УДК 004.056+003.26

АДАПТАЦИЯ СТЕГАНОГРАФИЧЕСКОГО МЕТОДА, ОСНОВАННОГО НА ИЗМЕНЕНИИ ПРОСТРАНСТВЕННОЙ ОБЛАСТИ, ДЛЯ ВЕКТОРНЫХ ИЗОБРАЖЕНИЙ ФОРМАТА SVG

Н. И. Уласевич, М. Г. Савельева

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Рассмотрены два стеганографических подхода: модификация цветовых каналов пикселей растрированного документа и внедрение дополнительных элементов в векторные изображения SVG. Предложена адаптация метода, использующего полутоновые значения текстовых символов для выбора контейнерных элементов, к векторной графике. В качестве модифицируемых атрибутов выступают координаты центров эллипсов, скрытых под закрашенными областями. Встраивание битов сообщения осуществляется по правилу четности координат. Разработанные алгоритмы имеют линейную сложность и сохраняют визуальную целостность изображения.

Ключевые слова: стеганография; растровая графика; векторная графика; SVG; полутоновые значения; эллипс; адаптация алгоритма.

ADAPTATION OF A STEGANOGRAPHIC METHOD BASED ON SPATIAL DOMAIN MODIFICATION FOR SVG VECTOR IMAGES

N. I. Ulasevich, M. G. Savelieva

Educational Institution “Belarusian State University of Informatics and Radioelectronics”, Minsk, Republic of Belarus

Abstract. Two steganographic approaches are considered: modification of pixel color channels in a rasterized document and embedding additional elements into SVG vector images. An adaptation of the method that uses halftone values of text symbols to select container elements is proposed for vector graphics. The coordinates of ellipse centers hidden under filled areas serve as modifiable attributes. Message bits are embedded according to the parity rule of the coordinates. The developed algorithms have linear complexity and preserve the visual integrity of the image.

Keywords: steganography; raster graphics; vector graphics; SVG; halftone values; ellipse; algorithm adaptation.

Введение

Защита авторских прав и скрытая передача данных являются важными задачами в области информационной безопасности [1]. Стеганографические методы позволяют внедрять тайные сообщения

в объекты-контейнеры без заметного искажения их свойств. Перспективными контейнерами выступают как растровые, так и векторные изображения.

В работе [2] предложен метод скрытия информации в растровых изображениях, полученных после растрирования векторных текстовых символов. Выбор пикселей для встраивания определяется сопоставлением их цветовых характеристик с ключевыми значениями. В методе [3] для векторных изображений SVG используется правило визуального ранжирования: дополнительные эллипсы, помещенные в начало документа, перекрываются закрашенными фигурами и становятся невидимыми, а информация кодируется в дробных частях угла и расстояния от ключевой точки.

Цель работы – адаптировать метод [2], основанный на полутоновых значениях текстовых символов и модификации по четности, для использования в векторных файлах SVG, что позволит объединить преимущества методов.

Основная часть

В работе [2] контейнером служит растровое изображение, полученное после растрирования векторных текстовых символов с заданным разрешением. При растрировании возникают полутоновые пиксели, контур буквы «расплывается», и общее количество пикселей увеличивается. Именно в эти новые пиксели предлагается встраивать информацию. Формируется массив пикселей, для которых значение выбранного цветового канала равно заданному эталону. Встраивание бита сообщения в другой цветовой канал осуществляется изменением четности значения: если бит не соответствует текущей четности, к значению прибавляется нечетное число (шаг изменения). Извлечение производится путем анализа четности значений того же цветового канала у тех же пикселей.

В работе [3] используется векторный формат SVG, основанный на XML и позволяющий описывать графические объекты с помощью математических координат. В документ добавляются эллипсы с малым радиусом, которые располагаются в коде до закрашенных фигур. Благодаря правилу визуального ранжирования такие эллипсы перекрываются вышележащими фигурами и не отображаются на экране. Центры эллипсов выбираются внутри многоугольников, полученных из исходных примитивов. Информация кодируется путем выбора позиций в дробных частях угла наклона прямой, соединяющей центр эллипса с ключевой точкой, и расстояния до нее.

Предлагается перенести ключевые принципы работы [2] – выбор элементов на основе полутоновых значений текстовых символов и встраивание битов по правилу четности – в векторную среду. В качестве

контейнера рассматривается SVG-документ, содержащий текстовые элементы и закрашенные векторные фигуры (прямоугольники, многоугольники и т.п.).

Для каждого текстового элемента (символа или его части) вычисляется числовое значение, которое является аналогом полутонового оттенка из растрового метода. В простейшем случае это может быть хеш-код от строки символа или значение яркости при виртуальном растрировании с фиксированным разрешением. Задается эталонное значение. Если вычисленное значение совпадает с эталоном, то данный текстовый элемент выбирается для формирования точки-кандидата. В качестве такой точки используется, например, центр ограничивающего прямоугольника текстового элемента или точка, смещенная от него по диагонали (по аналогии с исходным методом, где брался пиксель, расположенный по диагонали от проверяемого).

В найденной точке создается эллипс с малым радиусом (например, 0,1 условных единиц). Этот эллипс добавляется в начало SVG-документа (чтобы оказаться под всеми закрашенными фигурами) и включается в массив эллипсов, предназначенных для встраивания. Таким образом, массив формируется на основе текстовых элементов, удовлетворяющих ключевому условию.

Скрываемое сообщение преобразуется в двоичную последовательность. Для каждого бита последовательно используется эллипс из сформированного массива. Выбор модифицируемого атрибута задается ключом. Правило встраивания: если бит сообщения равен единице, целая часть выбранной координаты должна быть нечетной; если бит равен нулю – четной. Если текущее значение уже удовлетворяет требуемой четности, изменение не производится. В противном случае к значению прибавляется нечетное число. Поскольку прибавляемое число нечетное, четность меняется на противоположную. Величина шага выбирается минимальной, чтобы изменение координаты было незаметным. Так как радиус эллипса крайне мал, а сам эллипс скрыт под закрашенной фигурой, даже заметное смещение его центра не будет обнаружено визуально.

Извлечение производится в обратном порядке. Из SVG-документа выбираются все эллипсы с радиусом, не превышающим заданный порог. Для каждого такого эллипса определяется значение выбранной. Четность целой части определяет бит сообщения: четное – ноль, нечетное – единица. Последовательность битов преобразуется в исходное сообщение. Если при встраивании использовалась служебная информация, например, длина сообщения, она извлекается аналогичным образом.

Заключение

Предложена адаптация стеганографического метода, первоначально разработанного для растровых изображений, к векторному формату SVG. В отличие от исходного подхода, где контейнером выступают пиксели, модификация переносится на координаты эллипсов, скрытых под закрашенными фигурами. Выбор эллипсов осуществляется на основе числовых характеристик текстовых элементов, что сохраняет принцип избирательности, свойственный исходному методу. Дальнейшие исследования могут быть направлены на оценку пропускной способности, устойчивости метода к атакам, а также на использование других векторных примитивов и атрибутов для увеличения емкости.

Список использованных источников

1. Урбанович П. П. (2016) *Защита информации методами криптографии, стеганографии и обфускации*. Минск, БГТУ.

2. Савельева М. Г. (2024) Метод стеганографического преобразования на основе изменения пространственной области растрированного документа-контейнера. *Веб-программирование и интернет-технологии (WebConf2024): материалы 6-й Междунар. науч.-практ. конф.* , 337–340.

3. Уласевич Н. И., Жиляк Н. А. (2025) Стеганографический метод на основе встраивания дополнительных элементов под закрашенные участки в изображениях в формате SVG. *Труды БГТУ. Сер. 3, Физико-математические науки и информатика, (2),* 76–82.

References

1. Urbanovich P. P. Information protection by cryptography, steganography and obfuscation methods. Minsk, BGTU Publ., 2016. 220 p. (In Russian).

2. Savelieva M. G. Method of steganographic transformation based on spatial domain modification of a rasterized container document. *Web Programming and Internet Technologies (WebConf2024): Proceedings of the 6th International Scientific and Practical Conference*, p. 337–340 (in Russian)

3. Ulasevich N. I., Zhilyak N. A. A steganographic method based on embedding additional elements under the colored areas in SVG format images. Proceedings of BSTU, issue 3, Physics and Mathematics. Informatics, 2025, no. 2 (296), pp. 76–82. (In Russian).

Сведения об авторах

Уласевич Н.И. ассистент кафедры информационных систем и технологий. учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», koliaulasevich@gmail.com

Савельева М.Г. ассистент кафедры информационных систем и технологий. учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», saveleva@belstu.by

Information about the authors

Mikalai I. assistant of the Department of Information Systems and Technologies, Educational Institution "Belarusian State University of Informatics and Radioelectronics", koliaulasevich@gmail.com

Marina G. assistant of the Department of Information Systems and Technologies, Educational Institution "Belarusian State University of Informatics and Radioelectronics", saveleva@belstu.by