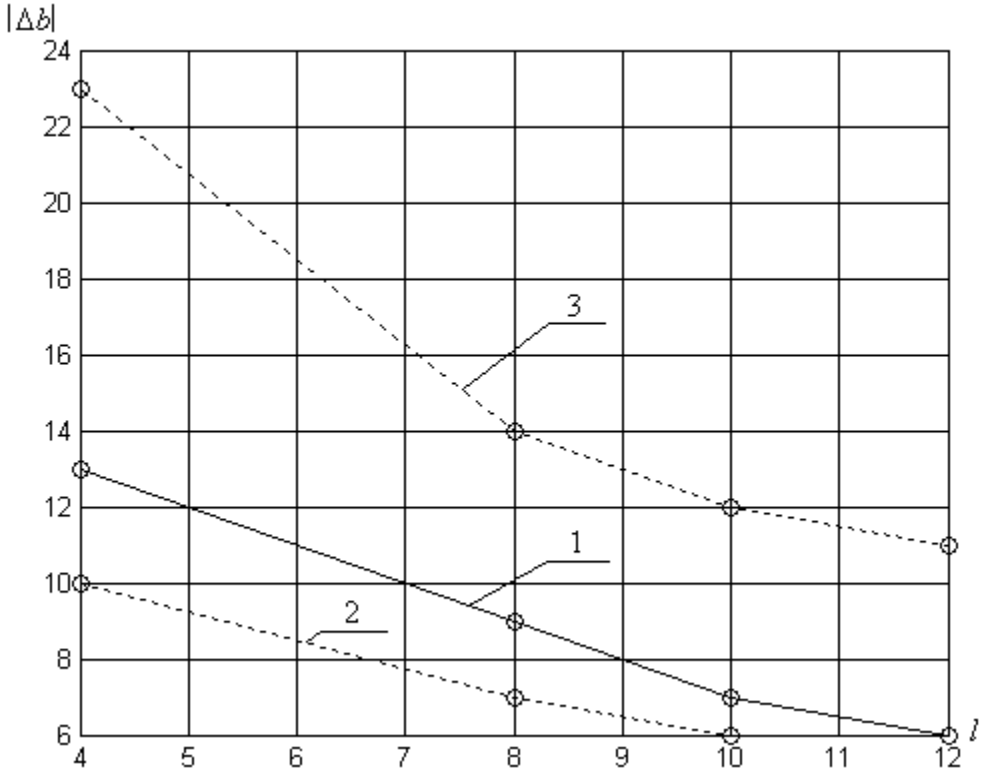
l	Середні знач-я по всім протестованим ЦЗ				Збереження надійності сприйняття
	$M^{(i)}$	$m^{(i)}$	$S^{(i)}$	$PSNR$ (dB)	
4	78	4	26	28	–
8	95	14	42		
10	102	16	47		
12	111	19	54		

У ході обчислювального експерименту фіксувалися максимальні значення $\left\|\Delta\overline{B}\right\|_2$ при кожному розмірі l блоку для кожного виду розглянутого шуму. Результати знайшли своє відображення на графіках, представлених на рис. 1(а).

Аналіз отриманих результатів (табл. 1–3, рис. 1(а)), на перший погляд, говорять про перевагу блоків малого розміру l для організації СПР відповідно до згаданої вище достатньої умови стійкості стеганометоду, оскільки $\left\|\Delta\overline{B}\right\|_2$ для таких блоків має найменше значення. Однак, з врахуванням (1), для стійкості запропонованого стеганометоду до накладання гауссівського/мультиплікативного/пуассонівського шуму з розглянутими варіантами параметрів при $l=4$ має сенс брати $|\Delta b|>\frac{50}{4}/|\Delta b|>\frac{37}{4}/|\Delta b|>\frac{90}{4}$; при $l=8$ – $|\Delta b|>\frac{65}{8}/|\Delta b|>\frac{49}{8}/|\Delta b|>\frac{111}{8}$; при $l=10$ – $|\Delta b|>\frac{69}{10}/|\Delta b|>\frac{56}{10}/|\Delta b|>\frac{116}{10}$; при $l=12$ – $|\Delta b|>\frac{71}{12}/|\Delta b|>\frac{60}{12}/|\Delta b|>\frac{125}{12}$, тобто, наприклад, ті значення, які відображені на рис. 1(б), що, враховуючи необхідність збереження надійності сприйняття СП, надає переваги блокам більшого розміру. Однак, збільшення розміру блоку приведе до зменшення прихованої пропускної спроможності стеганографічного каналу зв'язку, що відповідно з вимогою 4 до стеганоалгоритму є небажаним. Таким чином, з врахуванням усього вищесказаного, компромісними варіантами розміру блоку l є величини 8,10.



а



б

Рис. 1. Залежність від величини l при різних шумах: а – максимального значення, що мало місце в експерименті $\|\Delta\overline{B}\|_2$; б – Δb: 1 – гауссівський; 2 – мультиплікативний; 3 – пуассонівський шум

Висновки

На основі отриманої раніше достатньої умови стійкості в роботі розроблений новий стеганографічний метод, стійкий до збурних дій, що здійснює вбудову додаткової інформації в просторовій області зображення-контейнера шляхом збурення значень яскравості пікселів блоків матриці основного повідомлення.

Як збурна дія, детально досліджене накладення різних шумів з різними параметрами: гауссівського, мультиплікативного, пуассонівського. У ході дослідження встановлена залежність основного параметра розробленого методу – величини Δb збурення яскравості пікселів блоку контейнера при стеганоперетворенні, від розміру l блока.

Отримані рекомендації для величини розміру блоку l, що дозволяють забезпечити: стійкість стеганометоду до накладання шуму; надійність сприйняття формованого стеганоповідомлення; уникнути зменшення прихованої пропускної спроможності стеганографічного каналу зв'язку, що організується, за рахунок величини l.

Список літератури

1. Ленков, С.В. Методы и средства защиты информации: в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. — К.: Арий, 2008 — . — Т.2: Информационная безопасность. — 2008. — 344 с.
2. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.
3. Стеганография, цифровые водяные знаки и стеганоанализ : [монография] / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. — М.: Вузовская книга, 2009. — 220 с.
4. Костырка, О.В. Анализ преимуществ пространственной области цифрового изображения-контейнера для стеганопреобразования / О.В. Костырка // Інформатика та математичні методи в моделюванні. — 2013. — Т. 3, № 3. — С. 275–282.
5. Кобозєва, А.А. Загальний підхід до оцінки властивостей стеганографічного алгоритму, заснований на теорії збурень / А.А. Кобозєва // Інформаційні технології та комп'ютерна інженерія. — 2008. — № 1(11). — С. 164–171.
6. Кобозева, А.А. Условия обеспечения устойчивости стеганоалгоритма при организации стеганопреобразования в пространственной области контейнера-изображения / А.А. Кобозева, О.В. Костырка // Інформаційна безпека. — 2013. — № 4.
7. Деммель, Д. Вычислительная линейная алгебра [Текст] : теория и приложения / Д. Деммель; Пер. с англ. Х.Д. Икрамова. — М. : Мир, 2001. — 430 с.
8. NRCS Photo Gallery : *[Електронний ресурс]* // United States Department of Agriculture. Washington, USA. Режим доступу: http://photogallery.nrcs.usda.gov (Дата звернення: 26.07.2012).
9. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
10. Кобозева, А.А. Учет свойств нормального спектрального разложения матрицы контейнера при обеспечении надежности восприятия стегосообщения / А.А. Кобозева, Е.А. Трифонова // Вестник НТУ «ХПИ». — 2007. — № 18. — С. 81–93.

УСТОЙЧИВОЕ СТЕГАНОПРЕОБРАЗОВАНИЕ В ПРОСТРАНСТВЕННОЙ ОБЛАСТИ ИЗОБРАЖЕНИЯ-КОНТЕЙНЕРА

В.Н. Рудницкий[1], О.В. Костырка[2]

[1] Черкасский государственный технологический университет,
бул. Шевченко, 460, Черкассы, 18006, Украина
[2] Академия пожарной безопасности имени Героев Чернобыля ГСЧС Украины,
ул. Оноприенко, 8, Черкассы, 18034, Украина; e-mail: chaykaov@rambler.ru

В работе предлагается новый стеганографический метод, устойчивый к возмущающим воздействиям, осуществляющий погружение дополнительной информации в пространственной области изображения-контейнера. В качестве возмущающего воздействия детально исследовано наложение различных шумов с различными параметрами (гауссовского, мультипликативного, пуассоновского) на цифровое изображение, в ходе которого установлена зависимость основного параметра разработанного метода – величины возмущения яркости пикселей блока контейнера при стеганопреобразовании, от размера блока.
Ключевые слова: стеганографический метод, цифровое изображение, пространственная область изображения, возмущающее воздействие, гауссовский шум, мультипликативный шум, пуассоновский шум

ROBUST STEGANO TRANSFORMATION IN SPATIAL DOMAIN OF COVER IMAGE

Volodymyr M. Rudnitsky[1], Olesya V. Kostyrka[2]

[1] Cherkasy State Technological University,
460 Shevchenko Ave., Cherkasy, 18006, Ukraine
[2] Academy of Fire Safety named after Chernobyl Heroes,
8 Onoprienko str., Cherkasy, 18034, Ukraine; e-mail: chaykaov@rambler.ru

In this work, a new robust-to-distortion steganography technique ensuring embedding of additional data into the spatial domain of cover image is proposed. As a distortion, investigated was addition of various (Gaussian, multiplicative and Poisson) noises with different parameter values to digital image. Within this investigation, a relationship between the main parameter of the technique developed, the value of brightness distortion of cover block pixel during stego transformation, and the block size, was established.
Keywords: steganographic method, digital image, spatial domain, disturbance, Gaussian noise, speckle noise, Poisson noise

УДК 004.932.2

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 4, pp. 361-368

МЕТОД ЗАХИСТУ QR-КОДУ З ВИКОРИСТАННЯМ ЦИФРОВОГО ВОДЯНОГО ЗНАКУ

О.В. Наріманова, Д.М. Семенченко

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: semejka@ua.fm

В роботі розроблено новий метод нанесення та вилучення цифрового водяного знаку для захисту контенту QR-коду, що може бути використаний для перевірки цілісності та автентичності QR-коду після його зчитування за допомогою мобільного пристрою з паперового носія. На основі розробленого методу реалізовано програмний продукт для мобільного пристрою на операційній системі Windows Phone.

Ключові слова: цифровий водяний знак, QR-код, автентифікація, перевірка цілісності

Вступ

Постійне збільшення об’ємів інформації, що необхідно отримувати, аналізувати, обробляти та зберігати, призводить до появи нових інформаційних технологій. В роботі чи на відпочинку, вдома чи закордоном, людина звикла покладатися на мобільні пристрої, GPS-навігатори, отримувати бажану інформацію у будь-який час з Інтернету, інших пристроїв чи просто зчитувати її мобільним телефоном з QR-кодів [1]. На сьогоднішній день QR-коди набули такого широкого використання, що майже вся друкована інформація (рекламні та інформаційні плакати, етикетки різноманітних виробів, оголошення тощо) дублюється за допомогою QR-кодів чи супроводжується ними.

Проте, як відомо, новітні технології (особливо інформаційні) можуть бути використані і проти людини та її прав. У сьогоденні стало розповсюдженим таке явище соціальної інженерії як фішинг [2]. Суть махінацій полягає у заміні оригінального QR-коду іншим кодом, який після зчитування телефоном видає користувачеві неправдиву інформацію (приклад недобросовісної конкуренції) чи наводить останнього на web-сторінку зловмисника, що може призвести до крадіжки та/або втрати конфіденційної та персональної інформації.

Отже, використання технології QR-коду потребує залучення технологій забезпечення інформаційної безпеки. Однією з таких технологій є нанесення цифрового водяного знаку (ЦВЗ).

Мета та задачі дослідження

Метою даної роботи є розробка методу автентифікації та перевірки цілісності QR-коду за допомогою ЦВЗ.

Для досягнення мети роботи були поставленні наступні задачі:

1) Провести аналіз існуючих методів, що використовують ЦВЗ, та сформулювати основні вимоги до методу автентифікації та перевірки цілісності QR-коду;

2) Розробити метод для автентифікації та перевірки цілісності QR-коду, що використовує ЦВЗ, згідно з основними вимогами;

3) Реалізувати програмний продукт нанесення та перевірки ЦВЗ для QR-коду;

4) Провести обчислювальний експеримент для визначення точних значень параметрів розробленого методу для забезпечення виконання сформульованих вимог для організації захисту контенту QR-коду.

Основні вимоги до методу автентифікації та перевірки цілісності QR-коду за допомогою цифрового водяного знаку

QR-код (абревіатура розшифровується як *Quick Response* – «швидкий відгук») – це матрична двовимірна картинка, в якій знаходиться зашифрована інформація набагато більшого розміру, ніж вміщується в звичайний штрих-код. За допомогою QR-коду можна закодувати будь-яку інформацію, наприклад: текст, номер телефону, посилання на сайт або візитну картку. Навівши на код камеру телефону, користувач отримує закодовану інформацію на екрані. Зчитуються QR-коди за допомогою мобільного телефону, в який вбудована фотокамера і є спеціальне програмне забезпечення (спеціальний додаток для мобільних пристроїв – QR-reader).

У загальному вигляді QR-код поділяється на декілька зон, основні з яких виділені на рис. 1.

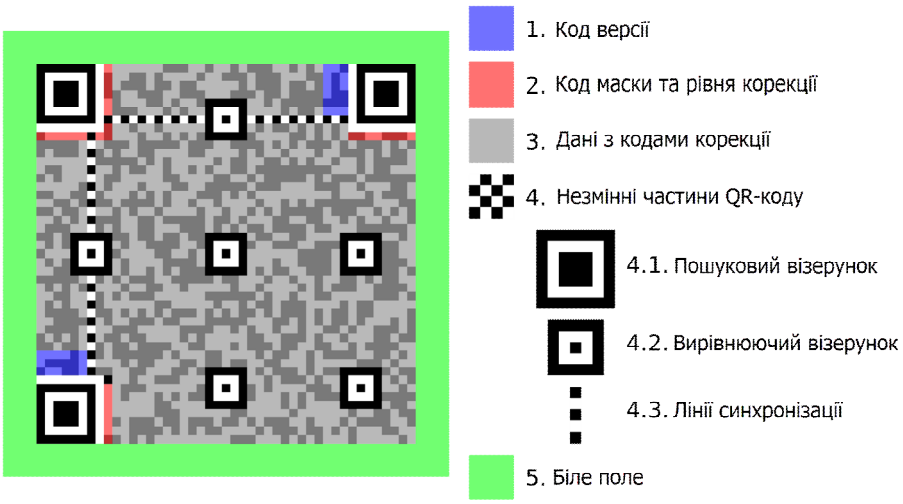


Рис. 1. Схема нанесення інформації на QR-код

З урахуванням правил формування QR-коду сформулюємо основні загальні вимоги до методу автентифікації та перевірки його цілісності за допомогою ЦВЗ. Повідомлення ЦВЗ має обиратися з урахуванням, що його довжина обмежена зверху значенням кількості байтів в QR-коді. При нанесенні цифрового водяного знаку має бути збережена (за можливості) візуальна стійкість, тобто цифровий водяний знак не повинен бути помітним для ока людини. Проте метод нанесення ЦВЗ має бути стійким до процесів друку та зчитування камерою телефону. Візуальною стійкістю можна поступитися на користь високого відсотку вірно декодованого повідомлення ЦВЗ за умови, що розпізнавання QR-коду не буде порушено. Отже, коротко основні вимоги до методу автентифікації та перевірки цілісності QR-коду можна сформулювати наступним чином:

1) Довжина повідомлення ЦВЗ не повинна перевищувати довжину повідомлення QR-коду;

2) Нанесений ЦВЗ не повинен перешкоджати зчитуванню QR-коду стандартними засобами;

3) Розроблений метод, що використовує ЦВЗ, має бути стійким до процесів друку та зчитування камерою телефону та (за можливості) задовольняти умові візуальної стійкості.

З урахуванням сформульованих основних вимог був проведений аналіз відомих технік та методів ЦВЗ.Найбільш поширеними та відомими робастними методами ЦВЗ є методи Куттера-Джордана-Боссена, Коха і Жао та їхні модифікації [3-6]. Проте вони не забезпечують ефективності вилучення повідомлення ЦВЗ після друку стеганоповідомлення на паперовому носії та зчитування камерою телефону. Тому постає задача розробки нового методу для захисту контенту QR-коду, враховуючи особливості його представлення і, насамперед, вимогу стійкості до процесів друку та зчитування камерою телефону. При розробці нового методу перевага надається роботі в просторовій області зображення, оскільки робота в частотній області вимагає додаткових обчислень та не гарантує стійкості до такого значного збурного впливу як процес друку та зчитування камерою.

Метод захисту контенту QR-коду, що використовує цифровий водяний знак

Було визначено, що найбільш доцільним для вирішення поставленої в роботі задачі є нанесення ЦВЗ на QR-код шляхом зміни значення яскравості пікселів матриці QR-коду. При цьому для підвищення стійкості повідомлення ЦВЗ до збурних дій пропонується корекція значення усіх трьох компонент зображення QR-коду: R – червоної, G – зеленої, B – блакитної. Далі необхідно визначити, які саме пікселі будуть підпадати корекції, та за яким правилом ця корекція буде виконуватися.

При формуванні QR-коду кожному біту інформації ставиться у відповідність всього один білий або чорний піксель у зображенні, проте при друці зображення QR-коду масштабується для того, щоб QR-код можна було прочитати камерою телефону. Для можливості нанесення ЦВЗ пропонується після формування QR-коду (до друку) кожному пікселю зображення поставити у відповідність 9 пікселів того ж кольору як показано на рисунку 2. Далі сукупність 3×3 пікселів будемо називати «квадрат» QR-коду.

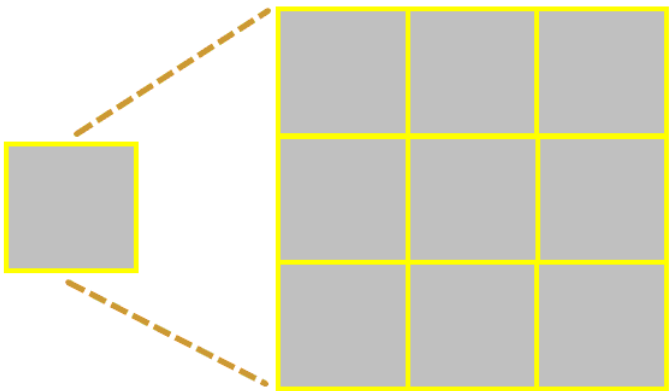


Рис. 2. Формування квадрату QR-коду для одного пікселя

Після такого масштабування QR-коду будемо проводити нанесення ЦВЗ шляхом модифікації середнього пікселя кожного квадрату 3×3.

Зауваження 1. Заміна саме середнього пікселя при зчитуванні ЦВЗ має певні переваги. По-перше, незначна корекція яскравості тільки одного з дев'яти пікселів не завадить зчитуванню безпосередньо повідомлення QR-коду стандартними засобами. По-друге, наявність корекції яскравості середнього пікселя навіть після збурного впливу можна встановити, проаналізувавши оригінальні значення сусідніх пікселів, бо первісно вони мають той самий колір.

Зауваження 2. Таке правило визначення пікселів, що підлягають корекції своїх значень, на перший погляд, дає пропускну здатність алгоритму 1/9 біт на піксель. Проте по відношенню до первісного (ще до масштабування) зашифрованого у QR-код повідомлення маємо пропускну здатність 1 біт на піксель.

Отже, було отримане правило, за яким визначаються пікселі, що підлягають корекції своїх значень. Далі необхідно визначити правило, за яким буде виконуватися корекція значень пікселів QR-коду. Пропонується наступне.

Нехай необхідно нанести повідомлення ЦВЗ, яке має послідовність біт $\{1,1,0,0\}$. Нанесення виконується на фрагмент QR-коду, який до масштабування за кожною з компонент $\{R,G,B\}$ приймає значення $\begin{Bmatrix}255,0\\255,0\end{Bmatrix}$. На рис. 3 представлена схема такого нанесення ЦВЗ.

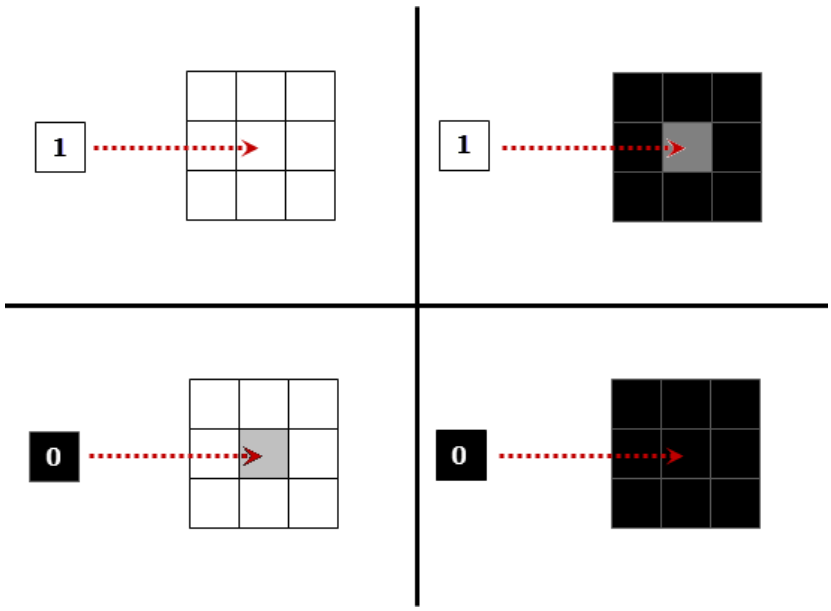


Рис. 3. Корекція значень квадрату QR-коду в залежності від біту повідомлення ЦВЗ, що вбудовується

Таким чином, корекція значення середнього пікселя квадрату QR-коду на деяке значення $\pm\Delta$ необхідна тільки у двох випадках з чотирьох: при вбудовуванні одиниці в квадрат чорних пікселів $(+\Delta)$ та нуля в квадрат білих пікселів $(-\Delta)$. Корекція значення середнього пікселя квадрату QR-коду для кожної з компонент $\{R,G,B\}$ в цих випадках виконується за наступною формулою:

$$\overline{p}_{i,j}=\begin{cases}p_{i,j}-\Delta, & p_{i,j}=255;\\ p_{i,j}+\Delta, & p_{i,j}=0.\end{cases} \qquad (1)$$

де

$p_{i,j}$ та $\overline{p}_{i,j}$ — значення яскравості середнього пікселя квадрату QR-коду до та після корекції відповідно;

Δ — значення корекції, деяке невід'ємне значення з інтервалу $(0,127)$.

Вилучення кожного біту ЦВЗ виконується у відповідності з формулами:

$$\overline{\Delta} = \frac{p_{i-1,j-1} + p_{i-1,j} + p_{i-1,j+1} + p_{i,j-1} + p_{i,j+1} + p_{i+1,j-1} + p_{i+1,j} + p_{i+1,j+1}}{8} - p_{i,j};$$

$$m_k = \begin{cases} 1, & \overline{\Delta} \le -\Delta, \overline{\Delta} + p_{i,j} \le 127; \\ 0, & \overline{\Delta} > -\Delta, \overline{\Delta} + p_{i,j} \le 127; \\ 0, & \overline{\Delta} \ge \Delta, \overline{\Delta} + p_{i,j} > 127; \\ 1, & \overline{\Delta} < \Delta, \overline{\Delta} + p_{i,j} > 127, \end{cases} \quad (2)$$

де

$p_{i,j}$ — значення яскравості середнього пікселя квадрату QR-коду після зчитування;

Δ — значення корекції з формули (1);

m_k — вилучений k-й біт ЦВЗ.

Отже, можемо визначити основні кроки алгоритмів нанесення та вилучення цифрового водяного знаку для QR-коду.

Основні кроки алгоритму нанесення ЦВЗ:

1) визначити послідовність та довжину повідомлення ЦВЗ;

2) визначити послідовність пікселів, в які буде виконуватись вбудування ЦВЗ;

3) послідовно виконати корекцію значень пікселів QR-коду, якщо це необхідно, за формулою (1).

Основні кроки алгоритму вилучення ЦВЗ:

1) визначити послідовність пікселів зображення для вилучення ЦВЗ;

2) обчислити значення біту вбудованої інформації за формулами (2).

В даному розділі представлена розробка методу ЦВЗ для захисту контенту QR-коду та наведені основні кроки алгоритмів нанесення та вилучення повідомлення цифрового водяного знаку. Для можливості практичної реалізації розробленого методу необхідно визначити таке значення корекції Δ, яке задовольняло би сформульованим у першому розділі вимогам: нанесений ЦВЗ не повинен перешкоджати зчитуванню QR-коду стандартними засобами; метод ЦВЗ має бути стійким до процесів друку та зчитування камерою телефону та (за можливості) задовольняти умові візуальної стійкості. У наступному розділі описана програмна реалізація алгоритмів нанесення та вилучення ЦВЗ для QR-коду, описаний обчислювальний експеримент та представлені його результати для визначення значення корекції Δ та перевірки стійкості розробленого методу до зазначених збурних дій.

Програмний продукт для захисту контенту QR-коду

Для програмної реалізації розроблених алгоритмів нанесення та вилучення ЦВЗ для QR-коду було обрано мобільну операційну систему Windows Phone, враховуючи розповсюдженість та перспективи розвитку мобільних пристроїв саме з цією операційною системою. Реалізація програмного продукту була проведена з використанням набору інструментів Microsoft Visual Studio 2010 Express for Windows Phone. Формування та зчитування QR-коду проводилося за допомогою стандартної для цієї задачі бібліотеки ZXing [7].

Нижче наведений приклад роботи та інтерфейс створеного програмного продукту (див. рис. 4, 5).

Рис. 4. Нанесення ЦВЗ на сформований QR код з подальшим його збереженням

Рис. 5. Відкриття QR-коду та вилучення повідомлення ЦВЗ

При проведенні обчислювального експерименту використовувалися різні значення корекції Δ з проміжку від 1 до 127. При цьому фіксувалися можливість зчитування QR-коду стандартними засобами і відсоток вірно вилученої інформації

повідомлення ЦВЗ, а також оцінювалася візуальна стійкість. При проведенні обчислювального експерименту було визначено, що для коректної та ефективної роботи програмного продукту на мобільному пристрої необхідна камера з роздільною здатністю не менше 8.0 мегапікселів. Основні результати обчислювального експерименту представлені в табл. 1.

Таблиця 1.

Результати обчислювального експерименту з використання камери з роздільною здатністю 8.7 мегапікселів

Діапазон значень корекції Δ	Можливість зчитування QR-коду стандартними засобами	Відсоток вірно вилученої інформації повідомлення ЦВЗ, %	Дотримання вимоги візуальної стійкості
$1 \div 9$	+	ЦВЗ не отримано	+
$10 \div 90$	+	100	–
$91 \div 127$	–	100	–

За представленими результатами значення корекції $\Delta = 10$ було обране для використання в алгоритмах нанесення та вилучення ЦВЗ як таке, що менше за всі порушує візуальну стійкість і при цьому задовольняє вимогам зчитування QR-коду стандартними засобами і дає 100% вірно вилученої інформації повідомлення ЦВЗ.

Висновки

В роботі розроблено новий метод нанесення та вилучення цифрового водяного знаку для захисту контенту QR-коду, що дозволяє перевіряти цілісність та автентичність QR-коду після його зчитування за допомогою мобільного пристрою з паперового носія.

В процесі розробки методу та програмного продукту на його основі були враховані особливості формування та змісту QR-кодів, а також наступні вимоги:

1) Можливість зчитування QR-коду стандартними засобами без наявного спеціалізованого програмного додатку, розробленого в даній роботі;

2) Ефективність вилучення ЦВЗ після зчитування роздрукованого на паперовому носії QR-коду камерою мобільного пристрою;

3) Незначні порушення візуальної стійкості після нанесення ЦВЗ, що є прийнятним для робастного методу ЦВЗ.

Розроблений в роботі програмний продукт для генерації QR-коду та нанесення на нього ЦВЗ може бути рекомендований для використання власними та часними підприємствами, державними установами та банками, які використовують QR-коди в будь-яких цілях. При цьому доцільним може бути використання асиметричних криптографічних алгоритмів для шифрування повідомлення ЦВЗ до його нанесення на QR-коду. Програмний продукт для зчитування і перевірки автентичності та цілісності QR-коду може бути розповсюджений у вільному доступі тим підприємством, що зацікавлений у захищеності своєї інформації або продукції і, як наслідок, своїх клієнтів.

Список літератури

1. What is a QR-code? : *[Електронний ресурс]* // QRCode.com. DENSO WAVE Incorporated. Режим доступу: http://www.qrcode.com/en/about/ (Дата звернення: 11.11.2013 р.)
2. Понимание киберпреступности: Руководство для развивающихся стран : *[Електронний ресурс]* // Международный союз электросвязи. Отдел приложений ИКТ и кибербезопасности. Департамент политики и стратеги. Сектор развития электросвязи МСЭ. Режим доступу: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFR.pdf (Дата звернення: 11.11.2013 р.)
3. Хорошко, В.О.Основи комп'ютерної стеганографії: Навч. посіб. для студ. і асп. / В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук; Нац. авіац. ун-т. — Вінниця, 2003. — 143 с.
4. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
5. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.
6. Защелкин, К.В. Усовершенствование метода стеганографического скрытия данных Куттера-Джордана-Боссена / К.В. Защелкин, А.И. Иващенко, Е.Н. Иванова // Радіоелектронні і комп'ютерні системи. — 2013. — № 5(64). — С. 151–155.
7. ZXing barcode for Windows Phone : *[Електронний ресурс]* // CodePlex. Project Hosting for Open Source Software. Режим доступу: http://zxingwindowsphone.codeplex.com/ (Дата звернення: 11.11.2013 р.)

МЕТОД ЗАЩИТЫ QR-КОДА С ИСПОЛЬЗОВАНИЕМ ЦИФРОВОГО ВОДЯНОГО ЗНАКА

Е.В. Нариманова, Д.М. Семенченко

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: semejka@ua.fm

В работе представлен новый метод нанесения и извлечения цифрового водяного знака для защиты контента QR-кода, который может быть использован для проверки целостности и аутентичности QR-кода после его считывания при помощи мобильного устройства с бумажного носителя. На основе разработанного метода реализован программный продукт для мобильного устройства на операционной системе Windows Phone.

Ключевые слова: цифровой водяной знак, QR-код, аутентификация, проверка целостности

DIGITAL WATERMARKING APPROACH FOR QR-CODE PROTECTION

Olena V. Narimanova, Daria M. Semenchenko

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: semejka@ua.fm

In this paper a new approach of digital watermarking for QR-code protection is developed. This approach can be used for authentication and integrity checking of QR-code after its reading with mobile device from paper. On the basis of proposed approach a software application for mobile device on Windows Phone is implemented.

Key words: digital watermarking, QR-code, authentication, integrity checking

УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 4, pp. 369-384

МЕТОД ВНЕДРЕНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В АППАРАТНЫЕ КОНТЕЙНЕРЫ С LUT-ОРИЕНТИРОВАННОЙ АРХИТЕКТУРОЙ

К.В. Защелкин, Е.Н. Иванова

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, Украина; e-mail: const-z@te.net.ua

Рассмотрена задача внедрения цифровых водяных знаков в информационный объект с целью контроля его использования. Отмечены типичные подходы к организации такого внедрения. Предложен метод внедрения цифровых водяных знаков в аппаратные контейнеры с LUT-ориентированной архитектурой. Показаны алгоритмы реализации предложенного метода. Описана аппаратно-программная реализация метода и результаты экспериментов в среде этой реализации. Показаны возможности применения предложенного метода для организации цифровых водяных знаков в пространстве LUT-ориентированного контейнера с целью контроля его использования в динамике проектирования и жизненного цикла.

Ключевые слова: цифровые водяные знаки, стеганография, защита информации, аппаратный стего-контейнер, LUT-ориентированная архитектура, FPGA, контроль использования FPGA-проектов

Введение

Цифровой водяной знак (ЦВЗ) представляет собой данные, внедряемые в информационный объект с целью контроля его использования. Технология ЦВЗ основана на применении стеганографических приемов, в рамках которых скрывается факт наличия ЦВЗ в информационном объекте (контейнере). При этом ЦВЗ может быть считан из контейнера при наличии стего-ключа, определяющего правила доступа к элементам ЦВЗ [1, 2].

В современных информационных системах ЦВЗ получили широкое распространение для контроля использования мультимедийного контента: растровых графических файлов, видеофайлов, оцифрованного звука [3, 4]. Существенная особенность файлов-контейнеров для такого контента состоит в том, что все они являются *пассивными* информационными объектами, выполняющими только функцию хранения данных. Очевидно, что необходимость в контроле использования информационных объектов не ограничивается только контейнерами данного вида. Такая необходимость имеет место и для *активных* информационных объектов выполняющих некоторую вычислительную или управляющую функцию.

В последнее время активизировались исследования в области использования нетрадиционных активных стего-контейнеров, как для непосредственно стеганографических задач (скрытой передачи и хранения защищенной информации), так и для задач внедрения ЦВЗ в такие контейнеры. В частности появились работы предлагающие использовать в качестве стего-контейнеров или объектов для внедрения ЦВЗ исполняемые файлы [5–7] или исходные коды программ [8, 9] микропроцессоров и микроконтроллеров.

В данной работе предлагаются подходы к внедрению ЦВЗ в аппаратные контейнеры, построенные на основе LUT-ориентированной архитектуры (далее LUT-контейнеры). К таким контейнерам относятся, например, микросхемы FPGA (*Field Programmable Gate Array*), являющиеся на текущий момент весьма используемой элементной базой для построения компьютерных и управляющих систем. По многим параметрам FPGA конкурируют с микропроцессорами и микроконтроллерами, а по параметрам производительности и возможности организации параллельных вычислений превосходят их [10].

Постановка цели работы

На текущий момент, элементная база, основанная на LUT-ориентированной архитектуре (например, микросхемы FPGA) является крайне востребованной при построении компьютерных и управляющих систем. Исходя из этого, можно констатировать перспективность исследования возможности внедрения информации в LUT-контейнеры с целью контроля их использования, а так же для организации стего-защищенных систем передачи и хранения данных на их основе. *Цель* данной работы состоит в развитии технологии цифровых водяных знаков путем ее распространения на LUT-контейнеры.

Особенности контейнеров с LUT-ориентированной архитектурой

LUT (*Look Up Table* – таблица поиска) представляет собой структуру данных, используемую с целью заменить вычисления на операцию поиска заготовленных данных [10]. Подход, основанный на применении LUT, получил название «Вычисления с памятью» (*Computing with Memory*) [11]. Наибольшего своего развития этот подход достиг в структуре программируемых логических интегральных схем (ПЛИС), в частности в наиболее современной их разновидности FPGA [12]. Упрощенно архитектура FPGA представляет собой совокупность вычислительных модулей, упорядоченных в виде двухмерной матрицы. Основную вычислительную функцию этих модулей выполняют блоки LUT, имеющие обычно 4 (реже 5 или 6) входов и 1 или 2 выхода. Блоки LUT могут быть определенным образом соединены между собой, а так же со специализированными модулями (памяти, аппаратного умножения) и выводами микросхемы. Определенная конфигурация соединения блоков LUT, а так же запись в них определенного содержимого приводит к организации, требуемой для данной задачи, вычислительной среды.

Блоки LUT в FPGA обычно представляют собой одноразрядную оперативную память. Входы блока LUT при этом являются адресными входами такой памяти (рис. 1). При количестве входов, равном n, блок LUT хранит в себе 2^n бит информации и способен выполнить вычисление значения одной n-аргументной булевой функции.

Предлагаем рассматривать LUT-контейнер как четверку вида:

$$LC = \left(L, E, Interface, Extern\right), \tag{1}$$

где

L — множество блоков LUT;

E — множество связей между элементами множества L;

Interface — множество входов и выходов контейнера;

Extern — множество связей блоков LUT с входами и выходами контейнера.

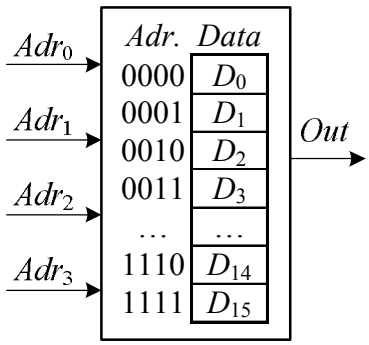


Рис. 1. Организация 4-х входового блока LUT микросхемы FPGA

Каждый элемент LUT_i множества L представляет собой следующую тройку:

$$LUT_i = \left(In_i, Out_i, Mem_i\right), \tag{2}$$

где

In_i — множество входов блока LUT_i;

Out_i — множество выходов блока LUT_i;

Mem_i — содержимое памяти блока LUT_i (внутреннее значение блока).

Таким образом, LUT-контейнер фактически представляет собой логическую схему, элементами которой являются настраиваемые блоки LUT. Следует отметить следующие особенности LUT-контейнеров, отличающие их от мультимедийных контейнеров, используемых в традиционных стеганографических методах.

1) LUT-контейнер является активным информационным объектом, выполняющим некоторую вычислительную или управляющую функцию.

2) Элементарные единицы контейнера (блоки LUT) в общем случае явно связанны друг с другом т.к. могут вычислять часть общей булевой функции. Таким образом, элементарные единицы контейнера не являются автономными, а оказывают взаимное влияние на функционирование друг друга.

3) Информация, находящаяся в каждой из элементарных единиц контейнера представляется точно. Произвольное изменение содержимого блока LUT приводит к разрушению контейнера, которое выражается в невозможности выполнения им целевой функции.

Далее предлагается метод внедрения ЦВЗ в LUT-контейнер. Метод основан на указанных особенностях контейнера, позволяющих выполнить его эквивалентное преобразование, сопряженное с внедрением секретных данных.

Основные положения предлагаемого метода внедрения данных в LUT-контейнер

Основное содержание метода далее излагается в виде совокупности специальных положений, определяющих последовательность и условия реализации процесса скрытия данных в LUT-контейнере.

Первое положение метода: для встраивания одного разряда секретной двоичной последовательности используется один из разрядов блока LUT, задействованного в выполнении целевой функции контейнера. Номер этого разряда (адрес) или правило его определения является элементом стего-ключа.

Второе положение метода: встраивание разряда секретной последовательности основано на следующем утверждении.

Пусть задана некоторая булева функция:

$$y = f\left(y_1^{\lambda_1}, y_2^{\lambda_2} \ldots, y_m^{\lambda_m}, a_1, a_2, \ldots, a_p\right). \quad (3)$$

При этом часть аргументов данной функции являются результатом вычислений значений следующей совокупности булевых функций:

$$\begin{gathered} y_1^{\lambda_1} = f_1^{\lambda_1}\left(x_1^1, x_2^1, \ldots, x_{n_1}^1\right) \\ y_2^{\lambda_2} = f_2^{\lambda_2}\left(x_1^2, x_2^2, \ldots, x_{n_2}^2\right) \\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots \\ y_m^{\lambda_m} = f_m^{\lambda_m}\left(x_1^m, x_2^m, \ldots, x_{n_m}^m\right) \end{gathered} \quad (4)$$

и для функций (3) и (4) установлена следующая система правил:

$$\begin{gathered} y_i^{\lambda_i} = \begin{cases} y_i, \text{ при } \lambda_i = 1; \\ \overline{y_i}, \text{ при } \lambda_i = 0; \end{cases} \\ f_i^{\lambda_i}\left(x_1^i, x_2^i, \ldots, x_{n_i}^i\right) = \begin{cases} f_i^{\lambda_i}\left(x_1^i, x_2^i, \ldots, x_{n_i}^i\right), \text{ при } \lambda_i = 1; \\ \overline{f_i^{\lambda_i}}\left(x_1^i, x_2^i, \ldots, x_{n_i}^i\right), \text{ при } \lambda_i = 0. \end{cases} \end{gathered} \quad (5)$$

где $\lambda_i \in \{0, 1\}$, $i = 1 \ldots m$.

В выражении (3) допускается отсутствие аргументов $a_1, a_2, \ldots, a_p$.

Утверждение 1. Значения булевой функции (3) при аргументах (4) и правилах (5) на любых двоичных наборах не зависят от значений переменных $\lambda_1, \lambda_2, \ldots, \lambda_m$.

Действительно, при инвертировании любой из функций $f_i^{\lambda_i}$ (4) и сопровождающейся повторным инвертированием (5) подстановке ее значения в функцию (3), в действительности в функцию (3) в соответствии с законом двойного отрицания будет подставлено прямое значение $f_i^{\lambda_i}$, которое имело место до инвертирования. Таким образом, инвертирование любых функций из (4) с учетом (5) не приводит к изменению значений функции (3).

Из данного утверждения следует, что любые комбинации значений переменных $\lambda_1, \lambda_2, \ldots, \lambda_m$ в системе выражений (3) – (5) порождают равносильные булевы функции (3), дающие одинаковые значения на любых наборах.

Принцип встраивания разряда секретной последовательности связан с приведенным *утверждением* следующим образом. Пусть функцию (3) реализует некоторый блок *LUT'*, а функции (4) некоторый набор блоков LUT_1, LUT_2, …, LUT_m. Тогда выборочным инвертированием значений LUT_1, LUT_2, …, LUT_m можно добиться наличия в каждом из них, таких значений определенных разрядов, которые соответствуют разрядам внедряемой в контейнер секретной двоичной последовательности. При этом значения, вычисляемые блоком *LUT'* с учетом выражений (5) не претерпят каких-либо изменений.

Третье положение метода определяет ограничения на структуру схемы LUT-контейнера, в который внедряется секретная информация. Предлагаемый метод может быть применен только к схеме, имеющей более одного уровня блоков LUT (ранг которой $r > 1$). Действительно, минимальный вариант схемы, совместно реализующей выражения (3) – (5) должен включать набор блоков LUT, расположенных на первом

уровне и предназначенных для вычисления функций (4), а также один или несколько блоков LUT, расположенных на втором уровне и предназначенных для вычисления функции (3).

Четвертое положение метода определяет ограничения на использование блоков LUT, входящих в контейнер, для задачи встраивания секретной последовательности.

Первое ограничение такого рода состоит в том, что для встраивания нельзя использовать блоки LUT, непосредственно подключенные к выходам схемы. Это ограничение обусловлено тем, что встраивание секретной информации выполняется в блоки LUT, реализующие выражения (4), к выходам которых, должны быть подключены блоки LUT следующего уровня, реализующие выражение (3). Если же блок LUT подключен к выходу схемы, то следующие за ним блоки, реализующие выражение (3) отсутствуют.

Второе ограничение состоит в том, что блок LUT, в который уже встроен разряд секретной последовательности, не может быть подвергнут инвертированию при выполнении встраивания данных в другой блок LUT данного контейнера. Из этого ограничения следует, что количество блоков LUT, которые можно задействовать для внедрения разрядов секретной последовательности зависит от порядка обхода контейнера.

Таким образом, первое указанное ограничение задает верхнюю оценку количества блоков LUT, которые можно задействовать для внедрения секретной информации, а второе ограничение – нижнюю оценку. Указанные верхнее и нижнее значения зависят от общего количества блоков, конфигурации их соединения и порядка обхода контейнера в процессе встраивания в него секретной последовательности.

Пятое положение метода определяет порядок формирования стего-ключа для встраивания и извлечения секретной последовательности. Ключ определяется как двойка следующего вида:

$$key = (set, order) \tag{6}$$

где

set – номер (адрес) разряда LUT, в который выполняется внедрение бита секретной последовательности. Вместо фиксированного значения *set*, этот компонент ключа может содержать некоторое правило, позволяющее получить номер разряда встраивания для каждого шага встраивания;

order – порядок обхода блоков LUT в контейнере для выполнения встраивания или извлечения секретной последовательности. Вместо фиксированного порядка обхода блоков LUT этот компонент ключа может содержать правило, задающее порядок обхода на каждом шаге встраивания.

Пример реализации предлагаемого метода

Рассмотрим пример, иллюстрирующий основные положения предлагаемого метода. На рис. 2 (а) представлена схема контейнера, состоящая из пяти блоков LUT и реализующая две логические функции y' и y''. Двоичный вес каждого из входов блоков LUT, обозначен рядом с соответствующим входом. Необходимо внедрить в данную схему, секретную последовательность $M = (1,0,0)$ используя для этого значения, расположенные в блоках LUT по адресу 3. Порядок обхода блоков схемы в ходе встраивания определен их нумераций.

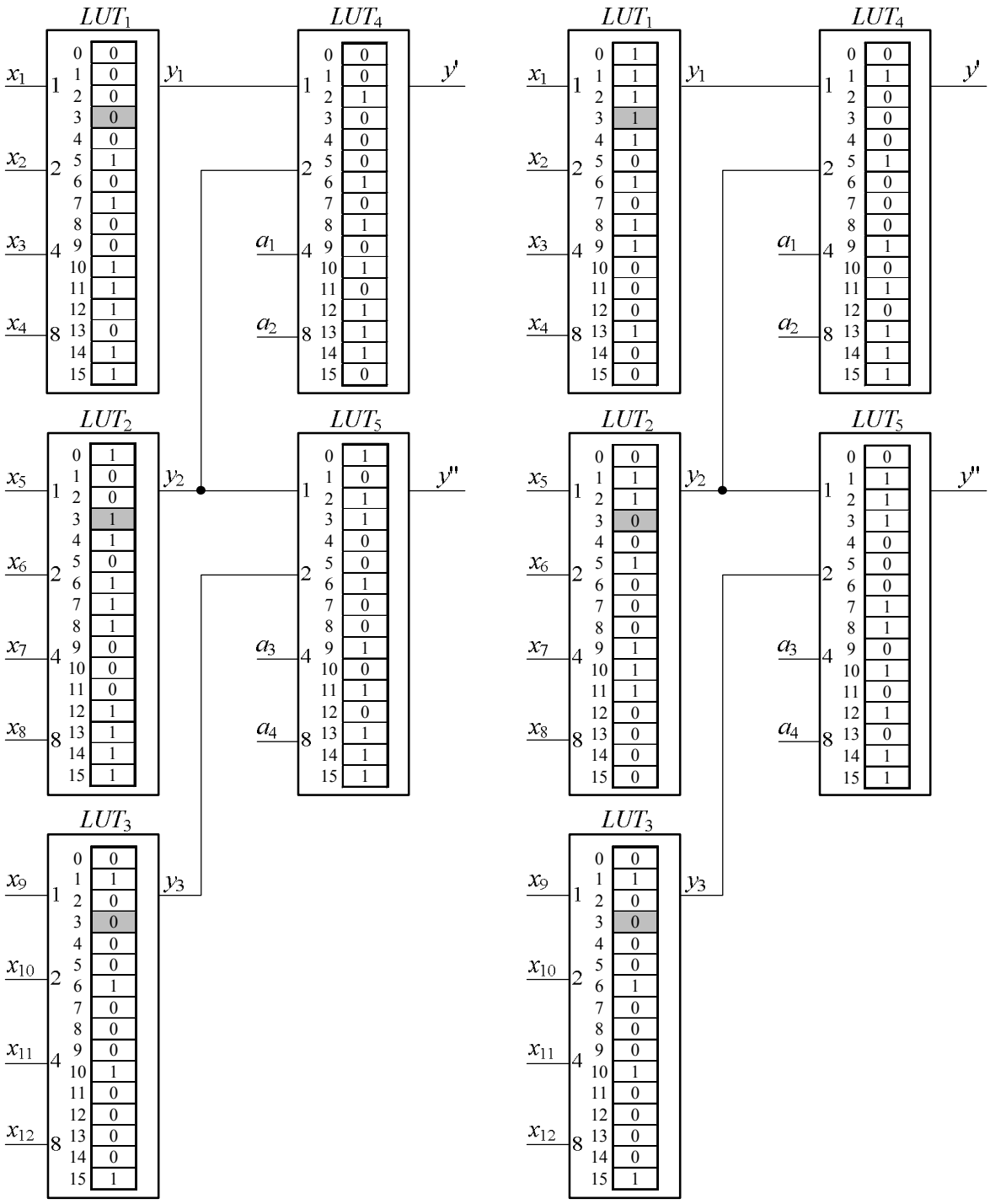


Рис. 2. Пример встраивания секретной двоичной последовательности $M = (1,0,0)$ в LUT-ориентированный контейнер, состоящий из 5-и блоков LUT: а – исходные значения контейнера; б – значения после встраивания

Структура данной схемы соответствует выражениям (3) и (4) для которых может быть применена система правил (5) 2-го положения метода. В соответствии с 3-м положением метода схема, показанная на рис. 2(а) может быть использована в качестве контейнера для встраивания секретной информации, т.к. она имеет два уровня. В

соответствии с 4-м положением для встраивания могут быть задействованы блоки LUT не подключенные к выходам схемы, т.е. блоки LUT_1, LUT_2, LUT_3.

Для внедрения разрядов последовательности будем в порядке нумерации использовать блоки LUT первого уровня. В блоке LUT_1 по адресу 3 хранится значение «0». По этому адресу необходимо поместить значение «1». В соответствии со 2-м положением метода выполним инвертирование всех значений, хранящихся в блоке LUT_1. После этого, в соответствии с правилами (5), выполним инвертирование значения на входе блока LUT, принимающего данные от блока LUT_1, т.е. блока LUT_4. В результате выполнения этих действий, функции, вычисляемые схемой, останутся неизменными, однако в блок LUT_1 по адресу 3 будет внедрен первый разряд секретной последовательности, равный значению «1» (рис. 2(б)).

Аналогичным образом, используя 1-е и 2-е положение предложенного метода, заменяем значение «1», хранящееся в блоке LUT_2 по адресу 3 на второй разряд секретной последовательности «0». Для этого инвертируем все значения, хранящиеся в блоке LUT_2 с одновременным инвертированием значений на входах блоков LUT, принимающих данные от блока LUT_2, т.е. блоков LUT_4 и LUT_5. Для внедрения третьего разряда секретной последовательности «0» в блок LUT_3 нет необходимости выполнять какие-либо изменения значений блоков LUT данной схемы, т.к. в блоке LUT_3 по адресу 3 уже хранится значение 0.

Рассмотренный пример показывает возможность внедрения секретной последовательности в LUT-контейнер в соответствии с предложенным методом. В результате такого внедрения функционирование контейнера не изменяется (схемы, изображенные на рис. 2(а) и рис. 2(б) формируют одинаковые значения на одинаковых входных наборах), т.е. его целевая функция остается неизменной. Однако контейнер становится носителем информации, которую можно использовать в качестве элемента ЦВЗ или для организации стего-защищенных систем передачи и хранения данных.

Алгоритм внедрения данных в контейнер в соответствии с предложенным методом

Основные положения предложенного метода встраивания данных в LUT-контейнер обуславливают рассмотренный далее алгоритм реализации этого метода.

Исходные данные алгоритма:

1) секретная двоичная последовательность $M = (m_1, m_2, \ldots, m_k)$;

2) LUT-контейнер LC, реализующий некоторую вычислительную или управляющую функцию. На множестве блоков LUT в контейнере LC установлено отношение порядка (нумерация, система координат) дающее возможность выполнить обход блоков контейнере в заданном порядке в ходе встраивания разрядов секретной последовательности;

3) ключ *key* для встраивания и извлечения секретной информации.

Результат применения алгоритма – LUT-контейнер LC^*, в который внедрена последовательность *M*. Функционирование контейнера LC^*, выражающееся в выполнении его целевой функции, не отличается от функционирования контейнера *LC*.

Последовательность действий по внедрению данных в LUT-ориентированный контейнер:

1) Определение возможности встраивание последовательности *M* в контейнер *LC* на основании 3-го положения предлагаемого метода. Если схема, содержащаяся в контейнере, имеет более одного уровня, то встраивание возможно.

2) Оценка возможности встраивания последовательности *M* целиком в контейнер *LC*, исходя из количества боков LUT, которые можно использовать для встраивания.

Оценка доли последовательности *M*, которую можно встроить в контейнере, в случае невозможности встроить последовательность целиком.

3) Формирование списков блоков LUT, предназначенных для проверки соблюдения ограничений 4-го положения метода:

- формирование списка *ExternalList*, в который заносятся идентификаторы блоков LUT, непосредственно подключенные к выходам схемы (4-е положение метода, 1-е ограничение);
- формирование списка *BlockList*, в который в ходе движения по контейнеру помещаются идентификаторы заблокированных для встраивания блоков LUT (4-е положение метода, 1-е ограничение).

4) В соответствии с заданным порядком обхода блоков LUT контейнера, с учетом ограничений, определенных 4-м положением метода, каждый разряд секретной последовательности m_j на основании следующего правила встраивается в индивидуальный блок LUT_i:

$$\forall LUT_i \mid \left(LUT_i \notin ExternalList \;\&\; LUT_i \notin BlockList \;\&\; OutList\left(LUT_i\right) \cap BlockList = \varnothing\right)$$
$$\text{if } LUT_i(set) \neq m_j \text{ then } Embed\left(LUT_i, m_j\right); \qquad (7)$$
$$LUT_i \rightarrow BlockList,$$

где

$OutList\left(LUT_i\right)$ — список блоков LUT, подключенных своими входами к выходу блока LUT_i;

set — номер (адрес) разряда LUT, в который выполняется внедрение секретного бита m_j;

Embed — процедура встревания разряда m_j в блок LUT_i по адресу *set*;

«$\rightarrow$» — операция включения идентификатора блока LUT в список.

Внешнее условие правила (7) определяет возможность использования блока для встраивания очередного разряда секретной последовательности (4-е положение метода). Данное сложное условие определяет то, что блок LUT_i, предназначенный для встраивания информации:

- не должен содержаться в списке блоков, непосредственно подключенных к выходам схемы;
- не должен содержаться в списке *BlockList* заблокированных для встраивания блоков;
- его выход не должен быть подключен на вход блоков из списка *BlockList*.

Таким образом, данное сложное условие проверяет отсутствие обоих ограничений, наложенных 4-м положением метода.

Внутреннее условие правила (7) означает, что *Embed* – процедура встревания разряда m_j в блок LUT_i по адресу *set*, выполняется только тогда, когда значение, содержащееся в данном блоке по указанному адресу, не совпадает со значением разряда, который необходимо встроить. В противном случае отсутствует необходимость выполнения встраивания в данный блок LUT_i.

Блоки LUT, не удовлетворяющие внешнему или внутреннему условию правила (7), игнорируются в процессе обхода контейнера. Встраивание информации в них не производится. Блоки LUT, удовлетворяющие внешнему условию, но не удовлетворяющие внутреннему условию правила (7) хранят элементы секретной последовательности, но встраивание в них не производится по причине совпадения исходного их значения со значением, подлежащим встраиванию. В ходе применения правила (7), независимо от того, каким образом в очередной блок LUT был помещен разряд секретной последовательности (при помощи процедуры *Embed* или этот разряд

находился в контейнере изначально, и применение процедуры *Embed* не требовалось), идентификатор данного блока LUT заносится в список заблокированных блоков *BlockList*.

Процедура встраивания Embed.

Процедура *Embed*, выполняющая встраивание разряда m_j в блок LUT_i по адресу *set* состоит из двух действий:

1) инвертирование значений блока LUT_i (каждое из значений, хранящихся в блоке меняется на противоположное);

2) выполнение *процедуры распространение инверсии* на входы всех блоков LUT, содержащихся в списке $OutList(LUT_i)$. Распространение инверсии состоит в инвертировании входа блока LUT. Такое инвертирование сводится к перестановке значений, хранящихся в блоке LUT, и определяется следующим образом.

Введем обозначения. Пусть блок LUT_i имеет набор из n входов $In_i = \left(in_i^{n-1}, in_i^{n-2}, \ldots, in_i^1, in_i^0\right)$. Каждый из входов in_i^k при $k = \overline{0, n-1}$ задает один из разрядов адреса блока LUT, и соответственно имеет вес 2^k. Количество значений, хранящихся в данном блоке LUT равно $N = 2^n$. Обращение (на чтение или на запись) к значению, хранящееся в блоке LUT_i по адресу s определим как $LUT_i(s)$, где s может задаваться в виде двоичного числа, количество разрядов которого, совпадает с количеством входов блока LUT или в виде десятичного эквивалента этого числа.

Следующим образом определим процедуру перестановки значений блока LUT:

$$Permutation(LUT_i, w):\ \forall s\ \ LUT_i\left(s_w^0\right) \leftrightarrow LUT_i\left(s_w^1\right), \tag{8}$$

где

s — любой допустимый адрес для данного блока LUT_i;

s_w^0 и s_w^1 — двоичные наборы, которые различаются только значением в разряде, имеющем вес w, а в остальных разрядах совпадают. Наборы s_w^0 и s_w^1 содержат в разряде с весом w ноль и единицу соответственно;

«$\leftrightarrow$» — операция обмена значений блока LUT (значение, указанное в качестве левого операнда, помещается на место правого операнда и наоборот).

Таким образом, принцип перестановки в ходе распространения инверсии зависит от двоичного веса входа, на который распространяется инверсия. Например, для распространения инверсии на вход блока LUT, имеющий минимальный вес $w = 1$, в соответствии с выражением (8), выполняется взаимный обмен значений, расположенных по адресам, отличающимся только в младшем разряде (с весом 1). Это приводит к обмену значениями, находящимися по ближайшим четным и нечетным адресам: $LUT(0) \leftrightarrow LUT(1)$; $LUT(2) \leftrightarrow LUT(3)$; $LUT(4) \leftrightarrow LUT(5)$ и т.д. Аналогичным образом, распространение инверсии на вход блока LUT, имеющий вес $w = 2$ приводит к взаимному обмену значениями, расположенными по адресам, отличающимся в разряде с весом 2: $LUT(0) \leftrightarrow LUT(2)$; $LUT(1) \leftrightarrow LUT(3)$; $LUT(4) \leftrightarrow LUT(6)$; $LUT(5) \leftrightarrow LUT(7)$ и т.д.

На рис. 3 показаны правила распространения инверсии для 4-х входового блока LUT. Столбцы *A*, *B*, *C*, *D* содержат разряды адреса, подаваемые на соответствующие входы. Веса входов увеличиваются слева направо: *A* – вес 1, *B* – вес 2, *C* – вес 4, *D* – вес 8. В столбце *out* находятся значения, содержащиеся в блоке LUT. На рис. 3 (а) показаны первоначальные значения блока LUT, на рис. 3(б–д) показаны результаты распространения инверсии на входы этого блока *D*, *C*, *B*, *A* соответственно.

Блоки LUT, используемые в современных средствах цифровой техники имеют небольшое количество входов (от 3 до 6). В силу этого нет необходимости выполнять поиск наборов, на которых значения LUT в соответствии с выражением (8) подлежат

обмену. Правила обмена для таких блоков LUT могут быть жестко определены в реализации алгоритма распространения инверсии.

D^8	C^4	B^2	A^1	out
0	0	0	0	h_0
0	0	0	1	h_1
0	0	1	0	h_2
0	0	1	1	h_3
0	1	0	0	h_4
0	1	0	1	h_5
0	1	1	0	h_6
0	1	1	1	h_7
1	0	0	0	h_8
1	0	0	1	h_9
1	0	1	0	h_{10}
1	0	1	1	h_{11}
1	1	0	0	h_{12}
1	1	0	1	h_{13}
1	1	1	0	h_{14}
1	1	1	1	h_{15}

а

D^8	C^4	B^2	A^1	out
0	0	0	0	h_8
0	0	0	1	h_9
0	0	1	0	h_{10}
0	0	1	1	h_{11}
0	1	0	0	h_{12}
0	1	0	1	h_{13}
0	1	1	0	h_{14}
0	1	1	1	h_{15}
1	0	0	0	h_0
1	0	0	1	h_1
1	0	1	0	h_2
1	0	1	1	h_3
1	1	0	0	h_4
1	1	0	1	h_5
1	1	1	0	h_6
1	1	1	1	h_7

б

D^8	C^4	B^2	A^1	out
0	0	0	0	h_4
0	0	0	1	h_5
0	0	1	0	h_6
0	0	1	1	h_7
0	1	0	0	h_0
0	1	0	1	h_1
0	1	1	0	h_2
0	1	1	1	h_3
1	0	0	0	h_{12}
1	0	0	1	h_{13}
1	0	1	0	h_{14}
1	0	1	1	h_{15}
1	1	0	0	h_8
1	1	0	1	h_9
1	1	1	0	h_{10}
1	1	1	1	h_{11}

в

D^8	C^4	B^2	A^1	out
0	0	0	0	h_2
0	0	0	1	h_3
0	0	1	0	h_0
0	0	1	1	h_1
0	1	0	0	h_6
0	1	0	1	h_7
0	1	1	0	h_4
0	1	1	1	h_5
1	0	0	0	h_{10}
1	0	0	1	h_{11}
1	0	1	0	h_8
1	0	1	1	h_9
1	1	0	0	h_{14}
1	1	0	1	h_{15}
1	1	1	0	h_{12}
1	1	1	1	h_{13}

г

D^8	C^4	B^2	A^1	out
0	0	0	0	h_1
0	0	0	1	h_0
0	0	1	0	h_3
0	0	1	1	h_2
0	1	0	0	h_5
0	1	0	1	h_4
0	1	1	0	h_7
0	1	1	1	h_6
1	0	0	0	h_9
1	0	0	1	h_8
1	0	1	0	h_{11}
1	0	1	1	h_{10}
1	1	0	0	h_{13}
1	1	0	1	h_{12}
1	1	1	0	h_{15}
1	1	1	1	h_{14}

д

Рис. 3. Правила распространения инверсии на входы 4-х входового блока LUT: а – исходные значения; б – распространение инверсии на вход D; в – распространение инверсии на вход C; г – распространение инверсии на вход B; д – распространение инверсии на вход A

В общем случае процедура распространения инверсии может иметь место не по одному входу блока LUT, а по нескольким его входам (групповое распространение инверсии). Выполнение такого группового распространения инверсии основано на следующем утверждении.

Утверждение 2. Результат группового распространения инверсии на входы блока LUT не зависит от порядка выполнения процедуры распространения инверсии на отдельные его входы.

Доказательство этого утверждения состоит в следующем. Распространение инверсии основано на перестановке, по правилу (8), значений, хранящихся в блоке LUT. Каждая такая перестановка приводит к взаимному изменению только одного разряда адреса для переставляемых значений. Разряды адреса в ходе выполнения перестановок не зависят друг от друга. В силу этого порядок изменения разрядов по выражению (8) при нескольких последовательных изменениях с разными значениями w не влияет на результат данных изменений. Следовательно, и порядок выполнения распространения инверсии на отдельные входы блока LUT не влияет на получаемый результат.

На рис. 4 графически показаны перестановки значений в ходе распространения инверсии на отдельные входы 4-х входового блока LUT.

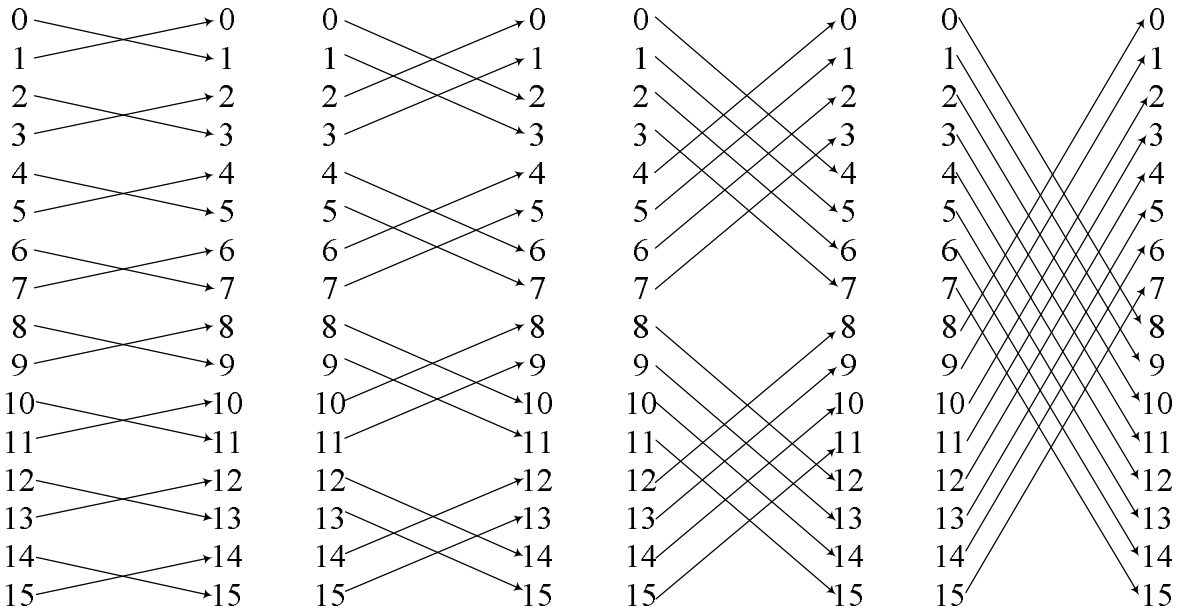


Рис. 4. Графическая интерпретация перестановок, возникающих в ходе распространения инверсии на входы 4-х входового блока LUT: а – распространение на вход с весом 1; б – распространение на вход с весом 2; в – распространение на вход с весом 4; г – распространение на вход с весом 8

Таким образом, на основании утверждения 2, в случае если процедура распространения инверсии осуществляется от нескольких блоков LUT на разные входы одного блока LUT, то необходимо по отдельности выполнить распространение инверсии на каждый вход, причем порядок обработки входов не имеет значения.

Обобщенная блок-схема алгоритма реализации предложенного метода встраивания секретной двоичной последовательности в LUT-контейнер приведена на рис. 5.

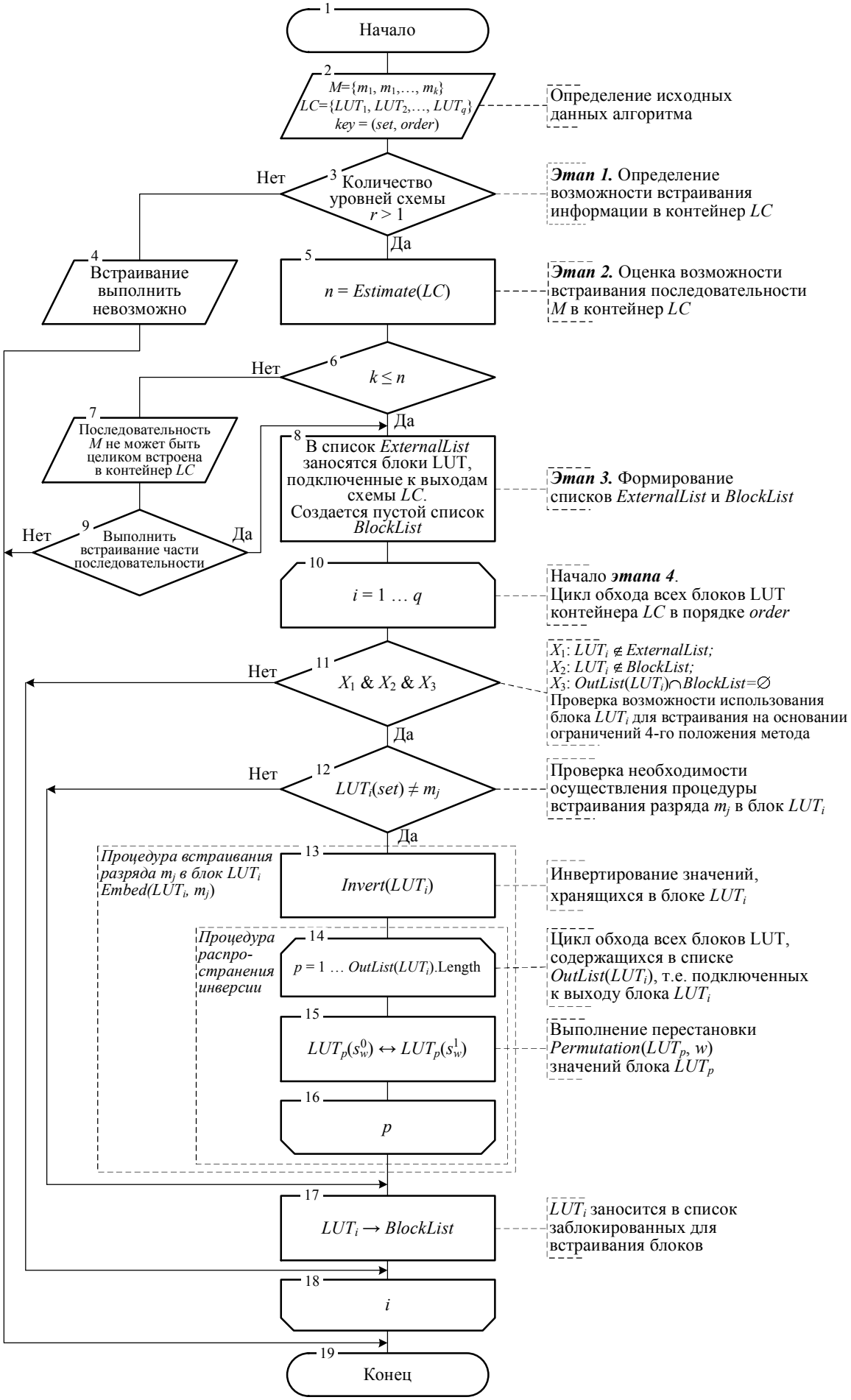


Рис. 5. Блок-схема алгоритма реализации предложенного метода встраивания

Алгоритм извлечения данных из контейнера в соответствии с предложенным методом

Далее рассматривается алгоритм извлечения из LUT-контейнера секретных данных, встроенных в соответствии с предлагаемым методом.

Исходные данные алгоритма:

1) LUT-контейнер LC^*, содержащий встроенную в него секретную двоичную последовательностью $M = (m_1, m_2, \ldots, m_k)$;

2) Ключ $key = (set, order)$ для извлечения встроенной информации.

Результат применения алгоритма – извлеченная из контейнера двоичная последовательность $M^* = (m_1^*, m_2^*, \ldots, m_k^*)$, которая при успешном извлечении должна совпадать с последовательностью $M = (m_1, m_2, \ldots, m_k)$.

Последовательность действий, необходимая для извлечения встроенных данных представлена на рис. 6 в виде блок-схемы. Несмотря на то, что информация о порядке обхода контейнера является составной частью стего-ключа, не все блоки LUT, лежащие на стего-пути, могли быть использованы для внедрения двоичной последовательности на этапе встраивания (ограничения 4-го положения метода). В силу чего (аналогично тому, как это было реализовано в алгоритме встраивания) при излечении необходимо использовать два служебных списка *ExternalList* и *BlockList*. Анализ этих списков позволяет определить мог ли блок LUT, лежащий на стего-пути, быть использован для внедрения бита секретной последовательности на этапе встраивания. Из блоков LUT, в отношении которых принято решение о том, что они могли быть использованы при встраивании, производится считывание значений по адресу *set*, являющемуся элементом стего-ключа. Считанные таким образом значения образуют извлеченную последовательность *M**.

Экспериментальное исследование предлагаемого метода

Для экспериментального исследования предлагаемого метода были разработаны аппаратно-программные средства, основанные на использовании микросхем FPGA Altera Cyclone II и САПР Altera Quartus II. На языке TCL была организована группа скриптов, выполняющих взаимодействие с САПР Altera Quartus II для считывания и записи содержимого блоков LUT. Непосредственно подсистема обработки считанных данных, в соответствии с предложенным методом, была реализована на языке C# в рамках платформы .Net.

Материалом для экспериментов выступили 25 FPGA-проектов разного объема и назначения. Эксперименты состояли во внедрении случайных секретных последовательностей в LUT-контейнеры FPGA-проектов; исследовании влияния такого внедрения на скоростные характеристики проекта, характеристики энергопотребления и тепловыделения; извлечении секретных последовательностей из заполненных контейнеров. Характеристики проекта измерялись средствами САПР Altera Quartus II Timing Analyzer и Power Play.

Экспериментальное исследование показало незначительное влияние применения метода на скоростные характеристики реализованных FPGA-проектов (изменение в среднем на 0.1%), характеристики энергопотребления и тепловыделения (изменение в среднем на 0.25%). Таким образом, установленные изменения указанных характеристик находится на уровне погрешности средств измерения и не могут считаться существенными.

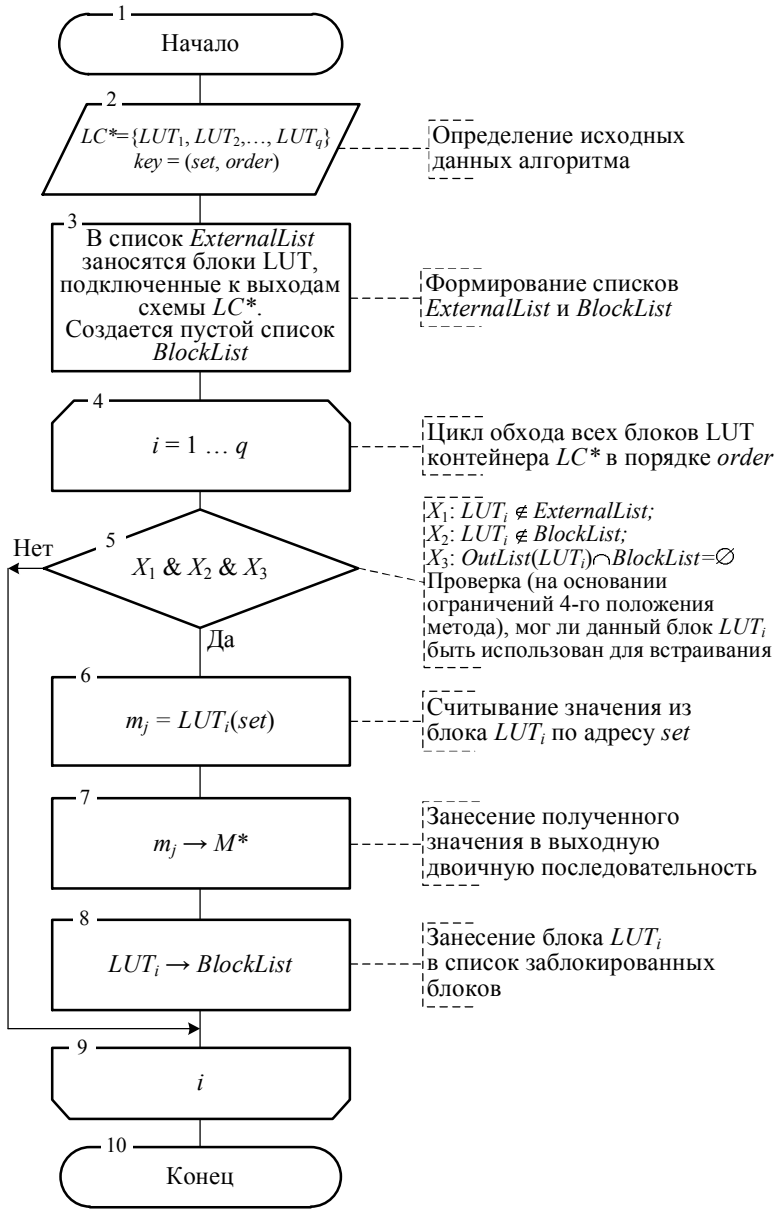


Рис. 6. Блок-схема алгоритма извлечения данных из LUT-контейнера

Преимущества и области использования предлагаемого метода

В отличие от традиционных мультимедийных стего-конвейеров, контейнеры, используемые в рамках предлагаемого метода являются активными, имеют влияющие друг на друга элементарные единицы, которые хранят в себе данные, представленные точно. Взаимное влияние элементарных единиц контейнера друг на друга дает возможность производить локальные изменения их содержимого, не меняя при этом глобальной функциональности контейнера. Точное представление данных порождает подходы к противодействию активным стего-атакам типа «стирание секретной информации», недоступные для традиционных мультимедийных контейнеров.

Природа данных, находящихся в элементарных единицах LUT-контейнеров не дает существенной статистической связи, как между разрядами отдельных единиц, так и между разрядами соседних единиц контейнера. Это не позволяет произвести

пассивную статистическую стего-атаку на такой контейнер методами стего-анализа, применяемыми для традиционных контейнеров.

Предложенный в данной работе метод может быть использован для внедрения ЦВЗ в компьютерные и управляющие устройства, построенные на основе элементной базы FPGA и ПЛИС со схожими архитектурами. Такое внедрение дает возможность контролировать правомерность использования проектной информации и самих устройств на различных этапах технологии проектирования и жизненного цикла (синтезированный FPGA проект, конфигурационный файл FPGA**,** действующее устройство).

Предложенный подход может найти применение при организации стего-защищенных систем передачи и хранения данных на основе LUT-контейнеров. Физически в качестве таких контейнеров могу выступать:

- файлы проектов в САПР FPGA устройств;
- конфигурационные файлы FPGA;
- действующие микросхемы FPGA в составе функционирующих устройств.

Кроме того, предложения данной работы могут быть использованы при организации стего-систем на основе LUT-контейнеров иной природы (не связанных с архитектурой микросхем FPGA). Однако выявление и исследование таких контейнеров требует дополнительных исследований.

Выводы

В работе предложен метод внедрения ЦВЗ в аппаратные контейнеры с LUT-ориентированной архитектурой. Метод позволяет внедрять двоичную информацию в LUT-контейнер, подвергая элементарные единицы контейнера локальным изменениям, не меняя при этом глобальную функциональность контейнера. Показаны алгоритмы реализации предложенного метода в части встраивания и извлечения секретной двоичной последовательности, которая представляет собой ЦВЗ. Метод предлагается использовать для внедрения секретных данных в LUT-контейнеры (на примере микросхем FPGA) с целью организации в их пространстве ЦВЗ, которые дают возможность контроля использования контейнера на всех этапах его жизненного цикла.

Список литературы

1. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
2. Cox, I.J. Digital Watermarking and Steganography / I.J. Cox, *et al.* — 2nd edition. — Burlington: Morgan Kaufmann Publishers, 2008. — 624 p.
3. Fridrich, J. Steganography in Digital Media: Principles, Algorithms, and Applications / J. Fridrich. — New York: Cambridge University Press, 2010. — 462 p.
4. Shih, F.Y. Multimedia Security: Watermarking, Steganography, and Forensics / F.Y. Shih. — New York: CRC Press, 2012. — 424 p.
5. Skoudis, E. Malware: Fighting Malicious Code / E. Skoudis, L. Zeltser. — New Jersey: Prentice Hall, 2004. — 672 p.
6. El-Khalil, R. Hydan: Hiding Information in Program Binaries / R. El-Khalil, A.D. Keromytis // Proceedings of International Conference on Information and Communications Security (ICICS'2004), 27–29 October, Malaga, Spain. — PP. 187–199.
7. Hamilton, A. Survey of Static Software Watermarking / A. Hamilton, S. Danicic // Proceedings of World Congress on Internet Security (WorldCIS-2011), 21–23 February, London, UK. — PP. 100–107.
8. Hakun, L. New Approaches for Software Watermarking by Register Allocation / L. Hakun, K. Kaneko // Proceedings of the Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel Distributed Computing, 6–8 August 2008, Phuket, Thailand. — PP. 63–68.

9. XiaoCheng, L. Software Watermarking Algorithm Based on Register Allocation / L. XiaoCheng, C. Zhiming // Proceedings of the 2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES), 10–12 August, Hong Kong. — PP. 539–543.
10. Максфилд, К. Проектирование на ПЛИС: Архитектура, средства и методы. Курс молодого бойца [Текст] / К. Максфилд ; Пер. с англ. — М. : «Додэка-XXI», 2007. — 408 с.
11. Paul, S. Reconfigurable Computing Using Content Addressable Memory for Improved Performance and Resource Usage / S. Paul, S. Bhunia // Proceedings of the 45th annual Design Automation Conference ACM/IEEE (DAC-2008), 8–13 June 2008, Anaheim, USA. — PP. 786–791.
12. Грушвицкий, Р.И. Проектирование систем на микросхемах с программируемой структурой / Р.И. Грушвицкий, А.Х. Мурсаев, Е.П. Угрюмов. — 2-е изд., перераб. и доп. — СПб. : БХВ-Петербург, 2006. — 736 с.

МЕТОД ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ В АПАРАТНІ КОНТЕЙНЕРИ З LUT-ОРІЄНТОВАНОЮ АРХІТЕКТУРОЮ

К.В. Защолкін, О.М. Іванова

Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: const-z@te.net.ua

Розглянуто задачу вбудовування цифрових водяних знаків в інформаційний об'єкт з метою контролю його використання. Відзначені типові підходи до організації такого вбудовування. Запропоновано метод вбудовування цифрових водяних знаків в апаратні контейнери з LUT-орієнтованою архітектурою. Показані алгоритми реалізації запропонованого методу. Описана апаратно-програмна реалізація методу і результати експериментів в середовищі цієї реалізації. Показано можливості застосування запропонованого методу для організації цифрових водяних знаків у просторі LUT-орієнтованого контейнера з метою контролю його використання в динаміці проектування та життєвого циклу.
Ключові слова: цифрові водяні знаки, стеганографія, захист інформації, апаратний стего-контейнер, LUT-орієнтована архітектура, FPGA, контроль використання FPGA-проектів

METHOD OF EMBEDDING OF DIGITAL WATERMARKS IN HARDWARE CONTAINERS WITH LUT-ORIENTED ARCHITECTURE

Kostyantyn V. Zashcholkin, Olena M. Ivanova

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: const-z@te.net.ua

A problem of embedding digital watermarks in information object to control the use of the latter was considered. Typical approaches to organizing such an embedding were noted. A technique to embed digital watermarks in hardware cover objects of LUT architecture was proposed. The algorithms to implement the technique proposed were demonstrated. Hardware-and-software implementation of the technique and the results of experiments within this implementation were described. The possibility of implementing the technique proposed for organization of digital watermarks in the domain of a cover object of LUT architecture to control its use within the project and life cycles was shown.
Keywords: digital watermarks, steganography, information security, hardware stego container, LUT-oriented architecture, FPGA, control of use FPGA-projects

Алфавітний покажчик авторів
Том 3, 2013

Author Index
Volume 3, 2013

Березовська, Ю.В.	43	Berezovska, J.	43
Березовський, А.А.	190	Berezovsky, A.	190
Бобок, І.І., *к.т.н.*	323	Bobok, I., *PhD*	323
Браун, В.О., *к.т.н.*	43	Brown, V., *PhD*	43
Бурячок, В.Л., *д.т.н.*	123	Buryachok, V., *EngD*	123
Вайсфельд, Н.Д., *д.ф.-м.н.*	35	Chirkov, D., *PhD*	113
Вичужанін, В.В., *д.т.н.*	240	Danilenko, E., *EngD*	132
Вігура, А.М.	200	Dubchak, L., *PhD*	91
Гахович, С.В., *к.т.н.*	156	Dudnik, A.	233
Гребень, Н.Є.	266	Fedorova, N., *PhD*	283
Губернаторов, В.П.	331	Gakhovich, S., *PhD*	156
Даніленко, Є.Л., *д.т.н.*	132	Greben, N.	266
Дубчак, Л.О., *к.т.н.*	91	Gubernatorov, V.P.	331
Дудник, А.О.	233	Ivanova, O.	369
Журавель, В.В.	225	Karpinsky, M., *EngD*	314
Іванова, О.М.	369	Kasyanchuk, M., *PhD*	266
Замаруєва, І.В., *д.т.н.*	75	Khokhlachova, Y.	69
Защолкін, К.В., к.т.н.	369	Khoroshko, V., *EngD*	69
Зоріло, В.В., *к.т.н.*	5	Kobozeva, A., *EngD*	5; 169
Зубарєв, В.В., *д.т.н.*	215	Krchenko, O., *EngD*	314
Карпінський, М.П., *д.т.н.*	314	Kostyrka, O.	275; 353
Касянчук, М.М., *к.ф.-м.н.*	266	Kozina, M.	169
Кобозєва, А.А., *д.т.н.*	5; 169	Kozlovsky, V., *PhD*	61
Козіна, М.О.	169	Lebedyeva, O.	5
Козловський, В.В., *к.т.н.*	61	Lenkov, S., *EngD*	43; 215; 233
Корченко, О.Г., д.т.н.	314	Lipovsky, V.	113
Костирка, О.В.	275; 353	Lomakina, L., *EngD*	200; 331
Лебедєва, О.Ю.	5	Lysenko, R.	61
Лєнков, С.В., *д.т.н.*	43; 215; 233	Lytvynenko, L.	75
Лисенко, Р.М.	61	Mardarenko, E., *PhD in History*	288
Литвиненко, Л.О.	75	Melnik, M.	146; 248
Ліповський, В.Г.	113	Mushak, A., *PhD*	299
Ломакіна, Л.С., *д.т.н.*	200; 331	Miroshnichenko, O., *PhD*	156
Мардаренко, О.В., *к.и.н.*	288	Narimanova, O., *PhD*	163; 361
Мельник, М.О.	146; 248	Nikolaevsky, O.	75
Мірошніченко, О.В., *к.т.н.*	156	Okhramovich, M., *PhD*	156
Мушак, А.Я., *к.т.н.*	299	Muayad Omar Abdullah	190
Наріманова, О.В., *к.т.н.*	163; 361	Pavlenko, S.	103
Ніколаєвський, О.Ю.	75	Pavlov, I., *PhD*	50
Омар Муаяд Абдуллах	190	Polozhaenko, S., *EngD*	103
Охрамович, М.М., *к.т.н.*	156	Pustovit, M.	258
Павленко, С.В.	103	Rajba, S., *PhD*	314
Павлов, І.М., *к.т.н.*	50	Rudnichenko, N.	240
Положаєнко, С.А., *д.т.н.*	103	Rybalsky, O., *EngD*	225
Пустовіт, М.О.	258	Savchenko, T., *PhD*	156
Райба, С., *к.т.н.*	314	Selyukov, O., *EngD*	43; 215
Рибальський, О.В., *д.т.н.*	225	Semenchenko, D.	361
Рудніченко, Н.Д.	240	Shiyan, A., *PhD*	342
Савченко, Т.В., *к.т.н.*	156	Shtepa, V., *PhD*	233
Семенченко, Д.М.	361	Shvorov, A.	233
Сєлюков, О.В., *д.т.н.*	43; 215	Solovyev, V., *PhD*	225
Соловйов, В.І., *к.т.н.*	225	Timoshenko, L., *PhD in Economics*	266
Тимошенко, Л.М., *к.е.н.*	266	Tolubko, V., *EngD*	75
Толубко, В.Б., *д.т.н.*	75	Trifonova, E.	22; 163
Трифонова, К.О.	22; 163	Tsytsaryev, V., *PhD*	43; 215

Узун, І.А.	179	Uzun, I.	179
Федорова, Н.В., *к.т.н.*	283	Vaysfel'd, N., *Dr.sc.math.*	35
Хорошко, В.О., *д.т.н.*	69	Vichuzhanin, V., *EngD*	240
Хохлачова, Ю.Є.	69	Vigura, A.	200
Цицарєв, В.М., *к.т.н.*	43; 215	Yakymenko, I., *PhD*	82; 266
Чирков, Д.В., *к.т.н.*	113	Yaremchuk, Y., *PhD*	13; 306
Шворов, А.С.	233	Zamaruieva, I., *EngD*	75
Шиян, А.А., *к.ф.-м.н.*	342	Zashcholkin, K., *PhD*	369
Штепа, В.М., *к.т.н.*	233	Zhuravel, V.	225
Якименко, І.З., *к.т.н.*	82; 266	Zorilo, V., *PhD*	5
Яремчук, Ю.Є., *к.т.н.*	13; 306	Zubarev, V., *EngD*	215

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 3, номер 4, 2013. Одеса – 93 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 3, номер 4, 2013. Одесса – 93 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 3, No. 4, 2013. Odesa – 93 p.

Засновник: Одеський національний політехнічний університет

Зареєстровано Міністерством юстиції України 04.04.2011р.

Свідоцтво: серія КВ № 17610 - 6460Р

Друкується за рішенням Вченої ради Одеського національного політехнічного університету (протокол №1 від 30.08.2013)

Адреса редакції: Одеський національний політехнічний університет,

проспект Шевченка, 1, Одеса, 65044 Україна

Web: http://www.immm.opu.ua

E-mail: immm.ukraine@gmail.com