УДК 004.93:61

И.И. Маракова, д-р техн. наук, проф., Telecom Bretagne, Брест, Франция,
Л.А. Кузнецова, инженер,
А.А. Яковенко, магистр,
Одес. нац. политехн. ун-т

СИСТЕМА ВЕРИФИКАЦИИ МЕДИЦИНСКИХ ИЗОБРАЖЕНИЙ НА ОСНОВЕ РЕВЕРСИВНЫХ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

І.І. Маракова, Л.А. Кузнецова. О.О. Яковенко. **Система верифікації медичних зображень на основі реверсивних цифрових водяних знаків.** Пропонується метод впровадження реверсивних цифрових водяних знаків (ЦВЗ), заснований на попередньому інверсному перетворенні зображення. Сформований вектор зображення кодується без втрат, його конкатенація з ідентифікатором зображення і конфіденційною частиною медичного кода становить ЦВЗ зображення. Медичне зображення з ЦВЗ зберігається в розподіленій базі даних і може використовуватися в медичній практиці в силу непомітності ЦВЗ. Пропускна здатність залежить від непомітності ЦВЗ, при її збільшенні непомітність може погіршитися. Для пошуку компромісу між цими двома вимогами використовується оцінка параметрів попереднього інверсного перетворення на основі гістограм яскравості зображень.

Ключові слова: стеганографія, реверсивні цифрові водяні знаки, арифметичне кодування, растрове зображенння, медичні зображення.

И.И. Маракова, Л.А. Кузнецова, А.А. Яковенко. **Система верификации медицинских изображений на основе реверсивных цифровых водяных знаков.** Предлагается метод внедрения реверсивных цифровых водяных знаков (ЦВЗ), основанный на предварительном инверсном преобразовании изображения. Сформированный вектор изображения кодируется без потерь, его конкатенация с идентификатором изображения и конфиденциальной частью медицинской информации составляет ЦВЗ изображения. Медицинское изображение с ЦВЗ хранится в распределенной базе данных, и может быть использовано в медицинской практике в силу незаметности ЦВЗ. Пропускная способность зависит от незаметности ЦВЗ, при ее увеличении незаметность может ухудшиться. Для поиска компромисса между этими двумя требованиями используется оценка параметров предварительного инверсного преобразования на основе гистограмм яркости изображений.

Ключевые слова: стеганография, реверсивные цифровые водяные знаки, арифметическое кодирование, растровое изображение, медицинские изображения.

I.I. Marakova, L.A.Kuznetsova, O.O. Yakovenko. **Reversible watermarking scheme for medical imagery verification.** A reversible digital watermarking (DWM) technique based on the preliminary reversible image transform is proposed. The formed image vector is encoded loss-free. Its concatenation with an identifier of the image and a confidential part of the medical code forms the WM. The medical images with WM are stored in the distributed database, and as they are imperceptible, they could be used for medical practice. Embedding capacity depends on the WM imperceptibility, if the capacity gets bigger, the imperceptibility gets worse. To find a balance between those two factors, the estimation of the parameters of preliminary reversible treatment according to the image luminance histograms is used.

Keywords: steganography, reversible digital watermarking, arithmetic coding, bitmap, medical images.

Конфиденциальность и целостность медицинской информации, как правило, регламентируется законодательными и этическими нормами. Темпы развития информационных технологий, медицинского диагностического оборудования явно опережают разработку соответствующих законодательных норм. Это обусловило необходимость развития технологий защиты медицинской информации, представленной в цифровом виде.

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

При внедрении цифровых водяных знаков (ЦВЗ) в изображение некоторые его элементы неизбежно претерпевают изменение. Таким образом, в существующих системах ЦВЗ идет речь о достоверном установлении источника распространения изображения, а не о его информационной целостности, которая нарушается уже в момент добавления в изображения какого-либо идентификатора.

Однако, для некоторых видов изображений, в частности, для медицинских снимков магниторезонансной томографии, гарантия целостности изображения является одним из приоритетных критериев системы ЦВЗ. Целостность изображения в таком случае может гарантироваться так же, как и для других типов файлов — путем хеширования файла изображения. Хеш-суммы изображений могут храниться в отдельной защищенной базе данных, но для удобства системы также желательно, чтобы хеш или любой другой идентификатор гарантирующий целостность изображения, был внедрен в само изображение.

Проблема реализации указанной системы состоит в том, что она должна удовлетворять таким, на первый взгляд противоречивым, требованиям:

— в изображения должен внедряться идентификатор, гарантирующий его целостность на битовом уровне;

— идентификатор должен быть внедрен в информационную часть изображения, и должен быть незаметен либо слабо заметен невооруженным глазом;

— добавление идентификатора не должно увеличивать размер изображения.

Реализация такой системы возможна исключительно с применением реверсивных ЦВЗ — водяных знаков, алгоритм добавления которых предусматривает возможность полного восстановления изображения после извлечения скрытого идентификатора [1] .

Для решения этой проблемы предлагается метод внедрения реверсивных ЦВЗ в изображения формата BMP [2], а также система идентификации и верификации изображений медицинской диагностики, основанная на предложенном методе.

Изначально для каждого изображения необходимо сформировать его уникальный идентификатор, который может иметь произвольную форму. Эксперименты проводились с использованием 160-битного идентификатора, являющегося цифровой подписью SHA-1 [3] исходного изображения. Затем изображение в виде матрицы значений яркости каждого пикселя подвергается предварительному преобразованию, в ходе которого оценивается дискриминационная функция преобразования уровня [4]. Полученный идентификатор изображения погружается как невидимая цифровая метка в изображение, не увеличивая его объем. Процедуры идентификации и верификации включает следующие этапы: извлечение уникального идентификатора, погруженного в изображение, восстановление изображения, вычисление уникального идентификатора восстановленного изображения и сравнение двух этих идентификаторов. При их совпадении целостность изображения подтверждается.

Также к системе предъявляется специфическое требование, заключающееся в том, что последовательные операции погружения и извлечения идентификатора не должны повлечь за собой изменения даже одного бита восстановленного изображения по отношению к исходному [4]. Уникальный идентификатор изображения **ID** как правило, содержит не менее, чем 64 бита. Особенность медицинского приложения заключается в том, что требуется обеспечить надежный уровень восприятия изображения до момента его восстановления: в состоянии хранения изображения с ЦВЗ врач может потребовать хранение некоторого фрагмента изображения в неизмененном состоянии, но с обеспечением его верификации. При этом возможно формирование идентификатора для некоторой части изображения, и погружение этого идентификатора в оставшуюся часть, что, однако, потребует дополнительных усилий по сохранению основных параметров эффективности системы и надежности восприятия всего изображения.

Предлагаемый метод погружения реверсивных ЦВЗ для идентификации и верификации изображений в формате BMP позволяет восстановить исходное изображение с точностью до одного бита. При этом возможно погружение каждого бита идентификатора как в отдельно взятый пиксель, так и в группу пикселей. Предложенная система ЦВЗ несекретна, т.е. не требуется

знание секретного ключа; в ней не реализуется принцип Керкгоффса [5]; при извлечении ЦВЗ не требуется знание исходного изображения, т.е. детектор ЦВЗ является неинформированным.

Для упрощения изложения и без потери общности рассматриваются изображения в градации серого, т.е. с 8-битовой глубиной цвета пикселя. Размер изображения составляет $N1 \times N2$ пикселей, каждый из которых может характеризоваться дискретным значением яркости x в диапазоне $P = \{0,1,...,255\}$.

Представим исходное изображение $X = \{x_1, x_2, ..., x_{N1 \times N2}\}$ размером $N1 \times N2$ пикселей в виде K групп $G_k = \{x_1^k, x_2^k, ..., x_N^k\}$, $k \in \{1, ..., K\}$, из одинакового числа пикселей $N=n^2$ каждая. Изображение разбивается на группы G_k соседствующих пикселей аналогично разбиению на октеты в форматах JPEG и MPEG [6]. Предварительное преобразование заключается в формировании для каждой из групп G_k на основании функции преобразования уровня яркости пикселей $F(x)$ соответствующей группы $G1_k$:

$$G_k = \begin{vmatrix} x_{1,1}^k & x_{1,2}^k & ... & x_{1,n}^k \\ x_{2,1}^k & x_{2,2}^k & ... & x_{2,n}^k \\ & \vdots & & \\ x_{n,1}^k & x_{n,2}^k & & x_{n,n} \end{vmatrix} \Rightarrow G1_k = \begin{vmatrix} y_{1,1}^k & y_{1,2}^k & ... & y_{1,n}^k \\ y_{2,1}^k & y_{2,2}^k & ... & y_{2,n}^k \\ & \vdots & & \\ y_{n,1}^k & y_{n,2}^k & & y_{n,n} \end{vmatrix}, \quad (1)$$

где $x_{i,j}$ — значения яркости пикселей до преобразования;

$y_{i,j}^k = F(x_{i,j}^k)$ — значение яркости пикселей после преобразования;

$i, j = \{1, ..., n\}$;

$G1_k = \left\{ y_1^k, y_2^k, ..., y_N^k \right\}$, $N1 \times N2 = N \times K$, $k \in \{1, ..., K\}$.

Функция преобразования уровня $F(x)$ по сути является некоторым правилом (см. таблицу), в соответствии с которым осуществляется пересчет значения яркости пикселей каждой группы G_k в зависимости от заранее определенной амплитуды A преобразования $F(x)$.

Правило пересчета значения яркостей отдельных пикселей

Яркость пикселя исходного изображения, x / Амплитуда A преобразования $F(x)$	0	1	2	3	4	5	6	7	…	252	253	254	255
1	1	0	3	2	5	4	7	6	…	253	252	255	254
2	2	3	0	1	6	7	4	5	…	254	255	252	253
3	3	4	5	0	1	2	9	10	…	255	250	251	252
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
50	50	51	52	53	54	55	56	57	…	199	200	201	202

В аналитическом виде значение яркости пикселя y преобразованного изображения зависит от яркости пикселя x исходного изображения следующим образом:

$$y = F(x) = 2A\left\lfloor \frac{x}{2A} \right\rfloor + (x \bmod 2A + A) \bmod 2A, \quad (2)$$

где $\lfloor \ \rfloor$ — округление вниз до ближайшего целого;

mod — остаток от деления.

Функция $F(x)$ (2) характеризуется следующим важным для процедуры верификации свойством инволюции [7]:

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

$$F(F(x_n^k)) = x_n^k, \forall x_n^k \in P, \quad (3)$$

что впоследствии позволит осуществить однозначное восстановление изображения после погружения и извлечения идентификатора. Для дальнейшего преобразования групп G_k используется функция дискриминации уровня яркости пикселей [4]

$$f(G_k) = \sum_{n=1}^{N-1} \left| x_{n+1}^k - x_n^k \right|. \quad (4)$$

Аналогичные преобразования необходимо осуществить для групп $G1_k$

$$f(G1_k) = \sum_{n=1}^{N-1} \left| y_{n+1}^k - y_n^k \right|. \quad (5)$$

На основании сравнения полученных значений $f(G_k)$ (4) и $f(G1_k)$ (5) все группы можно разделить на следующие классы:

— (i) “регулярные” группы (РГ), для которых $f(G_k) < f(F(G_k))$;

— (ii) “сингулярные” группы (СГ), для которых $f(G_k) > f(F(G_k))$;

— (iii) “неиспользуемые” группы (НГ), для которых $f(G_k) = f(F(G_k))$.

Рассмотренные классы групп характеризуются следующими свойствами [4]:

— F(РГ) = СГ;

— F(СГ) = РГ;

— F(НГ) = НГ.

Формализация этапов предварительного преобразования исходного изображения:

— изображение представляется в виде k групп соседствующих пикселей G_k, $k \in \{1, ..., K\}$;

— на основании функции $F(x)$ при заданной амплитуде преобразования A множество групп G_k преобразуется в множество соответствующих групп $G1_k$;

— для каждой пары G_k и $G1_k$ рассчитывается функция дискриминации $f(x)$ (4), (5);

— формируется бинарный вектор $\mathbf{R} = \{r_1, r_2, ..., r_k, ..., r_L\}$ на основании правила сравнения групп G_k и $G1_k$:

— $r_k = 1$, если группа G_k является регулярной;

— $r_k = 0$, если группы G_k является сингулярной.

Группы, для которых $f(G_k) = f(F(G_k))$, не участвуют в формировании вектора $\mathbf{R}$, т.е. его длина $L \le K$. Вектор $\mathbf{R}$ содержит информацию о распределении различных групп G_k.

Далее к бинарному вектору $\mathbf{R}$ применим операцию арифметического кодирования [9]. Длина L_1 сжатого вектора $\mathbf{RS} = \{rs_1, rs_2, ..., rs_{L_1}\}$ (R-Short) будет меньше длины исходного вектора L. Разница $\Delta L = L - L_1$ соответствует числу бит, которые могут быть использованы для записи идентификатора изображения $\mathbf{ID}$, длина которого L_2. Если $L_2 < \Delta L$, то возникает возможность погружения дополнительной информации. В результате получим новый вектор $\mathbf{RS1}$.

Формализуем этапы процедуры формирования ЦВЗ:

— формирование вектора, представляющего идентификатор исходного изображения $\mathbf{ID} = \{d_1, d_2, ..., d_{L_2}\}$;

— сжатие бинарного вектора $\mathbf{R} = \{r_1, r_2, ..., r_L\}$. Результат арифметического кодирования вектора $\mathbf{R}$ — вектор $\mathbf{RS} = \{rs_1, rs_2, ..., rs_{L_1}\}$;

— конкатенация векторов $\mathbf{RS} = \{rs_1, rs_2, ..., rs_{L_1}\}$ и $\mathbf{ID} = \{d_1, d_2, ..., d_{L_2}\}$;

— результирующий вектор $\mathbf{RS1} = \{rs_1, rs_2, ..., rs_{L_1}, d_1, d_2, ..., d_{L_2}\} = \{rd_1, rd_2, ..., rd_L\}$ является ЦВЗ.

Правила погружения сформированного ЦВЗ:

— группа пикселей стеганоизображения S_k не отличается от соответствующей группы исходного изображения, если $f(G1_k) = f(G_k), S_k \to G_k$;

— группа пикселей стеганоизображения S_k не отличается от соответствующей группы исходного изображения, если $rd_k = r_k, S_k \to G_k$;

— группа пикселей стеганоизображения S_k образуется на основе преобразования (1) соответствующей группы исходного изображения, $G_k \to G1_k$, если $rd_k \neq r_k$.

Совокупность значений яркости пикселей, полученных в результате преобразования изображения по указанным правилам, и является множеством $S = \{s_1, s_2, ..., s_{N1 \cdot N2}\}$, которое хранится в базе данных.

Для верификации изображения $S = \{s'_1, s'_2, ..., s'_{N1 \times N2}\}$ необходимо выделить ЦВЗ, для чего выполняются следующие этапы преобразования $G_k^{s'} = \{s_1'^k, s_2'^k, ..., s_N'^k\}$:

— изображение с ЦВЗ $S = \{s'_1, s'_2, ..., s'_{N1 \times N2}\}$ разбивается на группы $G_k^{s'} = \{s_1'^k, s_2'^k, ..., s_N'^k\}$, $k \in \{1, ..., K\}$;

— стеганоизображение представляется в виде множества групп $G1_k^{S'}$;

— для всех $G1_k^{S'}$ рассчитывается функция дискриминации $f(x)$;

— на основании сравнения всех пар $G_k^{s'}$ и $G1_k^{s'}$ формируется вектор

$$\mathbf{RS1}' = \{rd'_1, rd'_2, ..., rd'_k, ..., rd'_L\} = \{rs'_1, rs'_2, ..., rs'_k, ..., rs'_{L_1}, d'_1, d'_2, ..., d'_k, ..., d'_{L_2}\};$$

— последние L_2-бит полученного вектора $\mathbf{RS1}'$ являются идентификатором

$$\mathbf{ID}' = \{d'_1, d'_2, ..., d'_k, ..., d'_{L_2}\};$$

— далее необходимо восстановить с точностью до одного бита исходное изображение, для чего выполняется арифметическое декодирование вектора

$$\mathbf{RS}' = \mathbf{RS1}' - \mathbf{ID} = \{rs'_1, rs'_2, ..., rs'_k, ..., rs'_{L_1}\};$$

Правила преобразование стеганоизображения:

— если $rd'_k = r'_k$, пиксели не подвергаются никаким изменениям,

$$G'_k = G_k^{S'}, \quad \{x_1'^k, x_2'^k, ..., x_N'^k\} = \{s_1'^k, s_2'^k, ..., s_N'^k\}.$$

—если $rd'_k \neq r'_k$, выполняется операцию преобразования уровней

$$G'_k \to G1_k^{S'}, \quad \{x_1'^k, x_2'^k, ..., x_N'^k\} = \{y_1'^k, y_2'^k, ..., y_N'^k\};$$

— пиксели НГ не изменяются:

$$G'_k \to G1_k^{S'}, \quad \{x_1'^k, x_2'^k, ..., x_N'^k\} = \{s_1'^k, s_2'^k, ..., s_N'^k\}.$$

Для восстановленного изображения вычисляется идентификатор $\mathbf{ID}$, на основании сравнения которого с $\mathbf{ID}' = \{d'_1, d'_2, ..., d'_k, ..., d'_{L_2}\}$ подтверждается целостность изображения.

На основе описанного метода реализована программная версия системы верификации и идентификации медицинских изображений. Программа разработана на платформе Microsoft.NET [8]. В программе реализовано внедрение в изображение его hash-значения SHA1. Система апробирована для базы данных изображений диагностики мозга. Три изображения диагностики мозга и соответствующие им гистограммы распределения яркости представлены (рис. 1). Для арифметического кодирования вектора **R** использовалась программа адаптивного арифметического кодирования [4].

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

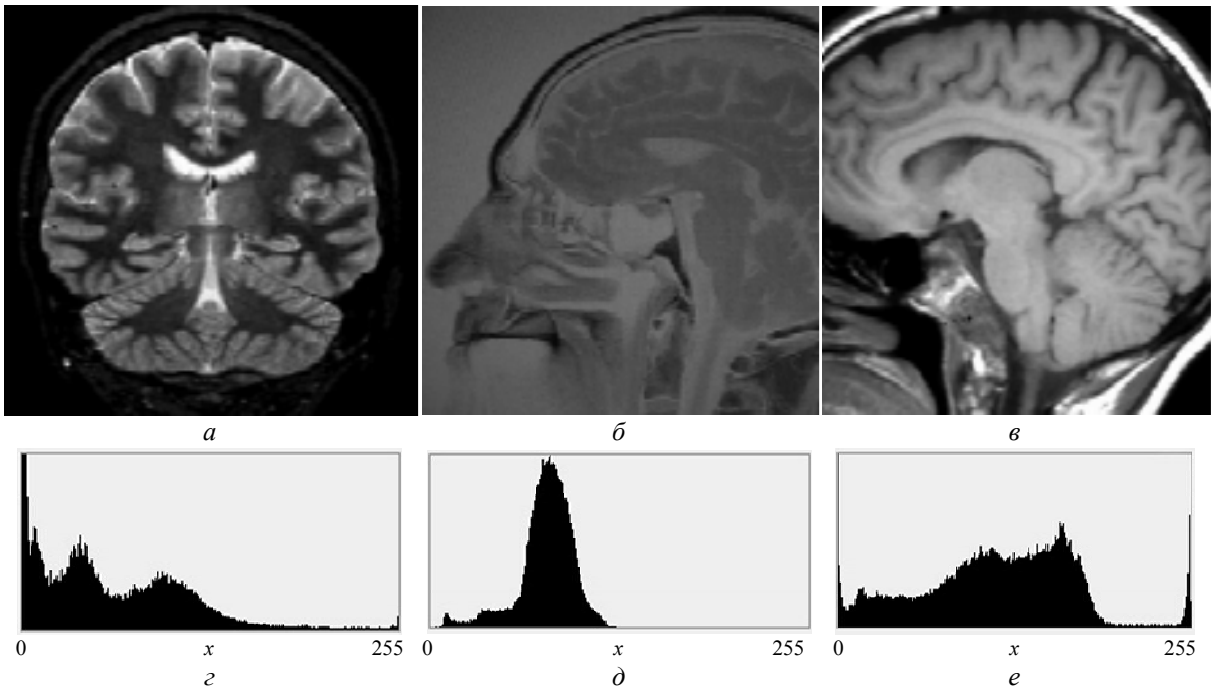

Рис. 1. Исходные изображения размером 256×256 пикселей (а, б, в), соответствующие гистограммы распределения яркости (г, д, е).

С точки зрения надежности восприятия изображения с погруженным идентификатором рассматривались амплитуды преобразования уровней $A = 2, 4, 8$ и размеры групп $N = 4, 16, 64$.

Пропускная способность системы верификации и аутентификации зависит от значений параметров предварительного преобразования $L, L_1, L_2, A, N1, N2$, которые, в свою очередь, определяются гистограммой яркости изображения (рис. 2). Для светлых изображений верификация при обеспечении незаметности ЦВЗ возможна при $N = 64$, $A = 4$. Однако, для темных изображений верификация выполнима при $N \le 16$, $A \ge 6$, и для обеспечения незаметности ЦВЗ могут потребоваться дополнительные усилия.

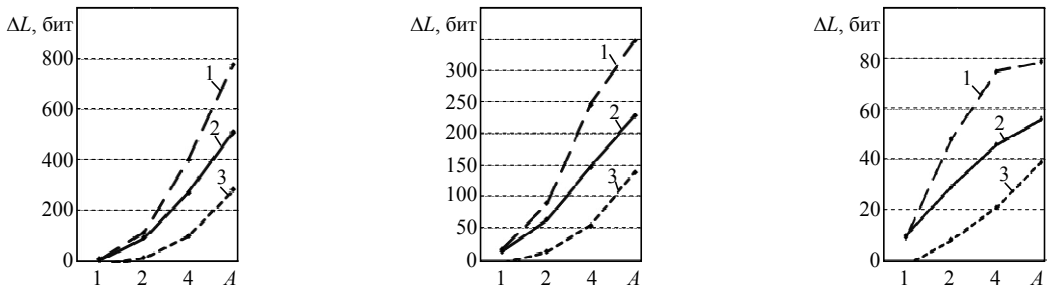

Рис. 2. Зависимость допустимого размера вектора **ID′**, *бит, от параметров преобразования A, $L_2 = f(A)$, при размерах G_k: 2×2 (а); 4×4 (б); 8×8 (в); 1, 2, 3 — для изображения а, б, в (рис. 1), соответственно*

Очевидна зависимость обеспечения незаметности ЦВЗ от параметра преобразования ЦВЗ *A* и размера группы преобразования. Для каждого изображения существует оптимальное соотношение данных параметров.

Предложен метод идентификации и верификации медицинских диагностических изображений, основанный на реверсивных ЦВЗ. Параметры преобразования, такие как размер группы преобразования N и параметр преобразования A, могут быть адаптивно настроены, что позволяет обеспечить необходимый уровень гибкости для достижения баланса между емкостью внедряемой в изображение информации ΔL и незаметностью внедрения. Метод был реализован и протестирован с использованием реальных данных. Результаты теста показали, что он может быть использован в распределенной базе данных медицинских изображений, где критерии целостности изображений и незаметности водяного знака являются определяющими.

На основании метода разработана система верификации медицинских изображений, реализующая преимущества описанного метода, и позволяющая проводить дальнейшие исследования с целью его дальнейшего развития и оптимизации.

Литература

1. Маракова, И.И. Алгоритмы цифровых водяных знаков с точным восстановлением основных покрывающих сообщений // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні: Наук.-техн. зб.— К.: НДЦ “Тезіс” НТУУ “КПІ”, 2004. — Вип. 9. — С. 45 — 53.
2. Computer Graphics: Principles and Practice / J.D. Foley, A. van Dam, S.K. Feiner, J. Hughes. — 2nd ed. — Addison-Wesley, 1995. — 1175 p.
3. Menezes, A.J. Handbook of Applied Cryptography / A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. — 5th ed. — N.Y.: CRC Press, 1996. — 816 p. — p.
4. Fridirich, J. Reliable detection of LSB Steganography in Grayscale and Color Images/ J. Fridirich, M.Goljan, R.Du // Magazine of IEEE Multimedia Special Issue on Security. October — November, 2001. P. 22 — 28.
5. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. — 2-е изд. — М.: Триумф, 2002. — 816 с.
6. Fairhurst, G. MPEG-2 [Электронный ресурс] / G. Fairhurst. — http://www.erg.abdn.ac.uk/future-net/digital-video/mpeg2.html — 01.09.2011.
7. Ell, T.A. Quaternion involutions and anti-involutions / T.A. Ell, S.J. Sangwine // Computers & Mathematics with Applications. — 2007. — Vol. 53 (1). — P. 137 — 143.
8. Просиз, Д. Программирование для Microsoft.NET / Д. Просиз. — М.: Русская редакция, 2003. — 704 с.
9. Witten, I.H. Arithmetic Coding for Data Compression / I.H. Witten, R.M. Neal, J.G. Cleary // Communications of the ACM. — 1987. — June. — Vol. 30(6). — P. 520 — 540.

References

1. Marakova, I.I. Algoritmy tsifrovykh vodyanykh znakov s tochnym vosstanovleniem osnovnykh pokryvayushchikh soobshcheniy [Algorythms of digital watermarks with exact reconstruction of basic covering messages] // Pravove, normatyvne ta metrolohichne zabezpechennia system zakhystu informatsii v Ukraini: Nauk.-tekhn. zb. [Legal, normative and metrologic security of information protection systems in Ukraine: Collected sci.-tech. papers] — Kyiv, 2004. — Issue 9. — PP. 45 — 53.
2. Computer Graphics: Principles and Practice / J.D. Foley, A. van Dam, S.K. Feiner, J. Hughes. — 2nd ed. — Addison-Wesley, 1995. — 1175 p.
3. Menezes, A.J. Handbook of Applied Cryptography / A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. — 5th ed. — N.Y.: CRC Press, 1996. — 816 p.
4. Fridirich, J. Reliable detection of LSB Steganography in Grayscale and Color Images/ J. Fridirich, M.Goljan, R.Du // Magazine of IEEE Multimedia Special Issue on Security. October — November, 2001. PP. 22 — 28.
5. Shnayer, B. Prikladnaya Kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke Si [Applied Cryptography. Protocols, algorythms, original texts in C] / B. Shnayer. — 2-e izd. [2-nd edition] — Moscow, 2002. — 816 p.
6. Fairhurst, G. MPEG-2 [Elektronnyy resurs] / G. Fairhurst. — Available at: http://www.erg.abdn.ac.uk/future-net/digital-video/mpeg2.html — 01.09.2011.
7. Ell, T.A. Quaternion involutions and anti-involutions / T.A. Ell, S.J. Sangwine // Computers & Mathematics with Applications. — 2007. — Vol. 53 (1). — PP. 137 — 143.

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

8. Prosiz, D. Programmirovanie dlya Microsoft.NET [Programming for Microsoft.NET] / D. Prosiz. — Moscow, 2003. — 704 p.
9. Witten, I.H. Arithmetic Coding for Data Compression / I.H. Witten, R.M. Neal, J.G. Cleary // Communications of the ACM. — 1987. — June. — Vol. 30(6). — PP. 520 — 540.

Рецензент д-р техн. наук, проф. Одес. нац. политехн. ун-та Клбозева А.А.

Поступила в редакцию 16 мая 2011 г.