УДК 681.391

А. Вахаб, Д. М. Романенко
Белорусский государственный технологический университет

МЕТОДЫ ЦИФРОВОЙ СТЕГАНОГРАФИИ НА ОСНОВЕ МОДИФИКАЦИИ ЦВЕТОВЫХ ПАРАМЕТРОВ ИЗОБРАЖЕНИЯ

Рассмотрены особенности реализации методов стеганографии для изображений с целью скрытой передачи данных и охраны прав интеллектуальной собственности. Методы основаны на модификации цветовых параметров пикселей изображения. Сокрытие данных может производиться во всех трех цветовых каналах: красном, зеленом, синем. Служебная информация графических файлов не затрагивается. Разработан и описан новый алгоритм стеганографического осаждения данных в растровые изображения, проанализированы его достоинства и недостатки, определены направления дальнейших исследований. Особенностью разработанного метода является то, что в отличие от классического LSB, осаждение данных осуществляется в десятичной форме, что позволяет добиться большей эффективности с точки зрения максимально возможного количества скрытых в изображении данных. Разработано программное средство, позволяющее осаждать/извлекать секретную авторскую информацию в графические файлы наиболее распространенных форматов (jpeg, bmp, png). Реализованные стеганографические методы предусматривают модификацию значений красного, зеленого и синего каналов любого пикселя изображения-контейнера. Выбор пикселей, подлежащих модификации, осуществляется в соответствии с секретным ключом пользователя, а также с учетом обеспечения высокой стегостойкости. Описаны функциональные возможности разработанного программного средства.

Ключевые слова: стеганография, изображение, осаждение, алгоритм, модель, цвет, авторское право.

A. Wahab, D. M. Romanenko
Belarusian State Technological University

METHODS OF DIGITAL STEGANOGRAPHY BASED ON THE MODIFICATION OF COLOR IMAGE PARAMETERS

Features of the steganography methods implementation for images for the purpose of hidden data transmission and protection of intellectual property rights are considered. The methods are based on the modification of the image pixels color parameters. Data concealment can be performed in all three color channels: red, green, blue. The service information of graphic files is not affected. A new algorithm for steganographic data precipitation in images is developed and described, its advantages and disadvantages are analyzed, directions for further research are determined. The main feature of the developed method, compares the classical LSB method, is that the data is deposited in decimal form, which allows to achieve greater efficiency in point of view the maximum possible hidden data amount in the image. A software tool has been developed that allows to precipitate/extract secret copyright information in graphic files of the most common formats (jpeg, bmp, png). The implemented steganographic methods provide the values modification of the red, green and blue channels of any pixel of the container image. The selection of the pixels to be modified is carried out in accordance with the user's secret key, and also with considering the maintenance of high stag resistance. The functional capabilities of the developed software are described.

Key words: steganography, image, precipitation, algorithm, model, color, copyright.

Введение. Проблема защиты авторских прав существенно обострилась в связи с вступлением человечества в цифровую эру, где вся информация хранится и передается в цифровом виде. Рассылка документов (текстовых, графических и т. д.) по сети предполагает, что их может получить большое число адресатов. Это также дает возможность недобросовестным пользователям адаптировать или перерабатывать информацию с целью извлечения коммерческой выгоды. Угроза информационного пиратства стала реальностью.

Авторское право распространяется на результаты науки, произведения литературы и искусства, находящиеся в какой-либо объективной форме (в том числе и цифровой):

- письменной (рукопись, машинопись, нотная запись);
- электронной (компьютерная программа, электронная база данных, текст); звуко- или видеозаписи (магнитная, оптическая, электронная);
- изображения (картина, рисунок, кино-, теле-, видео-, фотокадр);
- объемно-пространственной (скульптура, макет, сооружение).

Одним из направлений решения указанной проблемы в контексте защиты авторства на объекты в цифровом виде является применение

современных стеганографических методов. Стеганография – это искусство передачи скрытого сообщения [1]. Компьютерные технологии придали новый импульс развитию и совершенствованию стеганографии, появилось новое направление в области защиты информации – цифровая стеганография. Причем, в отличие от криптографии, данные методы скрывают сам факт передачи информации [2].

Цифровая стеганография – направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. Но, как правило, данные объекты являются мультимедиа объектами (изображения, видео, аудио, текстуры 3D-объектов) и внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека, не приводит к заметным изменениям этих объектов. Кроме того, в оцифрованных объектах, изначально имеющих аналоговую природу, всегда присутствует шум квантования, а при воспроизведении этих объектов появляется дополнительный аналоговый шум и нелинейные искажения аппаратуры, все это способствует большей незаметности сокрытой информации.

Все алгоритмы встраивания скрытой информации в мультимедиа объекты (в том числе и изображения) можно разделить на несколько подгрупп:

1. Работающие непосредственно с самим цифровым сигналом, например, изображением. Классическим примером является метод LSB (Least Significant Bit, метод наименьшего значащего бита) [3].

2. «Впаивание» скрытой информации. В данном случае происходит наложение скрываемого изображения (звука, иногда текста) поверх оригинала. Часто используется для встраивания цифровых водяных знаков (ЦВЗ).

3. Использование особенностей форматов файлов. Сюда можно отнести запись информации в метаданные или в различные другие не используемые зарезервированные поля файла.

Далее в данной статье будут рассматриваться вопросы применения именно методов цифровой стеганографии, работающих непосредственно с отдельными элементами (пикселями) растровых изображений, для осаждения информации, с помощью которой автор может защитить права интеллектуальной собственности.

Основная часть. Цифровая стеганография базируется на двух принципах. Первый заключается в том, что файлы, содержащие изображение в цифровом виде, могут быть до некоторой степени видоизменены без потери функциональности, в отличие от других типов данных, требующих абсолютной точности.

Второй принцип состоит в неспособности органов чувств человека различить незначительные изменения в цвете изображения, что особенно легко использовать применительно к объекту, несущему избыточную информацию, будь то 8-битное или, еще лучше, 48-битное изображение.

Некоторые современные методы стеганографии основываются именно на данных положениях. В цифровой стеганографии таким методом является, например, метод LSB.

Как известно, в графических форматах (например, BMP, JPEG) изображение хранится как матрица значений оттенков цвета для каждой точки хранимого изображения. Если каждая из компонент пространства RGB (их еще называют каналами цвета) хранится в одном байте, она может принимать значения от 0 до 255 включительно, что соответствует 24-битной глубине цвета (8 бит на канал). Особенность зрения человека заключается в том, что оно слабо различает незначительные колебания цвета. Для 24-битного цвета изменение в каждом из трех каналов одного наименее значимого бита (т. е. крайнего правого) приводит к изменению не более чем на 3–4% интенсивности (цвета) данной точки, что позволяет изменять их незаметно для глаза по своему усмотрению.

Далее рассмотрим более подробно непосредственно метод LSB. Если отбросить в расчетах обычно незначительную относительно размера изображения служебную информацию в начале файла, то получим возможность скрытно передать сообщение размером в 1/8 размера контейнера (равномерно распределенную по последним битам в каждом байте матрицы цветов пикселей) или же размером в 1/4 контейнера (соответственно при использовании двух последних бит в байтах).

Принцип работы стеганографического метода LSB заключается в следующем. Пусть имеется 24-битное изображение в градациях серого. Пиксель кодируется 3 байтами, и в них расположены значения каналов RGB. При изменении наименее значимого бита будет изменяться значение байта на единицу. Такие градации мало заметны для человека, они могут вообще не отобразиться при использовании низкокачественных устройств вывода. Приведенный ниже пример показывает, как сообщение может быть скрыто в первых 8 байтах, относящихся к трем пикселям 24-битного изображения (в рассматриваемом примере подчеркнуты только те три бита, которые были фактически изменены).

Исходные значения пикселей:

(00100111 11101001 11001000),
(00100111 11001000 11101001),
(11001000 00100111 11101001).

Осаждаемый текст: 01000001.
Результат осаждения:

(00100110 11101001 11001000),
(00100110 11001000 11101000),
(11001000 00100111 11101001).

Также известна небольшая модификация представленной методики осаждения стеганографической информации, позволяющая использовать для встраивания сообщения два или более младших бит на байт. Это увеличивает объем скрытой информации в объекте-контейнере, но скрытность сильно снижается, что облегчает обнаружение результатов осаждения информации.

В целом основной проблемой метода LSB является именно слабая стегостойкость. Так, например, существует интеллектуальное программное обеспечение, которое для выявления стеганографии проверяет области, состоящие из одного сплошного цвета. Для повышения скрытности следует избегать записи изменений в такие пиксели.

В рамках представленной работы предлагается модификация техники осаждения секретной (авторской) информации для метода графической стеганографии LSB. Суть модификации заключается в следующем. Авторский текст в соответствии с кодировкой ASCII преобразуется в числовой вид, т. е. символы заменяются на соответствующие числовые коды. Так при конвертации секретного текста Alaa получим: A (ASCII) = 65; L (ASCII) = 76; A (ASCII) = 65; A (ASCII) = 65. На следующем шаге с помощью секретного ключа определяется место осаждения информации (в рассматриваемом далее примере информация будет осаждаться относительно центра изображения, как представлено на рис. 1).

Для осаждения четырех тестовых символов в рассматриваемом случае потребуется четыре пикселя изображения. Пусть исходное изображение (стегоконтейнер) имеет размеры 281×179 пикселей. Тогда получится, что изменять в процессе осаждения будем цветовые составляющие, например, следующих точек с координатами (140, 58), (140, 87), (140, 88), (140, 89) (рис. 2).

Замена значений трех составляющих цвета (red, green, blue) будет осуществляться не в двоичном, как в классическом LSB методе, а в десятичном виде. Замене подлежат наименее значимые (правые) цифры значений соответствующего цветового канала (рис. 3).

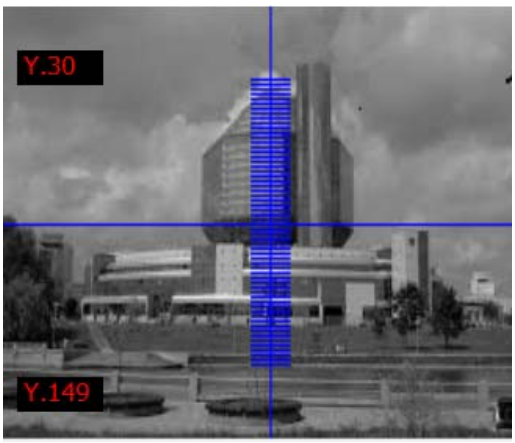

Рис. 1. Пример выбора места (пикселей) для осаждения авторской информации

R	G	B	X	Y	№	TEXT	DECIMAL
97	88	86	140	86	1	A	65
96	93	87	140	87	2	L	76
97	92	85	140	88	3	A	65
95	84	76	140	89	4	A	65

Рис. 2. Пример выбранных для осаждения пикселей

R	G	B	X	Y	№	TEXT	DECIMAL
9x	88	8x	140	86	1	A	65
9x	93	8x	140	87	2	L	76
9x	92	8x	140	88	3	A	65
9x	84	7x	140	89	4	A	65

Рис. 3. Пример цифр в выбранных пикселях, подлежащих замене при осаждении информации

Отметим, что если использовать символы кириллицы (ASCII коды >127), то потребуется задействовать и зеленую составляющую пикселя, либо увеличивать количество задействованных в процессе осаждения пикселей. При замене в красную составляющую будет записываться первая цифра двоичного кода символа, а в синюю составляющую – вторая цифра двоичного кода символа. Таким образом получим следующие значения цветовых составляющих пикселей, как показано на рис. 4.

Пиксели исходного изображения

R	G	B	X	Y	№	TEXT	DECIMAL
97	88	86	140	86	1	A	65
96	93	87	140	87	2	L	76
97	92	85	140	88	3	A	65
95	84	76	140	89	4	A	65

Пиксели изображения с осажденной информацией

R	G	B	X	Y	№	TEXT	DECIMAL
96	88	85	140	86	1	A	65
97	93	86	140	87	2	L	76
96	92	85	140	88	3	A	65
96	84	75	140	89	4	A	65

Рис. 4. Результат замены значений в выбранных пикселях при осаждении информации

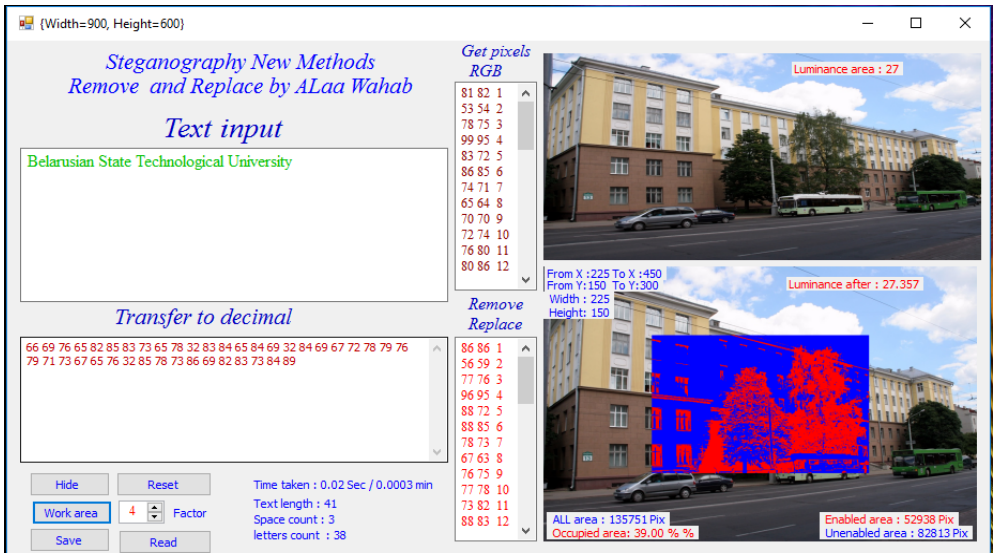

Рис. 5. Интерфейс главного окна программного средства

В целом можно заметить, что такой механизм осаждения информации будет изменять не один младший бит, как бы это было в классическом методе LSB, а целую группу бит, причем необязательно начиная с младшего разряда. Но при этом все равно будет достигаться незначительное изменение цвета пикселя. Так, например, если бы значение в красном канале для какого-то пикселя было изменено с 96 (в двоичной системе 1100000) на 95 (в двоичной системе 1011110), то это было бы эквивалентно изменению 5 бит. Это говорит о том, что применение представленного механизма осаждения информации позволит улучшить такую характеристику, как максимально возможное количество осаждаемой информации в контейнере (изображении).

Для реализации предлагаемого метода изменения цветовых значений изображения и классического LSB, а также с целью их дальнейшего изучения и сравнения было создано специальное программное средство, главное окно которого представлено на рис. 5.

Отметим, что сохранять изображения при использовании данного программного средства можно практически в любом графическом формате, но при этом не предусматривается использование jpeg со сжатием, так как в последнем применяются операции «выкалывания» и «прореживания», приводящие к замене группы значений на усредненное, а поэтому осажденная авторская информация при сохранении файла может быть повреждена. При использовании сжатого формата jpeg осаждать информацию надо в матрицу коэффициентов, получаемую при ортогональном DCT преобразовании изображения.

Проанализируем эффективность использования разработанной модификации стеганографического метода LSB. Как было показано ранее на примере с осаждением текста Alaa, в предложенном методе требуется изменить цветовые составляющие лишь одного пикселя для каждой буквы алфавита, а если бы использовался классическим алгоритм LSB, то задействованы были бы как минимум по 3 пикселя на один символ. Соответственно получим следующие графики зависимостей количества модифицируемых пикселей от количества осаждаемой информации (в байтах) (рис. 6).

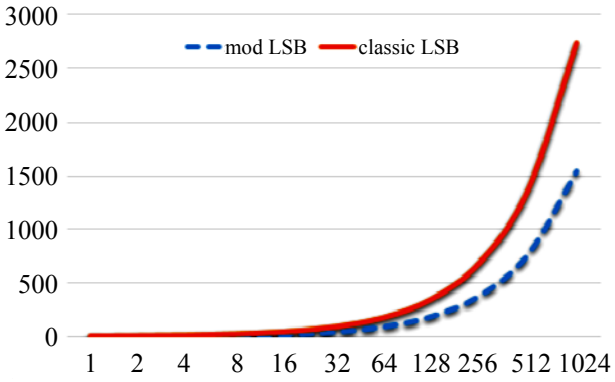

Рис. 6. Зависимости количества модифицируемых пикселей от количества осаждаемой информации

Как видно из рис. 6, модифицированный LSB метод превосходит классический с точки зрения емкости осаждаемой информации примерно на 40–50%. Однако очевидно, что такая высокая информационная емкость стегоконтейнера имеет и обратную сторону – потенциально возможную меньшую стегостойкость. В данном случае важнейшую роль в процессе осаждения будет играть непосредственно алгоритм выбора пикселей, в которые будет осаж-

даться информация, который еще предстоит оптимизировать с точки зрения критерия минимальности цветовых отклонений пикселей исходного изображения-контейнера и изображения с авторской информацией, что является важнейшим направлением для дальнейшего исследования. В качестве целевой функции предполагается использовать геометрическую разность цветов при представлении их в трехмерной системе координат.

Заключение. В качестве метода для защиты и доказательства прав собственности на растровые изображения предложена модификация стеганографического метода LSB, основанная на специальном изменении цветовых значений пикселей. Подробно описан метод стегонаграфического осаждения данных, проанализированы некоторые его свойства (например, максимальная емкость контейнера). Разработано программное средство, которое позволяет вносить в изображение авторскую текстовую информацию, а также ее извлекать.

Предложенная модификация метода характеризуются большей эффективностью, поскольку позволяет по сравнению с классическим LSB методом осаждать больше (на 40–50%) информации в пересчете на один пиксель.

В качестве дальнейшего направления исследований определено изучение оптимизация алгоритма выбора пикселей по цветогеометрическим параметрам, в которые предполагается осаждать информацию, подтверждающую авторство.

Литература

1. Bennett K. Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text. Purdue Univ., CERIAS Tech. Rep., 2004.

2. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. Киев: МК-Пресс, 2006. 288 с.

3. Urbanovich N., Plaskovitsky V. The use of steganographic techniques for protection of intellectual property rights. New Electrical and Electronic Technologies and their Industrial Implementation. 2011, P. 147–148.

References

1. Bennett K. Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text. Purdue Univ., CERIAS Tech. Rep., 2004.

2. Konakhovich G. F., Puzyrenko A. Yu. *Komp'yuternaya steganografiya. Teoriya i praktika* [Computer steganography. Theory and practice]. Kiev, MK-Press Publ., 2006. 288 p.

3. Urbanovich, N., Plaskovitsky V. The use of steganographic techniques for protection of intellectual property rights. *New Electrical and Electronic Technologies and their Industrial Implementation*, 2011, pp. 147–148.

Информация об авторах

Романенко Дмитрий Михайлович – кандидат технических наук, заведующий кафедрой информатики и веб-дизайна. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова, 13а, Республика Беларусь). E-mail: rdm@belstu.by

Алаа Вахаб – аспирант. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова, 13а, Республика Беларусь). E-mail: alaasouth@gmail.com

Information about the authors

Romanenko Dmitri Mikhailovich − PhD (engineering), Head of the Department of Informatics and Web-design. Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: rdm@belstu.by

Alaa Wahab − PhD student. Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: alaasouth@ gmail.com

Поступила 28.11.2017