

О. Н. ЛИТВИН, С. И. КУЛИК, А. И. ДРОБОТЯ

СОЗДАНИЕ ГРАФИЧЕСКОГО СТЕГОФАЙЛА НА ИЗОБРАЖЕНИИ КОНТЕЙНЕРЕ З ИСПОЛЬЗОВАНИЕМ ВЕЙВЛЕТОВ

Аннотация – краткая характеристика научной статьи с точки зрения ее назначения, содержания, вида, формы и других особенностей. В тексте аннотации автор указывает результаты, достигнутые в процессе проведенного исследования, их значимость для научной отрасли по сравнению с аналогичными работами, схожими по целевому назначению, тематике и т.д. Аннотация выполняет следующие функции: дает возможность установить основное содержание научной статьи, определить ее релевантность и решить, следует ли обращаться к полному тексту статьи; используется в информационных, в том числе автоматизированных системах для поиска информации. Правильное оформление текста аннотации гарантирует интерес потенциальной аудитории к научной статье и ее хорошее ранжирование основными поисковыми системами (Яндекс, Google). Цель, предмет, тема научной работы отображаются в аннотации только при неоднозначной формулировке заголовка статьи. Методология исследования описывается в случае новизны полученных результатов или проявленного интереса к полному тексту документа со стороны научного сообщества. Итоги проведенной работы описываются максимально четко, информативно. Автор указывает основные теоретические сведения, результаты экспериментов, выявленные закономерности/взаимосвязи в решении проблем, фактическими данными, использованные при написании статьи. Основной акцент – на важные открытия, новые решения, выводы, опровергающие общепризнанные постулаты. Рекомендуется подтверждать полученные выводы собственными оценками, предложениями и т.д. Текст аннотации составляется в научном стиле, без употребления сложных конструкций. Главное требование – лаконичность, четкость, отсутствие вводных слов и общих фраз, не относящихся к сути статьи. В аннотации запрещается использовать дословный, не переработанный текст из статьи, название работы, а также специальные символы, формулы, таблицы, графики и внутритекстовые ссылки.

Ключевые слова: научная статья, аннотация, постановка задачи, методы исследования, цель, содержание, тематика, поисковые системы.

О. М. ЛИТВИН, С. І. КУЛИК, А. І. ДРОБОТЯ

СТВОРЕННЯ ГРАФІЧНОГО СТЕГОФАЙЛУ НА ЗОБРАЖЕННІ-КОНТЕЙНЕРІ З ВИКОРИСТАННЯМ ВЕЙВЛЕТІВ

Анотація – це коротка характеристика наукової статті з точки зору її призначення, змісту, виду, форми та інших особливостей. В тексті анотації автор описує результати, досягнуті в процесі дослідження, їх значущість для наукової галузі у порівнянні з аналогічними роботами, схожими за цільовим призначенням або тематикою. Анотація виконує наступні функції: дає можливість встановити основний зміст наукової статті, визначити її актуальність і вирішити, чи слід звертатися до повного тексту статті; використовується в інформаційних, зокрема автоматизованих системах для пошуку інформації. Ціль, предмет, тема наукової роботи відображаються в анотації лише у випадку неоднозначного формулювання заголовка статті. Методологія дослідження описується лише якщо наукові результати є новими або проявлено інтерес до повного тексту статті з боку наукової спільноти. Підсумки проведеної роботи описуються максимально чітко та інформативно. У анотації автор подає основні теоретичні відомості, результати експериментів, встановлені закономірності/взаємозв'язки у вирішенні проблеми, фактичні дані, що були використані при написанні статті. Основний акцент – на важливі відкриття, нові рішення, висновки, які спростовують загальноприйняті постулати. Рекомендовано підтверджувати отримані результати власними оцінками, пропозиціями тощо. Анотація має бути написана у науковому стилі, без вживання складних конструкцій. Головна вимога – лаконічність, чіткість, відсутність вступних слів та загальних фраз, що не відносяться до суті статті. В анотації забороняється використовувати дослівний, не перероблений текст із статті, назву роботи, а також спеціальні символи, формули, таблиці, графіки та внутрішні посилання.

Ключові слова: наукова стаття, анотація, постановка задачі, методи дослідження, ціль, зміст, тематика.

Обсяг анотацій до наукової статті українською та англійською мовами має становити не менш ніж 1800 знаків, включаючи ключові слова. У запропонованому вище фрагменті 1800 знаків (разом з ключовими словами). Кількість ключових слів (або словосполучень) може бути від 6 до 10. Анотація російською мовою може бути виконана на розсуд автора, але має містити не менш ніж 500 знаків.

О. М. ЛЫТВИН, С. І. КУЛЫК, А. І. ДРОБОТЯ

CREATING A GRAPHIC STEGO FILE ON IMAGE-CONTAINER BY WAVELETS

The article suggests a method of creating graphical steganomessage based on static images, and wavelets. In a specific example (transmission of the confidential picture message), we reviewed the work of the algorithm, cited the results of the program and quoted the analysis results of the experiments. Also we consider some recommendations for further research....

Key words: steganography, steganology, steganomessage, container, wavelet transform....

Введение. Использование изображений, звуковых или видео-файлов в роле контейнеров для передачи стегосообщения открывает достаточно широкие возможности несмотря на большой объем информации...

© О. Н. Литвин, С. И. Кулик, А. И. Дроботя, 2022

**Анализ
последних**

исследований. Незначительная изменчивость первичных образов после «внедрения» стегосообщения, что не провоцирует подозрений относительно присутствия в них внешней информации рассматривалось в работах [1 – 3]...

Учитывая сказанное выше, актуальной задачей ...

Постановка задачи. Изображения имеют значительные преимущества по сравнению с другими носителями в роли контейнеров см. [5]. Задача шифрования состоит в незаметном вкраплении конфиденциальной информации путем ...

Задача дешифровки состоит в ... В этом случае появляется возможность дополнительно усложнить атаки на стегофайл, если ...



Рис. 1 – Эталонное изображение «Lena».

Математическая модель. Так, будем рассматривать подготовительное преобразование эталонного изображения для создания файла-контейнера используя *вейвлет преобразование Добеши четвертого порядка*. Приведем этапы работы алгоритма по шагам ...

...Удобно выбрать размер так, чтобы каждое из чисел M и N были степенью двойки ($M = 2^p$, $N = 2^q$). Тогда изображение...

...На рис. 1 видим эталонное изображение «Lena» (512×512 пикселей). Ему соответствует матрица L ...

Отметим общеизвестный факт, что в 1987 *Ингрид Добеши* сконструировала ортонормированный базис вейвлетов, который остаётся ключевым и сегодня для многих вейвлет-дополнений [7].

Для создания стегофайлов со скрытым сообщением необходимо выполнить следующую последовательность действий.

1. Предварительная обработка изображения заключается в применении двухмерного вейвлет-преобразования Добеши четвертого порядка W к функции $f(x, y)$, которая соответствует матрице L . Получим

$$f'(x, y) = W[f(x, y)], \text{ или } f(x, y) \xrightarrow{W} f'(x, y)$$

В пакете MathCAD вейвлет- преобразования Добеши четвертого порядка представлено функциями ...

В табл. 1 приведены результаты...

Таблица 1 – Результат работы процедуры...

Номер эксперимента	Параметр 1	Параметр 2	Параметр 3	Отклонения, %
1.	12345...	12345...	12345...	1,02...
2.	12345...	12345...	12345...	0,50...
...

3. На третьем этапе выполняем...

Функция d может быть, например, функцией, которая зависит от времени. В результате получим:

$$g(x, y) = f'(x, y) + S(x, y), \quad (1)$$

где $S(x, y) = d[z'(x, y)]$, $z'(x, y) = P[z(x, y)]$, или $z(x, y) \xrightarrow{P} z'(x, y)$.

Для упрощения теоретических преобразований, но, не нарушая общности ...

...при решении сходных проблем методами теории упругости рассматривается *контактная задача* для уравнения

$$\lambda \cdot \partial^2 u / \partial t = K_0 \cdot \operatorname{div} \operatorname{grad} u - G \cdot \operatorname{rot} \operatorname{rot} A,$$

и поле упругих смещений $u(M, t)$ описывается в виде суммы двух слагаемых – потенциального и вихревого:

$$u = \operatorname{grad} \varphi + \operatorname{rot} A, \quad (2)$$

где $\varphi(M, t)$ – скалярный потенциал, $A(M, t)$ – векторный потенциал поля; λ, G – плотность материала и модуль его упругости; K_0 – модуль всестороннего сжатия,

$$K_0 = (2 + 2\mu / (1 - 2\mu)) G,$$

μ – коэффициент Пуассона. ...

Результаты работы программы. На рис.7 для визуального сравнения приведен результат, полученный в

ходе работы программы дешифрования и оригинал секретного графического сообщения, которое вводится вначале программы по созданию графического стегофайла ...

Перспективы дальнейших исследований. Авторы считают перспективными пути исследования, связанные с созданием *стегоконтейнеров*, которые содержат скрытую графическую информация на основе подвижных изображений ...

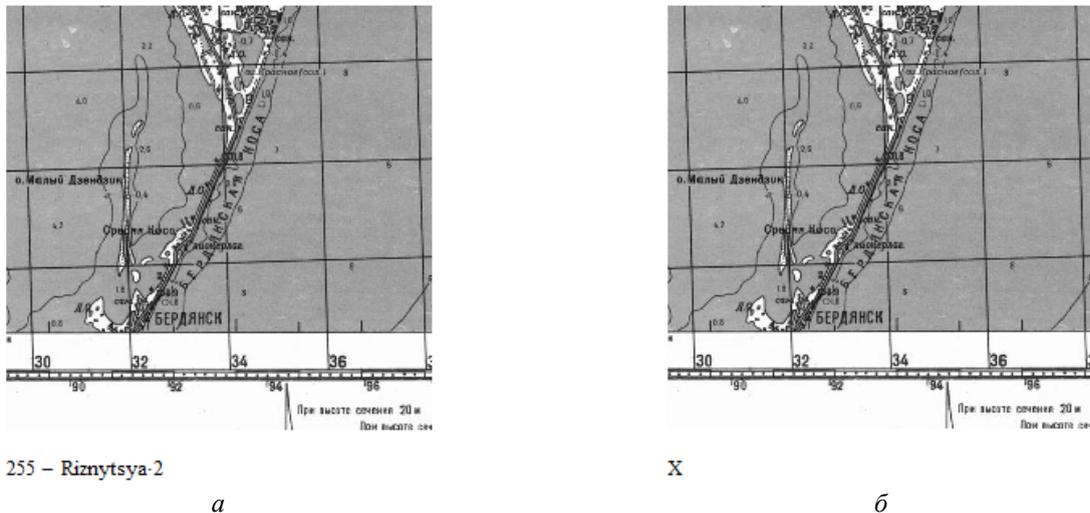


Рис. 7 – Визуальное сравнение работы программы с извлечения скрытого графического сообщения:
а – из полученного стегофайла; б – из оригинала секретного графического сообщения.

Выводы. Таким образом, в данной работе успешно реализован алгоритм создания стегофайла на стандартном изображении-контейнере ...

Следует также заметить, что ...

Список литературы

1. Задірака В. К., Мельникова С. С., Бородавка Н. В. Спектральні алгоритми комп'ютерної стеганографії // Искусственный интеллект. – 2002. – № 3. – С. 532 – 541.
2. Бородавка Н. В., Задірака В. К. Стеганоалгоритмы на базе теоремы о свертке // Кибернетика и системный анализ. – 2004. – №1. – С. 139 – 144.
3. Задірака В. К., Мельникова С. С., Кошкіна Н. В. Ефективні алгоритми побудови стегоконтейнерів з використанням швидкого перетворення Фур'є. Праці Міжнародної конференції «Питання оптимізації обчислень (ПОО XXXII)», присвяченої пам'яті академіка В. С. Михалевича. – Київ : Інститут кібернетики ім. В.М. Глушкова НАН України, 2005. – С. 78 – 79.
4. Яценко В. В. Введение в криптографию. – М. : МЦНМО – ЧеРо, 1999. – 186 с.
5. Шмаев В. В. Современная стеганография. Принципы, основные носители и методы противодействия. – Режим доступа : <http://www.re.mipt.ru/infsec>. – Дата обращения : 05 декабря 2021.
6. Дроботья А. І., Манжула О. В., Кулик С. І. Шифрування зображень з використанням алгоритму RSA та вейвлетів Добеші. Збірник наукових праць Бердянського державного педагогічного університету. Сер. : Педагогічні науки. – № 3. – Бердянськ : БДПУ, 2005. – С. 189 – 197.
7. Добеші І. Десять лекцій по вейвлетам. – М. : Іжевск : НИЦ «Регулярная и хаотическая динамика», 2001. – 464 с.
8. Тевяшев А. Д., Кобылинский К. В., Котелевцев А. В. Интеллектуальная система обнаружения утечек и несанкционированных отборов из конденсатопровода // Проблемы нефтегазовой промышленности. – 2007. – № 5. – С. 392 – 398.

References (transliterated)

1. Zadiraka V. K., Mel'nikova S. S., Borodavka N. V. Spektral'ni algoritmy komp'yuternoyi steganografii [Spectral algorithms of computer steganography]. *Iskusstvennyj intellekt*. 2002, no. 3, pp. 532–541.
2. Borodavka N. V., Zadiraka V. K. Steganoalgoritmy na baze teoremy o svertke [The convolution theorem based steganoalgorithms]. *Kibernetika i sistemnyj analiz*. 2004, no. 1, pp. 139–144.
3. Zadiraka V. K., Mel'nikova S. S., Koshkina N. V. Efektivni algoritmy pobudovy stegokontejneriv z vykorystannyam shvydkogo peretvorenniya Fur'e [Effective algorithms for creating stegocontainers using fast Fourier transform]. *Pratci Mizhnarodnoyi konferenciyi. "Pytannya optimizatsiyi obchyslen' (POO XXXII)", prysvyachenoyi pam'yati akademika V.S. Mykhalevycha* [Proc. of the Int. Conf. «The problems of computation optimization (PCO XXXII)», dedicated to the memory of V. S. Mikhalevich]. Kyiv, Glushkov Institute of Cybernetics of National Academy of Sciences of Ukraine Publ., 2005, pp. 78–79.
4. Jashchenko V. V. *Vvedenie v kriptografiyu* [Introduction to cryptography]. Moscow, MCNMO – CheRo, Russia Publ. 1999. 186 p.
5. Shmaev V. V. *Sovremennaya steganografiya. Printcipy, osnovnyye nositeli i metody protivodeystviya* [Modern steganography. Principles, main media, and methods of counteraction]. Available at <http://www.re.mipt.ru/infsec> (accessed 5 October 2014).
6. Drobotyа A. I., Manzhula O. V., Kulik S. I. Shyfruvannya zobrazhen' z vykorystannyam algoritmu RSA ta veyvletiv Dobeshi [Image encrypting using RSA algorithm and Daubechies wavelets]. *Zbirnyk naukovykh prac' Berdjans'kogo derzhavnogo pedagogichnogo universytetu. Ser.: Pedagogichni nauky* [Collection of works of the Berdiansk State Pedagogical University. Ser.: Pedagogical Science]. Berdyansk, BDPU, 2005, no.3, pp. 189–197.

7. Daubechies Ingrid. *Ten Lectures on Wavelets*. Philadelphia and Pennsylvania, Society for Industrial and Applied Mathematics (SIAM), 1992. 356 p. (Rus. ed.: Daubechies Ingrid. *Desyat' lekcij po veyvletam*. Moscow, Izhevsk, NITC "Regulyarnaya i haoticheskaya dinamika", Russia, 2001, 464 p.).
8. Tevyashev A. D., Kobylinskiy K. V., Kotelevtcev A. V. Intellektual'naya sistema obnaruzheniya utechek i nesankcionirovannykh otborov iz kondensatoprovoda [Intellectual system for detecting leakage and siphoning from condensate pipeline]. *Problemy naftogazovoyi promyslovosti*. 2007, no. 5, pp. 392–398.

Поступила (received) 17.01.2022

Відомості про авторів / Сведения об авторах / Information about authors

Литвин Олег Миколайович – доктор фізико-математичних наук, професор, професор кафедри вищої математики, Українська інженерно-педагогічна академія, м. Харків; тел.: (011) 123-12-12; email: litvin@mail.ua.

Литвин Олег Николаевич – доктор физико-математических наук, профессор, профессор кафедры высшей математики, Украинская инженерно-педагогическая академия, г. Харьков; тел.: (011) 123-12-12; email: litvin@mail.ua.

Litvin Oleg Nikolaevich – Doctor of Physical and Mathematical Sciences, Professor, Professor at the Department of Higher Mathematics, Ukrainian Engineering Pedagogics Academy, Kharkiv; tel.: (011) 123-12-12; email: litvin@mail.ua.

Дроботя Андрій Іванович – кандидат технічних наук, доцент, старший науковий співробітник кафедри машинобудування, Бердянський державний політехнічний університет, м. Бердянськ; тел.: (050) 999-99-99; email: dobrotya@inbox.ru.

Дроботя Андрей Иванович – кандидат технических наук, доцент, старший научный сотрудник кафедры машиностроения, Бердянский государственный политехнический университет, г. Бердянск; тел.: (050) 999-99-99; email: dobrotya @inbox.ru.

Dobrotya Andrey Ivanovich – Candidate of Technical Sciences, Associate Professor, Senior Research Fellow at the Department of Mechanical Engineering, Berdyansk State Pedagogical University, Berdyansk; tel.: (050) 999-99-99; email: dobrotya @inbox.ru.

Кулик Станіслав Іванович – кандидат фізико-математичних наук, доцент, доцент кафедри вищої математики, Національний технічний університет «Харківський політехнічний інститут», м. Харків; тел.: (093) 543-54-43; email: kulik@gmail.com.

Кулик Станислав Иванович – кандидат физико-математических наук, доцент, доцент кафедры высшей математики, Национальный технический университет «Харьковский политехнический институт», г. Харьков; тел.: (093) 543-54-43; email: kulik@gmail.com.

Kulik Stanislav Ivanovich – Candidate of Physical and Mathematical Sciences, Associate Professor, Associate Professor at the Department of Higher Mathematics, National Technical University «Kharkiv Polytechnic Institute», Kharkiv; tel.: (093) 543-54-43; email: kulik@gmail.com.

Відомості про авторів (прізвище, ім'я та по батькові, науковий ступінь, вчене звання, посада і місце роботи, телефон та електронна адреса) мають бути подані повністю українською, російською та англійською мовами.

Шановні автори, звертаємо Вашу увагу, що остання сторінка Вашої статті має бути заповнена не менш як на дві третини.