УДК 004.056.5

А.А. Менщиков, А.Н. Шниперов

Метод скрытого встраивания информации в векторные изображения

Рассматривается новый метод стеганографического встраивания информации в цифровые векторные изображения, содержащие в себе константы, представленные числами с десятичными дробями высокой точности. Приводится оценка вносимого данным методом дополнительного шума, уровень которого зависит от параметров встраивания скрытой информации. Данный метод может использоваться для скрытой передачи информации с высокой степенью надежности и стойкости к обнаружению.

Ключевые слова: стеганография, скрытая передача данных, защита конфиденциальной информации, цифровые водяные знаки.

Информация, передаваемая по открытым каналам связи, подвергается угрозам раскрытия, изменения и уничтожения [1]. Одним из возможных решений проблемы угрозы раскрытия является использование стеганографических методов [2]. Существующие стеганографические алгоритмы лишь частично удовлетворяют требованиям, которые предъявляются к системам скрытой передачи данных. Актуальной является задача поиска новых алгоритмов и каналов стеганографического встраивания информации. В процессе изучения данной проблемы, была выявлена резко возросшая популярность векторных форматов изображений, которые сейчас активно внедряются на веб-ресурсах и могут представлять собой достаточно эффективный стеганографический канал [3].

В данной работе приводится новый метод встраивания информации в векторные изображения, являющийся развитием стеганографического метода Least significant bit (LSB) [4]. На основе данного метода и сопутствующих алгоритмов был разработан программный продукт, который поддерживает популярный формат векторной графики – Scalable Vector Graphics (SVG). Проведено тестирование данного метода на широком наборе SVG-изображений, а также была дана оценка устойчивости метода к пассивному статистическому, а также визуальному стеганоанализам.

Обзор стеганографических методов. В настоящее время методы компьютерной стеганографии развиваются по двум основным направлениям [5]:

1. Методы, основанные на использовании специальных свойств компьютерных форматов.
2. Методы, основанные на избыточности аудио- и визуальной информации.

Одним из самых распространенных подходов, основанных на использовании избыточности, является метод LSB, суть которого заключается в использовании наименее значимых бит информации для передачи скрытого сообщения [6]. Достоинствами данного метода являются простота реализации, скорость работы и относительно большая вместимость. К недостаткам можно отнести возможность статистического стеганоанализа на основе выявления различных корреляций между младшими битами изображения [7]. Однако, существуют модификации, которые позволяют обойти данное ограничение и использовать такие механизмы встраивания, которые полностью нивелируют явные статистические закономерности.

Также широко используются методы трансформации вложений, например путём модификации матриц квантования коэффициентов дискретного косинусного преобразования или путём маскирования восприятия, основанного на модификации элементов изображения, к которым человеческий глаз наименее восприимчив [8].

Предлагаемый алгоритм относится к классу LSB-методов и заключается в использовании наименее значащих разрядов констант в векторных форматах данных. Рассмотрим разработанный стеганографический метод на примере формата векторных изображений SVG, однако справедливо заметим, что метод в целом применим для многих векторных форматов данных.

Существует несколько подходов к сокрытию информации и созданию цифровых водяных знаков (ЦВЗ) в векторных форматах данных. Условно их можно разделить на два класса: основанные на геометрических преобразованиях и на XML-формате [9–11]. В работе [9] рассматриваются общие

подходы к внедрению ЦВЗ в XML-документы. В работе [11] описывается механизм встраивания ЦВЗ в SVG-изображения, который основан на модификации дробных частей констант геометрических фигур. Данный метод показывает хорошие результаты для визуальных атак на стеганографическую систему, но является неустойчивым против экспертных атак посредством анализа кода т.к. необоснованно увеличивает длину дробных частей констант. В работе [12] предлагается общая схема защиты авторских прав SVG-изображений на основе встраивания ЦВЗ в различные геометрические фигуры. Доказывается устойчивость схемы к некоторым геометрическим преобразованиям, а также рассчитываются допустимые объемы встраивания с расчетом на различные статистические атаки, основанные на байесовской теории принятия решений и тесте отношения правдоподобия. В работе [10] рассматривается механизм защиты авторских прав на основе внедрения обратимой ЦВЗ в двумерные векторные изображения. Также приводятся предложения к использованию данной схемы для передачи секретных данных. В работе [13] рассматривается алгоритм встраивания ЦВЗ, основанный на диаграммах Вороного и триангуляции с ограничениями.

С учетом всей проанализированной литературы был разработан новый метод встраивания секретных данных в векторные изображения, а также сопутствующие алгоритмы на основе использования малозначащих разрядов дробных частей параметров геометрических фигур.

Схема передачи сообщения. Для встраивания выбираются константы, описывающие параметры и координаты геометрических фигур. Заметим, что константы выбираются в зависимости от того, какой формат векторной графики используется. Для формата SVG допустимо использовать параметры ломаных, многоугольников, эллипсов и кривых Безье [12, 13]. Для рассматриваемого метода нет ограничения на использование определенных изображений, но приоритет будет отдан тем изображениям, константы которых имеют максимальную длину дробного представления, а также тем, которые включают много различных геометрических элементов. Наилучшие показатели для этих требований достигаются при использовании абстрактных изображений либо изображений, полученных из растровых путём конвертации.

Алгоритмы встраивания и извлечения. Рассмотрим алгоритмическую реализацию предлагаемого стеганографического метода.

Для начала необходимо определить количество n младших разрядов дробной части константы координаты, которые будут использоваться. Также необходимо выбрать минимальную длину дробной части для тех координат, в которые будет осуществляться встраивание.

Алгоритм встраивания:

Шаг 1. Положим, что для записи битов встраиваемого сообщения будет использоваться два младших разряда дробной части константы координаты ($n = 2$). Будем выбирать только те координаты, длина дробной части которых не меньше трех.

Шаг 2. Выберем необходимые данные для встраивания – M, представленные в бинарном виде.

Шаг 3. С помощью системного генератора псевдослучайных последовательностей (ГПСЧ), например /dev/random в ОС Linux, сгенерируем секретный ключ K_S и сеансовый ключ K_C. В предлагаемой реализации $|K_S|=128$ бит, $|K_C|=10$ десятичных знаков.

Шаг 4. Аналогичным способом сгенерируем модуль размером 1024 бита, используемый в модульной арифметике ГПСЧ, основанного на алгоритме Blum-Blum-Shub [14, 15], который будет использован на дальнейших шагах, обозначим его как G^{BBS}.

Шаг 5. Сгенерируем псевдослучайную последовательность $X_M = G^{BBS}(K_S \cdot K_C)$, где $K_S \cdot K_C$ – вектор инициализации ГПСЧ, операция «·» – бинарная конкатенация K_S и K_C, а длина псевдослучайной последовательности $|X_M| = |M|$.

Шаг 6. Осуществим предварительное зашифровывание скрытого сообщения M путём гаммирования: $M^{encrypt} = X_M \oplus \mathrm{M}$, где $\oplus$ – операция поразрядного сложения по модулю 2. Данная операция позволит существенно нивелировать статистические закономерности скрытого сообщения.

Шаг 7. Осуществим разбиение $M^{encrypt}$ на вариативное количество N-блоков, т.е. $M_N^{encrypt} = \{m_1^{encrypt}, m_2^{encrypt}, \ldots, m_N^{encrypt}\}$, где длины $\left|m_1^{encrypt}\right| = \left|m_2^{encrypt}\right| = \left|m_{N-1}^{encrypt}\right|$, но при этом полагая, что в общем случае $\left|m_i^{encrypt}\right| \neq \left|m_N^{encrypt}\right|$, где $i \neq N$. Заметим, что в нашем примере $N = 2$, т.к. используется 2 младших разряда дроби константы (см. шаг 1).

Шаг 8. Каждый из блоков $m_i^{encrypt}$ для $i \neq N$ переводится в десятичную систему счисления. Последний блок $m_N^{encrypt}$ переводится в девятеричную модифицированную систему счисления (значащие разряды $[1,9]$, вместо $[0,8]$), чтобы впоследствии избежать использования нулей в младшем разряде десятичной дроби.

Шаг 9. Сгенерируем псевдослучайную последовательность $L^{binary} = G^{BBS}\left[hash(K_s \cdot K_c)\right]$ длиной $\left|L^{binary}\right| = N \times 20$ бит, которая будет использоваться для зашифровывания длин блоков $\left|m_i^{encrypt}\right|$, где $hash(K_s \cdot K_c)$ – вектор инициализации G^{BBS}, *hash* – функция хеширования, операция «·» – бинарная конкатенация K_s и K_c. В качестве функции хеширования был выбран алгоритм *md*5 [16], однако может использоваться и иной.

Шаг 10. Разобьём последовательность L^{binary} на битовые подблоки L_i^{binary} таким образом, чтобы при преобразовании их в десятичный вид они были одинаковой длины, равной 5. Например, битовый подблок $L_i^{binary} = \{01000001001100100101\}_{bin}$ в десятичном представлении будет $L_i^{dec} = \{41325\}_{dec}$. Далее осуществим преобразование всех подблоков L_i^{binary} в десятичное представление, каждый из которых обозначим как L_i^{dec}, таким образом, $L_i^{dec} = \left\{L_1^{dec}, L_2^{dec}, \ldots, L_N^{dec}\right\}$.

Шаг 11. Осуществим зашифровывание всех длин блоков $m_i^{encrypt}$ путем познакового сложения их десятичных чисел по модулю 10 с соответствующими знаками L_i^{dec}, т.е. $Len_i^{encrypt} = \left(L_i^{dec} + \left|m_i^{encrypt}\right|\right) \bmod 10$, где $i = [1,N]$, операция «+» – познаковое сложение. Заметим, что в настоящей реализации алгоритма $\left|Len_i^{encrypt}\right| = \left|L_i^{dec}\right| =$ 5 разрядов.

Шаг 12. Осуществим конкатенацию всех зашифрованных длин зашифрованных блоков, т.е. $Len_{encrypt} = Len_1^{encrypt} \cdot Len_2^{encrypt} \cdot \ldots \cdot Len_N^{encrypt}$, где $Len_{encrypt}$ – большое число в десятичном представлении, $\left|Len_{encrypt}\right| = N * 5$ десятичных знаков.

Шаг 13. К предпоследнему блоку $m_{N-1}^{encrypt}$ добавим сеансовый ключ K_c и $Len_{encrypt}$, т.е. $m_{N-1}^{encrypt} = K_c \cdot Len_{encrypt} \cdot m_{N-1}^{encrypt}$, где операция «·» – конкатенация K_c, $Len_{encrypt}$, $m_{N-1}^{encrypt}$.

Шаг 14. Осуществим встраивание блоков $m_i^{encrypt}$ в контейнер. Для этого из каждого блока последовательно берется по одному десятичному разряду и встраивается на соответствующее место в дробные части констант координат SVG. Например, для *N*=2 и блоков $m_1^{encrypt} = 13570$, $m_2^{encrypt} = 2468$ в первой координате SVG два младших разряда десятичной части будут заменены на 12, во второй координате – 34, в третьей – 56, в четвертой – 78, в пятой – 0*X*, где *X* – это та цифра, которая находилась на данном месте. Она остается неизменной, т.к. блок $m_2^{encrypt}$ исчерпан.

Алгоритм извлечения:

Шаг 1. Извлечем из SVG документа все дробные части констант координат.

Шаг 2. Составляем из них *N*-блоков путем извлечения соответствующих младших разрядов (обратно операции встраивания), т.е. получаем $E = \{E_1, E_2, \ldots, E_N\}$. При этом заметим, что в общем случае каждый блок $E_i = m_i^{encrypt} \cdot RandData$, где операция «·» – конкатенация соответствующего зашифрованного блока скрытого сообщения и некоторых данных *RandData*, которые для стеганосистемы не являются значимыми и которые надо отбросить, но для этого необходимо понимать размер скрытого сообщения.

Шаг 3. Зная, что в предпоследнем блоке $E_{N-1} = K_c \cdot Len_{encrypt} \cdot m_{N-1}^{encrypt} \cdot RandData$, а также длину сеансового ключа $|K_c|$=10 знаков и длину $|Len_{encrypt}| = N \cdot 5$ знаков, осуществляем их извлечение.

Шаг 4. Сгенерируем псевдослучайную последовательность $L^{binary} = G^{BBS}\left[hash\left(K_s \cdot K_c\right)\right]$ длиной $\left|L^{binary}\right| = N * 20$ бит, которая будет использоваться для расшифровывания длин блоков $\left|m_i^{encrypt}\right|$ и аналогично шагу 10 алгоритма встраивания приведём её к десятичному представлению.

Шаг 5. Осуществим расшифровывание всех длин блоков $m_i^{encrypt}$ путем познакового вычитания их десятичных чисел по модулю 10 с соответствующими разрядами L_i^{dec}, т.е. $Len_i^{plain} = \left(Len_i^{encrypt} - L_i^{dec}\right) mod\, 10$, где $i = [1, N]$, операция «–» – познаковое вычитание. На выходе получим длину каждого зашифрованного блока, используя которую, можно отбросить весь объём незначащих для стеганосистемы данных *RandData.*

Шаг 6. Приведём каждый зашифрованный блок $m_i^{encrypt}$ к двоичной системе счисления.

Шаг 7. Аналогично зашифровыванию, но с применением обратных преобразований, расшифровываем блоки и получаем $M_N^{plain} = \left\{m_1^{plain}, m_2^{plain}, \ldots, m_N^{plain}\right\}$.

Оценка стойкости разработанного алгоритма. В реальных условиях наиболее распространенным видом атаки пассивного нарушителя является атака по стеганоконтейнеру, т.к. исходный контейнер ему неизвестен. В данных условиях обнаружение скрытого сообщения возможно на основе выявления изменений закономерностей, присущих естественным контейнерам [2]. Был произведен анализ возможностей визуальной и статистической атак, а также проведена оценка стойкости стеганографических сообщений, сформированных с помощью разработанного программного продукта, к данным атакам.

Визуальная атака на стеганосистему. Рассмотрим принцип построения визуальной атаки, позволяющей выявить факт наличия скрываемого сообщения, вложенного в изображение-контейнер [17]. Зависимость между младшими элементами констант отличается от зависимостей, рассчитанных для растровых изображений, что не позволяет применять существующий стеганографический аппарат. Введем следующую качественную оценку для скрытности встраивания:

Отлично – изображения визуально неотличимы даже при пятикратном увеличении.

Хорошо – изображения визуально неотличимы при просмотре в оригинальном масштабе, при пятикратном увеличении проявляются незначительные отличия.

Удовлетворительно – видны отличия между изображениями в оригинальном масштабе, но они не влияют на комфортное восприятие изображения.

Плохо – отличия между изображениями видны и портят изображение.

Применим данную методику, варьируя типы изображений, размеры, объем данных для встраивания и число разрядов, используемых для встраивания. *Разрядностью* назовем отношение числа разрядов для встраивания к минимальной длине дробной части используемых чисел из контейнера, умноженное на 100%.

В результате выявлено, что эмпирические показатели скрытности встраивания слабо зависят от размеров изображения и объема данных для встраивания. Художественно-абстрактные изображения получают лучшие оценки и позволяют встроить гораздо больший объем информации. Скрытность встраивания отличная или хорошая при разрядности менее 50%, хорошая или удовлетворительная при разрядности в 50–65%, удовлетворительная при разрядности в 65–80% и плохая при разрядности более чем 80%.

Различие между пустым контейнером и заполненным визуально не проявляется при использовании разрядности менее 66%. В зависимости от контейнера данный показатель можно варьировать (особенно для изображений с большим числом знаков).

Статистическая атака на стеганосистему. Более перспективным является подход, представляющий собой внедрение в файл скрываемой информации и изучение нарушения статистических закономерностей естественных контейнеров [19]. Для изучения внесения дополнительных искажений (шума) в изображение при встраивании сообщения в контейнер используют взятые из радиотехники метрики искажений. В первую очередь мы использовали некоторые разностные показатели искажения.

Отношение сигнал/шум (метрика Signal to Noise Ratio, SNR) [18].

$$\mathrm{SNR} = 10 \times \lg \frac{\Sigma (C_x)^2}{\Sigma (C_x - S_x)^2} \text{ дБ},$$

где C_x – дробная часть константы исходного контейнера, S_x – соответствующего заполненного.

Нормированная средняя абсолютная разница (Normalized Average absolute Difference, NAD) указывает степень отличия между пустым и заполненным контейнером. Рассчитывается следующим образом [20]:

$$\mathrm{NAD} = \frac{\Sigma |C_x - S_x|}{|C_x|}.$$

Качество изображения (Image Fidelity, IF) является одной из основных оценочных характеристик для стеганоалгоритмов, работающих с изображениями, потому что визуальная атака основана на способности зрительной системы человека анализировать визуальные образы и обнаруживать существенные расхождения в изображениях. Рассчитывается следующим образом [20]:

$$\mathrm{IF} = 1 - \frac{\Sigma (C_x - S_x)^2}{{C_x}^2}.$$

Структурное содержание (Structural Content, SC) используется для оценки искажений, которые вносит стеганосистема в изображение. Рассчитывается следующим образом:

$$\mathrm{SC} = \frac{\Sigma {C_x}^2}{\Sigma {S_x}^2}.$$

Для проведения экспериментов был взят тестовый набор черно-белых и цветных изображений разного размера и начертания.

Результаты исследований. Для понимания объема искажений, которые вносятся в изображение, необходимо сравнить метрики для разных объемов встраиваемых данных. Также необходимо произвести проверку, как влияет увеличение разрядности на уменьшение надежности сокрытия. Исследование проведено на наборе из нескольких векторных изображений, результаты усреднены. В качестве типовых размеров данных для встраивания были взяты случайные 32, 64, 128, 256, 512, 1024, 2048 байтовые сообщения. Изображения-контейнеры в сжатом виде имеют размеры от 21 до 128 Кб. При этом изображения подобраны таким образом, что объем данных для встраивания колеблется от 5 до 34%.

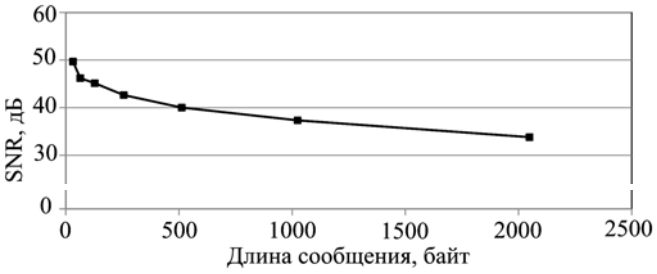

Рис. 1. Зависимость метрики SNR от длины встраемого сообщения

Введем следующую качественную оценку для скрытности встраивания: отлично – SNR >= 35 дБ; хорошо – SNR от 27 до 35 дБ; удовлетворительно – от 29 до 27 дБ; плохо – SNR <= 19 дБ. Метрика SNR для разрядности в 66% приведена на рис. 1.

Очевидно, что увеличение объема данных для встраивания в контейнер негативно влияет на статистику отображения, но данное влияние не снижает метрику ниже 33 дБ, что позволяет рассчитывать на отличную скрытность сообщений объемом от 5 до 34% от размера контейнера при разрядности менее 50% и хорошую при разрядности менее 66%.

В таблице приведены остальные метрики для того же набора сообщений и изображений.

Зависимость метрик SNR, NAD, IF, SC от длины встраемого сообщения

	SNR, дБ	NAD	IF	SC
32	49,67346	0,00032	0,99998	1,00003
64	46,19967	0,00057	0,99996	1,00021
128	45,14276	0,00098	0,99993	1,00022
256	42,64008	0,00202	0,99984	1,00019
512	40,02019	0,00391	0,99970	1,00072
1024	37,33800	0,00772	0,99940	1,00094
2048	33,80285	0,01533	0,99882	1,00209

Показатель NAD предсказуемо растет с увеличением длины сообщения, однако рост не является существенным, т.к. при длинах сообщений менее 43 Кб показатель не превышает 0,3%. Качество изображения и структурное содержание отклоняются от 1 в среднем на 0,2%.

Результаты согласуются с визуальными наблюдениями и находятся на уровне хорошо–удовлетворительно для длинных сообщений.

Приведем на рис. 2 сравнение показателей SNR для различной разрядности.

При увеличении числа используемых разрядов показатели ухудшаются и составляют менее чем 27 дБ. Стоит отметить, однако, что величина 50% не означает, что используются половина разрядов для каждого значения, а значит, что для встраивания используются значения, размер дробной части которых не менее чем в 2 раза больше, чем число используемых разрядов.

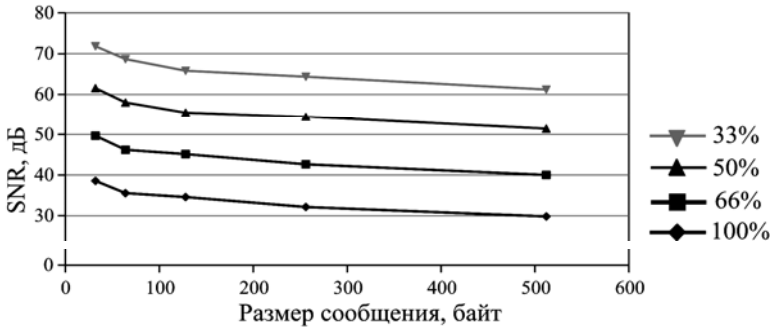

Рис. 2. Зависимость метрик SNR от длины встраемого сообщения для различных разрядностей

Заключение. В работе представлены проводимые исследования в области компьютерной стеганографии. В качестве результатов исследований была изложена концепция нового метода встраивания скрытой информации в векторные изображения, представлен общий алгоритм и разработан программный прототип. Кроме этого, в работе отражены некоторые общие методики оценки качества встраивания по отношению к пассивному противнику, их количественные и качественные оценки для разработанного стеганографического метода.

В результате проведенного исследования было показано, что цифровые векторные иображения, вполне пригодны к использованию в качестве стеганоконтейнера для встраивания секретных сообщений, разработанный метод стеганографического встраивания тому подтверждение. При этом было установлено следующее:

1. В зависимости от требований к надежности стеганографической системы можно варьировать число разрядов для встраивания, тем самым изменяя максимальный объем скрываемой информации.
2. Целесообразно использовать изображения с большим числом знаков дробной части констант и большим числом геометрических объектов. Это позволяет увеличивать число разрядов для встраивания информации.
3. Встраивание сообщения остается незамеченным при использовании 2 разрядов для заполения значений с дробной частью от 4 и более разрядов. При этом допустимо использовать и соотношение в 66%, но для небольших сообщений.

Теоретическая значимость полученных результатов заключается в расширении области применения компьютерной стеганографии. Практическая значимость полученных результатов заключается в возможности их применения для скрытой передачи информации с высокой надежностью и стойкостью к обнаружению.

Литература

1. Гатчин Ю.А. Теория информационной безопасности и методология защиты информации / Ю.А. Гатчин, В.В. Сухостат. – СПб.: СПбГУ ИТМО, 2010. – 98 с.

2. Аграновский А.В. Стеганография, цифровые водяные знаки и стеганоанализ / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин. – М.: Вузовская книга, 2009. – 220 с.

3. Статистика использования SVG для вебсайтов [Электронный ресурс]. – Режим доступа: http://w3techs.com/technologies/details/im-svg/all/all, свободный (дата обращения: 11.12.2014).

4. Барсуков В.С., Романцов А.П. Компьютерная стеганография вчера, сегодня, завтра [Электронный ресурс]. – Режим доступа: http://www.ess.ru/sites/default/files/files/articles/ 1998/0405/1998_0405_03.pdf, свободный (дата обращения: 11.12.2014).

5. Wang H. Cyber warfare: steganography vs. steganalysis / H. Wang, S. Wang // Communications of the ACM. – 2004. – Vol. 47. – P. 76–82.

6. Архипов О.П. Параметрический класс прямых прозрачных методов стегокодирования цветных изображений / О.П. Архипов, П.О. Архипов, З.П. Зыкова // Информационные технологии, вычислительные системы. – 2003. – Вып. 1–2. – С. 95–101.

7. Алиев А.Т. О применении стеганографического метода LSB к большим областям монотонной заливки // Вестник Дагестанского государственного технического университета. – 2004. – Т. 4, вып. 4 (22) . – С. 67–72.

8. Fortrini M. Steganography and digital watermarking: A global view // University of California, Davis. [Электронный ресурс]. – Режим доступа: http://www-lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti00/fortini/project.pdf, свободный (дата обращения: 11.12.2014).

9. Zhou X. Wmxml: A system for watermarking xml data / X. Zhou, H. Pang, K. Tan, D. Mangla // VLDB '05 Proceedings of the 31st international conference on Very large data bases. – 2005. – P. 1318–1321.

10. Wang G. A High Capacity Reversible Watermarking Scheme Based on an Integer Transform / G. Wang, X. Li, B. Yang // Advances in Multimedia Information Processing. – PCM. – 2009. – Vol. 5879. – P. 1287–1292.

11. Yang C.H., Lin T.M., Chang C.C. Information Hiding in SVG by Affine Transformation with Small Perturbation // 2008 International Conference on Advanced Information Technologies (AIT). [Электронный ресурс]. – Режим доступа: http://www.inf.cyut.edu.tw/AIT2008/ ft_251.pdf, свободный (дата обращения: 11.12.2014)

12. Zhou X. Watermark-Based Scheme to Protect Copyright of SVG Data / X. Zhou, X. Pan // ICCIAS. – 2006. – Vol. 2. – P. 1199–1202.

13. Huber S. Topology-Preserving Watermarking of Vector Graphics / S. Huber, M. Held, R. Kwitt, P. Meerwald // International Journal of Computational Geometry & Applications. – 2014. – Vol. 1. – P. 61–86.

14. Blum L. A Simple Unpredictable Pseudo-Random Number Generator / L. Blum, M. Blum, M. Shub // SIAM Journal on Computing. – 1986. – Vol. 15. – P. 364–383.

15. Blum L. Comparison of two pseudo-random number generators / L. Blum, M. Blum, M. Shub // Advances in Cryptology: Proceedings of Crypto. – 1982. – P. 61–78.

16. The MD5 Message-Digest Algorithm [Электронный ресурс]. – Режим доступа: https://tools.ietf.org/html/rfc1321, свободный (дата обращения: 11.12.2014).

17. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков. – М.: СОЛОН-ПРЕСС, 2009. – 265 с.

18. Коханович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Коханович, А.Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.

Менщиков Александр Алексеевич
Студент каф. прикладной математики и компьютерной безопасности
Института космических и информационных технологий Сибирского федерального университета
Тел.: 8-913-507-04-09
Эл. почта: ntpcp@yandex.ru

Шниперов Алексей Николаевич
Канд. техн. наук, доцент каф. прикладной математики и компьютерной безопасности
Института космических и информационных технологий Сибирского федерального университета
Тел.: +7 (391-2) 06-27-43
Эл. почта: Ashniperov@sfu-kras.ru

Menshchikov A.A., Shniperov A.N.

The method of data hiding in vector graphics formats

The paper describes a new method of steganographic data embedding with the use of digital vector graphics, which contain constants of high precision decimals. We estimate the additional noise, which appears depending on the parameters of data hiding process. This method could be used for hidden and secure communication with a high reliability and detection resistance.

Keywords: steganography, hidden data transmission, protection of confidential information, digital watermarks.