

УДК 004.056.53

**К. В. Защелкин**, канд. техн. наук,  
**Е. Н. Иванова**

### **ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ ВНЕДРЕНИЯ САМОВОССТАНАВЛИВАЮЩИХ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В LUT-ОРИЕНТИРОВАННЫЕ КОНТЕЙНЕРЫ**

***Аннотация.** Рассмотрены подходы к контролю использования информационных объектов при помощи технологии цифровых водяных знаков. Отмечена необходимость восстановления оригинала информационного объекта (контейнера для цифрового водяного знака) после извлечения цифрового водяного знака из него. Предложена информационная технология внедрения самовосстанавливающихся цифровых водяных знаков в контейнеры с LUT-ориентированной архитектурой. Технология основана на композиции подходов к организации самовосстанавливающихся цифровых водяных знаков в пассивных мультимедийных контейнерах и подходов к встраиванию дополнительной информации в LUT-контейнеры. Приведена информация о практической реализации предлагаемой технологии.*

***Ключевые слова:** цифровые водяные знаки, контроль использования информационных объектов, защита информации, стеганография, внедрение дополнительных данных, аппаратный стего-контейнер, LUT-ориентированная архитектура, микросхемы FPGA*

**K. V. Zashcholkin**, PhD.,  
**E. N. Ivanova**

### **INFORMATION TECHNOLOGY OF EMBEDDING SELF-RECOVERY DIGITAL WATERMARK IN LUT-ORIENTED CONTAINERS**

***Abstract.** The approaches to the control of use of information objects by means of technology of digital watermarking were reviewed. The necessity to recovery of original of information object (container for digital watermark) after extracting digital watermark from it was marked. We propose an information technology embedding self-recovery digital watermark in containers with LUT-oriented architecture. The technology is based on composition of approaches to organisation self-recovery digital watermarks in passive multimedia containers and approaches to embedding additional information in the LUT-containers. Information about the practical implementation of the proposed technology was presented.*

***Keywords:** digital watermarks, control of use of information objects, data protection, steganography, embedding of additional data, hardware stego-container, LUT-oriented architecture, FPGA chips*

**К. В. Защолкін**, канд. техн. наук,  
**О. М. Иванова**

### **ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ВБУДОВУВАННЯ САМОВІДНОВЛЮВАЛЬНИХ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ В LUT-ОРІЄНТОВАНІ КОНТЕЙНЕРИ**

***Анотація.** Розглянуто підходи до контролю використання інформаційних об'єктів за допомогою технології цифрових водяних знаків. Відзначена необхідності відновлення оригіналу інформаційного об'єкта (контейнера для цифрового водяного знака) після вилучення цифрового водяного знака з нього. Запропоновано інформаційну технологію вбудовування самовідновлювальних цифрових водяних знаків в контейнери з LUT-орієнтованою архітектурою. Технологія базується на композиції підходів до організації самовідновлювальних цифрових водяних знаків в пасивних мультимедійних контейнерах і підходів до вбудовування додаткової інформації в LUT-контейнери. Наведено інформацію про практичну реалізацію запропонованої технології.*

***Ключові слова:** цифрові водяні знаки, контроль використання інформаційних об'єктів, захист інформації, стеганографія, вбудовування додаткових даних, апаратний стего-контейнер, LUT-орієнтована архітектура, мікросхеми FPGA*

**Введение.** Технологии цифровых водяных знаков (ЦВЗ) [1] представляют собой эффективный подход к контролю использования информационных объектов. Одним из аспектов такого контроля выступает обеспечение защиты авторских прав на объект. Технологии ЦВЗ активно используются в составе DRM-систем (Digital Rights Management), однако их область применения чаще

всего ограничивается защитой мультимедийного контента: графических, звуковых и видео файлов [2], [3].

Технологии ЦВЗ основаны на применении стеганографических приемов, в рамках которых скрывается факт наличия ЦВЗ в информационном объекте (контейнере ЦВЗ). При этом ЦВЗ может быть считан из контейнера в случае наличия стего-ключа, определяющего правила доступа к элементам ЦВЗ

© Защелкин К.В., Иванова Е.Н., 2014

[4]. Контроль правомерности использования информационного объекта базируется на том, что правообладатель имеет возможность внедрить в объект ЦВЗ, содержащий идентифицирующие данные правообладателя. Факт наличия этого ЦВЗ в информационном объекте и его содержимое могут быть проявлены только правообладателем, обладающим стего-ключом.

В данной работе предлагается информационная технология внедрения самовосстанавливающихся ЦВЗ в активные аппаратные контейнеры, построенные на основе LUT-ориентированной архитектуры (далее LUT-контейнеры). К таким контейнерам относятся, например, микросхемы FPGA (Field Programmable Gate Array) [5], являющиеся, на текущий момент, весьма используемой элементной базой для построения компьютерных и управляющих систем. Основным элементом таких контейнеров выступают блоки LUT (Look Up Table – таблица поиска), которые представляют собой структуру данных, используемую с целью замены вычислений на операции поиска заготовленных данных [6]. Блоки LUT в FPGA обычно представлены в виде одноразрядной оперативной памяти. Входы блока LUT при этом являются адресными входами такой памяти. При количестве входов, равном  $n$ , блок LUT хранит в себе  $2^n$  бит информации и способен выполнить вычисление значения одной  $n$ -аргументной булевой функции.

В большинстве задач контроля использования информационных объектов существует необходимость восстановления оригинального вида объекта (вида, который тот имел до внедрения ЦВЗ) в процессе считывания ЦВЗ из объекта. Методы обеспечения технологии ЦВЗ, обладающие возможностью восстановления оригинала называются самовосстанавливающимися ЦВЗ.

Самовосстанавливающиеся ЦВЗ получили развитие в области контроля пассивных мультимедийных контейнеров, например графических, звуковых и видео файлов. Однако имеет место необходимость в контроле использования при помощи ЦВЗ не только для информационных объектов такого рода. Задача организации самовосстанавливающихся ЦВЗ в активных контейнерах, выполняющих некоторую

вычислительную или управляющую функцию, на текущий момент не решена. В работах [7], [8] предлагаются методы внедрения ЦВЗ в активные LUT-контейнеры. Однако данные методы не обладают возможностью восстановления оригинала контейнера.

**Цель настоящей работы** состоит в обеспечении возможности восстановления оригинала контейнера после извлечения из него ЦВЗ за счет развития методов организации ЦВЗ в LUT-контейнерах.

**Информационная технология внедрения самовосстанавливающегося ЦВЗ в LUT-контейнер.** Рассматриваемая в данной работе информационная технология является формализованным процессом применения предлагаемых и существующих методов, а также средств обработки информации, направленных на обеспечение организации ЦВЗ в пространстве LUT-контейнеров.

Предлагаемая информационная технология использует композицию подходов метода Фридрих-Голжан-Ду (далее метод ФГД) [9], [10] в части обеспечения самовосстановления контейнера и методов, предложенных авторами в работах [7], [8] в части встраивания ЦВЗ в LUT-контейнеры. Кроме того предлагаемая технология использует такие особенности LUT-контейнеров как активность, точное представление данных, неавтономность их элементарных единиц [7].

Метод ФГД [9], [10] основан на обработке групп – непересекающихся подмножеств элементарных единиц контейнера при помощи двух функций: Flipping-функции  $F()$  и функции дискриминации  $f()$ .

Функция дискриминации используется в методе ФГД для классификации групп контейнера путем отнесения их к классам регулярных, сингулярных и неиспользуемых групп. Определение значения функции на каждой группе контейнера требует вычисления суммы попарных разностей с перекрытием для элементарных единиц контейнера, входящих в группу.

Flipping-функция используется методом ФГД для преобразования групп в соответствии с некоторым правилом, обладающим свойством инволюции.

В предлагаемой информационной технологии учитываются особенности архитекту-

ры LUT-контейнеров, что определяет следующие отличия ее подходов от метода ФГД:

- в рамках предлагаемой технологии, в ходе встраивания ЦВЗ выполняются преобразования не над группами элементарных единиц контейнера, а над самими элементарными единицами (блоками LUT);

- в рамках предлагаемой технологии вычисление Flipping-функции  $F(x)$ , в отличие от метода ФГД, сводится к инвертированию значений блоков LUT в соответствии с процедурой, определенной в [7], [8]. Указанная процедура, состоит в инвертировании значений текущего обрабатываемого блока LUT и выполнении распространения инверсии на входы всех блоков LUT, подключенных к выходу текущего блока. Очевидно, что для данного вида Flipping-функции выполняется требование метода ФГД о наличии свойства инволюции, т.е.  $F(F(LUT_i)) = LUT_i$ , где  $LUT_i$  любое допустимое значение некоторого блока LUT;

- в отличие от метода ФГД, в рамках предлагаемой технологии определяется принцип выполнения классификации элементов контейнера, не прибегая к вычислению какой-либо функции дискриминации. Классификацию элементов предлагается свести к определению соотношения нулевых и единичных значений в кодах блоков LUT по следующему принципу: если блок LUT имеет больше нулевых значений, чем единичных, то он классифицируется как *регулярный блок* ( $R$ -блок); если блок имеет больше единичных значений, чем нулевых, то он классифицируется как *сингулярный блок* ( $S$ -блок); если количество нулевых значений блока LUT равно количеству его единичных значений, то блок классифицируется как *неиспользуемый блок* ( $U$ -блок).

Очевидно, что определяемые методом ФГД правила преобразования классов выполняются и в рамках предлагаемого подхода:

$$\begin{aligned} F(LUT_R) &= LUT_S; \\ F(LUT_S) &= LUT_R; \\ F(LUT_U) &= LUT_U, \end{aligned} \quad (1)$$

где  $LUT_R$ ,  $LUT_S$ ,  $LUT_U$  – блоки LUT, классифицируемые как  $R$ -блок,  $S$ -блок и  $U$ -блок соответственно;  $F()$  – Flipping-функция.

На рис. 1 показаны примеры применения Flipping-функции  $F()$  к блокам LUT. В при-

мере (рис. 1, а) выполняется инвертирование кода блока, классифицированного как  $R$ -блок из-за преобладания нулевых значений. В результате такого преобразования блок трансформируется в  $S$ -блок (в его коде преобладают единичные значения). На рис. 1, б, показан пример обратного преобразования  $S$ -блок – в результате инвертирования трансформируется в  $R$ -блок. В примере на рис. 1, в видно, что  $U$ -блок (блок с одинаковым количеством единичных и нулевых значений в коде) в результате подобного преобразования остается  $U$ -блоком.

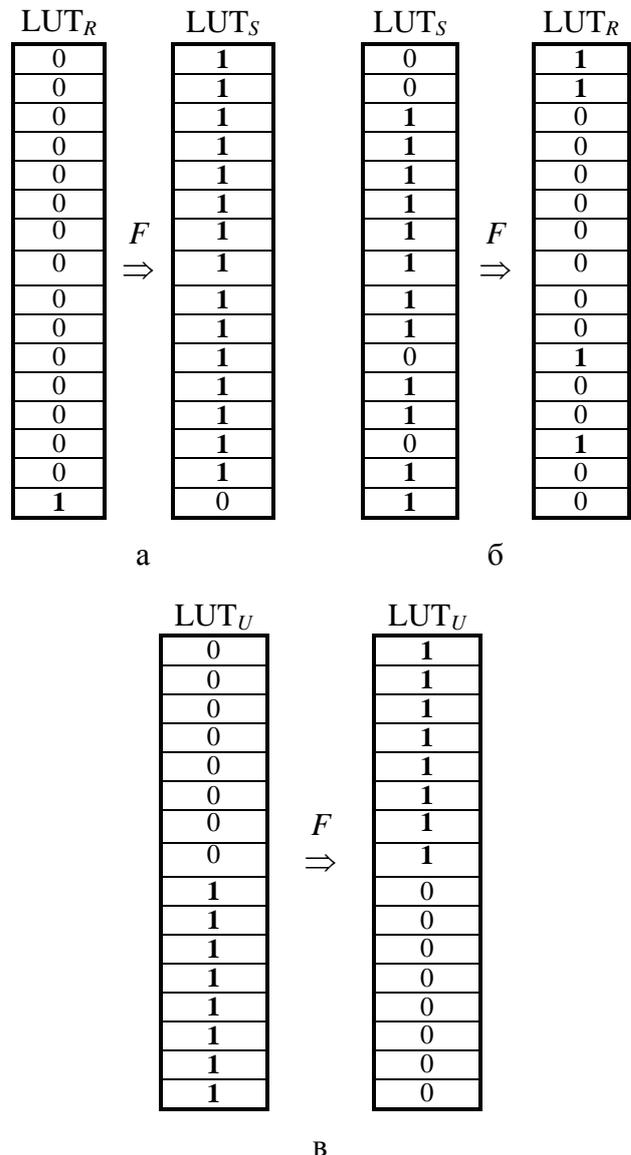


Рис. 1. Примеры взаимных преобразований классов для блоков LUT

Последовательность действий предлагаемой информационной технологии в части

внедрения ЦВЗ в LUT-контейнер состоит в следующем.

*Этап 1.* Осуществляется движение по блокам LUT контейнера в порядке, определяемом стегопутем. При этом выполняется отнесение каждого блока LUT к классам *R*-блоков, *S*-блоков или *U*-блоков на основании указанных выше правил классификации. По результатам классификации следующим образом формируется двоичный *RS*-вектор: если очередной блок LUT классифицирован как *R*-блок, то в *RS*-вектор заносится значение 0; если очередной блок классифицирован как *S*-блок, то в *RS*-вектор заносится значение 1; для *U*-блоков значения в *RS*-вектор не заносятся.

*Этап 2.* Выполняется сжатие полученного *RS*-вектора при помощи некоторого алгоритма сжатия без потерь. В результате формируется сжатый вектор  $RS_{com}$ . Очевидно, что размер вектора  $RS_{com}$  будет меньше размера вектора *RS*. Разность величин этих векторов обозначим  $\Delta L$ .

*Этап 3.* К вектору  $RS_{com}$  путем конкатенации добавляется ЦВЗ, который представляет собой двоичную последовательность, длина которой не превышает  $\Delta L$ . Полученный после конкатенации вектор  $RS^*$  дополняется до длины вектора *RS* произвольными двоичными значениями. Таким образом:

$$RS^* = RS_{com}.DWM.Add, \quad (2)$$

где «.» – операция конкатенации;  
*DWM* – ЦВЗ внедряемый в контейнер;  
*Add* – опциональное дополнение вектора  $RS^*$  до длины вектора *RS*.

*Этап 4.* Выполняется движение по блокам LUT контейнера в порядке, определяемом стегопутем. В ходе этого движения *U*-блоки игнорируются, а *R*-блоки и *S*-блоки модифицируются при помощи Flipping-функции в соответствии с таблицей.

### 1. Принцип преобразования блоков LUT

Класс текущего блока $LUT_i$	Очередной разряд вектора $RS^*$	Действие
<i>R</i>	0	—
<i>R</i>	1	Преобразовать $LUT_i$ в <i>S</i> -блок
<i>S</i>	0	Преобразовать

		$LUT_i$ в <i>R</i> -блок
<i>S</i>	1	—

Исходя из того, что действия Flipping-функции на блоки LUT выполняются в соответствии с правилами инвертирования блоков, изложенными в [7], [8], функционирование LUT-контейнера в результате встраивания в него ЦВЗ не претерпевает каких-либо изменений.

Стего-ключ для извлечения данных в рамках предложенной технологии представляет собой следующую четверку компонентов:

$$key = (order, classification, RSrule, \Delta L), \quad (3)$$

где *order* – информация, определяющая порядок обхода блоков LUT в контейнере (стегопуть) для выполнения встраивания или извлечения ЦВЗ;

*classification* – конкретизация принципа классификации блоков LUT (блок считается *R*-блоком при большем или же при меньшем количестве единиц в коде блока);

*RSrule* – правило интерпретации значений разрядов векторов *RS*,  $RS_{com}$ ,  $RS^*$ : для *R*-блоков в *RS*-вектор заносится значение 0, а для *S*-блоков – 1, или наоборот;

$\Delta L$  – разница между длиной вектора *RS* и длиной его сжатой версии  $RS_{com}$ .

Последовательность действий предлагаемой информационной технологии в части извлечения ЦВЗ и восстановления оригинального вида LUT-контейнера состоит в следующем.

*Этап 1.* Осуществляется движение по блокам LUT контейнера в порядке, определяемом стегопутем. При этом, аналогично тому, как это делалось при внедрении информации, на основании классификации блоков LUT, формируется двоичный вектор  $RS'$ .

*Этап 2.* Структура полученного вектора  $RS'$  соответствует структуре вектора  $RS^*$  (2), сформированного при внедрении ЦВЗ в контейнер. Последние  $\Delta L$  разрядов вектора  $RS'$  представляют собой ЦВЗ с возможным дополнением до необходимой длины вектора. На данном этапе выполняется считывание этих разрядов и получение ЦВЗ.

*Этап 3.* Остальные разряды вектора подвергаются процедуре декомпрессии, обратной сжатию, выполненному на этапе внедрения информации. В результате формируется двоичный вектор  $RS_{decom}$ .

*Этап 4.* На основании информации, содержащейся в векторе  $RS_{decom}$ , производится восстановление оригинального вида контейнера. Для этого выполняется движение по блокам LUT контейнера в порядке, определяемом стегапутем, и последовательный перебор значений вектора  $RS_{decom}$ . В ходе этого движения  $U$ -блоки игнорируются, а  $R$ -блоки и  $S$ -блоки модифицируются при помощи Flipping-функции в соответствии с табл. 1.

**Экспериментальное исследование предлагаемой технологии.**

*Цели экспериментального исследования:*

1) экспериментально показать, что LUT-контейнеры, в которые при помощи предложенной технологии были внедрены ЦВЗ, принимают свой первоначальный вид после извлечения ЦВЗ;

2) установить степень изменения основных характеристик контейнеров после внедрения в них ЦВЗ. В качестве основных характеристик рассматривались: а) максимальная частота тактирования, выражающая предельное быстродействие устройств, в рамках одного семейства целевых микросхем; б) энергопотребление системы ввода-вывода микросхемы; в) энергопотребление ядра микросхемы; г) тепловыделение микросхемы.

*Среда проведения экспериментов.* Для экспериментального исследования 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 предложенной технологией, реализована на языке C# в рамках платформы .Net. Измерения указанных выше характеристик проектов проводились средствами модулей САПР Altera Quartus II Timing Analyzer (оценка предельного быстродействия) и Power Play (оценка энергопотребления и тепловыделения). Состояния контейнера до внедрения ЦВЗ и после извлечения ЦВЗ сравнивались путем побитового анализа конфигурационных файлов соответствующих контейнеров.

*Материалом для экспериментов* выступили 40 FPGA-проектов различного объема и

назначения. Аппаратная сложность устройств в рамках данных проектов варьировался от 1,2% до 65% объема ресурсов (логических ячеек, блоков памяти) целевой микросхемы FPGA.

*Процесс проведения экспериментов.* Эксперименты для каждого исследуемого проекта состояли из следующих этапов:

1) измерение основных характеристик (быстродействие, энергопотребление, тепловыделение) для устройства, представленного в виде исходного контейнера;

2) внедрение случайной двоичной последовательности ЦВЗ в контейнер;

3) измерение основных характеристик для контейнера, содержащего встроенный ЦВЗ;

4) извлечение ЦВЗ из заполненного контейнера;

5) сравнение конфигурационных файлов полученного и исходного контейнеров.

*Результаты экспериментального исследования.* В результате проведения экспериментов для всех 40 исследованных проектов установлено полное совпадение конфигурационных файлов исходных контейнеров и контейнеров, полученных после извлечения из них ЦВЗ. Таким образом, благодаря свойству самовосстановления, после извлечения ЦВЗ из контейнеров, они принимали оригинальный вид и их характеристики возвращались к первоначальным значениям.

В части установления степени изменения основных характеристик контейнеров (после внедрения ЦВЗ) были получены следующие результаты. Имело место очень незначительное изменение характеристик контейнеров в результате внедрения ЦВЗ. При этом зависимость этого изменения от аппаратной сложности устройства и его структурных особенностей наблюдалась крайне малая. Так разница в изменении характеристик для устройств, занимающих 1,2 % и занимающих 65 % объема ресурсов целевой микросхемы FPGA, составляла сотые доли процента. В среднем (для всех исследованных 40 проектов) изменение скоростных характеристик составило 0,18 %, изменение характеристики энергопотребления и тепловыделения – 0,22 %. Как видно величина изменений находится на уровне погрешности средств измерения.

**Выводы.** Предложенная в работе информационная технология позволяет выпол-

нять внедрение ЦВЗ в контейнеры с LUT-ориентированной архитектурой. Технология дает возможность восстановить первоначальное состояние контейнера после извлечения из него ЦВЗ. Технология основана на композиции метода внедрения ЦВЗ в LUT-контейнеры, предложенного авторами данной работы и известного метода ФГД, ориентированного на работу с пассивными мультимедийными контейнерами. В отличие от метода ФГД, предлагаемая технология:

- использует более простую Flipping-функцию, учитывающую особенности контейнера;
- не предполагает вычисления функций дискриминации для выполнения классификации элементов контейнера;
- выполняет внедрение информации на уровне элементарных единиц контейнера (блоков LUT), а не на уровне групп элементарных единиц.

Мера эффективности предложенной технологии, в данной работе, носит качественный характер и выражается в обеспечении, отсутствующей ранее, возможности восстановления оригинала LUT-контейнера после извлечения из него ЦВЗ. Однако для данной технологии требуется определение и оценка также количественных мер ее эффективности. Этот вопрос является предметом дополнительных исследований, которые найдут отражение в последующих публикациях.

Предложенная технология может найти применение при разработке аппаратно-программного обеспечения, реализующего внедрение цифровых водяных знаков в вычислительные и управляющие устройства, построенные на основе LUT-ориентированной элементной базы (например, FPGA или программируемые логические интегральные схемы 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.

Целесообразность применения подходов предложенной информационной технологии определяется необходимостью восстановле-

ния первоначального вида LUT-контейнера. В случае отсутствия такой необходимости следует использовать вычислительно более простые методы встраивания дополнительной информации в LUT-контейнеры [7] и [8], не требующие процедур сжатия и декомпрессии информации.

#### Список использованной литературы

1. Cox I., Miller M., Bloom J., and Fridrich J. (2008), *Digital Watermarking and Steganography*, Burlington: Morgan Kaufmann Publishers, 592 p.
2. Конахович Г. Ф. Компьютерная стеганография [Текст] / Г. Ф. Конахович, А. Ю. Пузыренко. – К. : МК-Пресс, 2006. – 288 с.
3. Аграновский А. В. Стеганография, цифровые водяные знаки и стегоанализ [Текст] / А. В. Аграновский, А. В. Балакин, В. Г. Грибунин. – М. : Вузовская книга, 2009. – 220 с.
4. Shih F., (2012), *Watermarking, Steganography, and Forensics*, New York, CRC Press, 424 p.
5. Грушвицкий Р. И. Проектирование систем на микросхемах с программируемой структурой [Текст] / Р. И. Грушвицкий, А. Х. Мурсаев, Е. П. Угрюмов. – СПб.: БХВ, 2010. – 650 с.
6. Paul S., Bhunia S., (2008), *Reconfigurable Computing Using Content Addressable Memory for Improved Performance and Resource Usage*, *Proceedings of Design Automation Conference ACM/IEEE (DAC-2008)*, Anaheim, pp. 786 – 791.
7. Защелкин К. В. Метод стеганографического скрытия данных в LUT-ориентированных аппаратных контейнерах [Текст] / К. В. Защелкин, Е. Н. Иванова // *Электротехнические и компьютерные системы*. – К. : 2013. – № 12 (88). – С. 83 – 90.
8. Защелкин К.В. Развитие метода стеганографического скрытия данных в LUT-ориентированных аппаратных контейнерах [Текст] / К.В. Защелкин, Е.Н. Иванова // *Электротехнические и компьютерные системы*. – К. : 2014. – № 13 (89). – С. 231 – 239.
9. Fridrich J., Goljan M., and Du R., (2002), *Lossless Data Embedding – New Paradigm in Digital Watermarking*, *Journal on Applied Signal Processing: Emerging Applications*

of *Multimedia Data Hiding*, USA, New York, *Hindawi Publishing*, pp. 185 – 196.

10. Goljan M., Fridrich J., and Du R. (2001), Distortion-Free Data Embedding for Images, *Proceedings of the 4th International Workshop on Information Hiding (IHW-01)*, USA, *Pittsburg*, pp. 27 – 41.

Получено 25.1.2014

#### References

1. Cox I., Miller M., Bloom J., and Fridrich J., (2008), Digital Watermarking and Steganography, Burlington, *Morgan Kaufmann Publishers*, 592 p. (In English), doi: 10.1016/b978-012372585-1.50015-2.

2. Konahovich G.F., and Puzirenko A.U., (2006), *Kompyuternaya steganografiya* [Computer Steganography], Kiev, Ukraine, *MK-Press Publ.*, 288 p. (In Russian).

3. Agranovsky A.V., Balkin A.V., and Gribunyn V.G., (2009), *Steganografiya, tsifrovye vodyanye znaki i stegoanaliz* [Steganography, Digital Watermarks and Stegoanalysis], Moscow, Russian Federation: *University Book Publ.*, 220 p. (In Russian).

4. Shih F. (2012), Watermarking, Steganography, and Forensics, New York, *CRC Press Publ.*, 424 p. (In English), doi: 10.1201/b12697-6.

5. Grushvitsky R.I., Mursaev A.H. and Ugryumov E.P. (2010), *Proektirovanie sistem na mikroskhemakh s programmiruemoi strukturoi* [Design of Systems on a Chip with Programmable Structure], St. Petersburg, Russian Federation, *BHV Publ.*, 650 p. (in Russian).

6. Paul S., and Bhunia S., (2008), Reconfigurable Computing Using Content Addressable Memory for Improved Performance and Resource Usage, *Proceedings of Design Automation Conference ACM/IEEE (DAC-2008)*, Anaheim, pp. 786–791, (in English), doi: 10.1145/1391469.1391670.

7. Zashcholkin K.V. and Inanova E.N., (2013), Metod steganograficheskogo skrytiya dannykh v LUT-orientirovannykh apparatnykh konteinerakh [Method of Steganographical Hiding of Information in LUT-oriented Hardware Containers], *Electrotechnic and Computer Sys-*

*tems*, Kiev, Ukraine, No. 12 (88), pp. 83 – 90 (In Russian).

8. Zashcholkin K.V. and Inanova E.N., (2014), Razvitie metoda steganograficheskogo skrytiya dannykh v LUT-orientirovannykh apparatnykh konteinerakh [Method Development for Implementing the Steganography Data Hiding in LUT-oriented Hardware Containers], *Electrotechnic and Computer Systems*, Kiev, Ukraine, No. 13 (89), pp. 231 – 239 (In Russian), doi: 10.15276/etks.13.89.2014.33.

9. Fridrich J., Goljan M. and Du R., (2002), Lossless Data Embedding – New Paradigm in Digital Watermarking, *Journal on Applied Signal Processing: Emerging Applications of Multimedia Data Hiding*, USA, New York: *Hindawi Publishing*, pp. 185 – 196 (in English), doi: 10.1155/s1110865702000537.

10. Goljan M., Fridrich J., and Du R., (2001), Distortion-Free Data Embedding for Images, *Proceedings of the 4th International Workshop on Information Hiding (IHW-01)*, USA, *Pittsburg*, pp. 27 – 41 (in English), doi: 10.1007/3-540-45496-9\_3.



Защелкин  
Константин Вячеславович,  
канд. техн. наук, доц. каф.  
компьютерных интеллектуальных систем и сетей  
Одесского нац. политехнич. ун-та,  
тел.: (048) 734-83-22,  
e-mail: const-z@te.net.ua



Иванова  
Елена Николаевна,  
ст. преподаватель каф. компьютерных систем  
Одесского нац. политехнич. ун-та,  
тел.: (048) 734-83-91,  
e-mail: enivanova@ukr.net