проблемами. Кроме того, разрабатываются программные средства, нацеленные на решение вопросов кибербезопасности электронной системы обучения университета.

Обеспечение информационной безопасности невозможно без выполнения следующих действий:

- обеспечение защиты от несанкционированного доступа;
- обеспечение защиты интеллектуальной собственности;
- предотвращение распространения в Интернете компьютерных вирусов, спама и шантажа;
- развитие национальной законодательной базы определения порядки применения специальных средства защиты в Интернет среде;
- разработка регулирующих условий для выявления и наказания злоумышленников;
- подготовка кадров, способных бороться с самыми опасными угрозами в цифровой среде.

Выполнение этих работ поможет решить проблему обеспечения безопасности Цифровой системы образования.

Список использованных источников

4. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Учебное пособие. - М.: ИД. "Форум": ИНФРА - М. 2013-592с.

5. Karl Maria Michael de Leeuw, Jan Bergstra - The History of Information Security: A Comprehensive Handbook, Elsevier Science, 2007.

6. M.Çuriýew. Maglumatlary goramak. Ýokary okuw mekdepleri üçin okuw kitaby. –A.: Türkmen döwlet neşirýat gullugy, 2013, 206 s.

УДК 003.26

Н.И. Уласевич
Белорусский государственный технологический университет
Минск, Беларусь

СТЕГАНОГРАФИЧЕСКИЕ РЕШЕНИЯ В SVG ФАЙЛАХ

Аннотация. *В рамках статьи изучаются и анализируются методы и алгоритмы встраивания информация в векторных файлах. Рассмотрены некоторые особенности отображения и стеганографии в векторных файлах.*

N.I. Ulasevich
Belarusian State Technological University
Minsk, Belarus

STEGANOGRAPHIC SOLUTIONS IN SVG FILES

Abstract. *The article includes the study and analysis of methods and algorithms for embedding information in vector files. The specific feature associated with the display of vector files and explores steganography in them.*

Цифровые технологии не только позволяют хранить и передавать различные типы данных, такие как изображения, тексты и звук, но и являются средством их создания. Однако такое преимущество цифровых технологий также может быть использовано для негативных целей, таких как незаконное копирование, распространение, использование или даже уничтожение информации. В силу этого все более важной становится проблема разработки и использования методов и инструментальных средств для защиты информации, включая права интеллектуальной собственности.

Одним из возможных решений данной проблемы для графических файлов является технология цифрового водяного знака. К особенностям защиты можно отнести достаточно большой объём файла необходимый для хранения информации, в следствии чего возникают возможности для встраивания (осаждения) различных невидимых меток.

В основном исследования сосредоточены на растровых форматах изображений, для которых разработано большое число методов в том числе и стенографических. Кроме использования растровых изображения также повсеместно используются векторные изображения что привело к исследованиям и разработке стенографических методов для обеспечения целостности и защиты прав интеллектуальной собственности.

Возможности осаждения скрытой информации в векторных файлах описываются в многочисленных источниках.

В источнике [1] рассмотрен механизм внедрения скрытой информации в SVG-изображения, который основан на модификации дробных частей координат вершин геометрических фигур, что имеет аналог в виде метода НЗБ (Наименьшего Значащего Бита) для растровых изображений. К недостатку данного метода можно отнести незначительное изменение размера фигур, которое может быть критично для некоторых программных продуктов.

В источнике [2] упоминается метод основанный на прорисовке отдельных точек поверх существующих линий. Если линия и точка имеют один цвет и размер точки не превышает толщину линии, то при визуальной проверке невозможно найти добавленную точку. К недостатку можно отнести то что в большинстве случаев достаточно просто вычислить функцию или набор функций для каждого тега и проверить наличие отдельных точек на линии.

В источнике [3] упоминается подход для встраивания данных в SVG-файлы состоящий в разбиении кривых Безье на части в некотором соотношении. Для извлечения данных берутся две последовательных кривые, и если они образуют единую кривую, то вычисляется коэффициент деления кривой на части. К недостатку можно отнести увеличение размера файла вследствие добавления большого числа точек для описания одного бита информации.

Помимо встраивания информации непосредственно в параметры тегов в файлах формата SVG можно использовать стеганографические методы для текстовых контейнеров. При использования данного подхода при определенных условиях, объём передаваемой информации может превысить значения, свойственные растровой графике. Кроме того, стенографические алгоритмы, разработанные для изображений в SVG-формате, могут быть использованы для сокрытия информации в PDF-документах. Алгоритм представленный в источнике [4] предусматривает извлечение изображения из PDF-файла, преобразования его в формат SVG, встраивания скрытой информации и обратного добавления изображения в документ.

Рассматривая часть кода файла в формате SVG на рис. 1. Он формирует два исходных прямоугольника в файле векторного изображения представленного на рис. 2.

```
<g>
<rect x="50" y="50" width="100" height="100"
      fill="none" stroke="blue" stroke-width="3"/>
<rect x="100" y="100" width="100" height="100"
      fill="none" stroke="red" stroke-width="5"/>
</g>
```

Рис. 1 - Текст файла SVG с исходными прямоугольниками

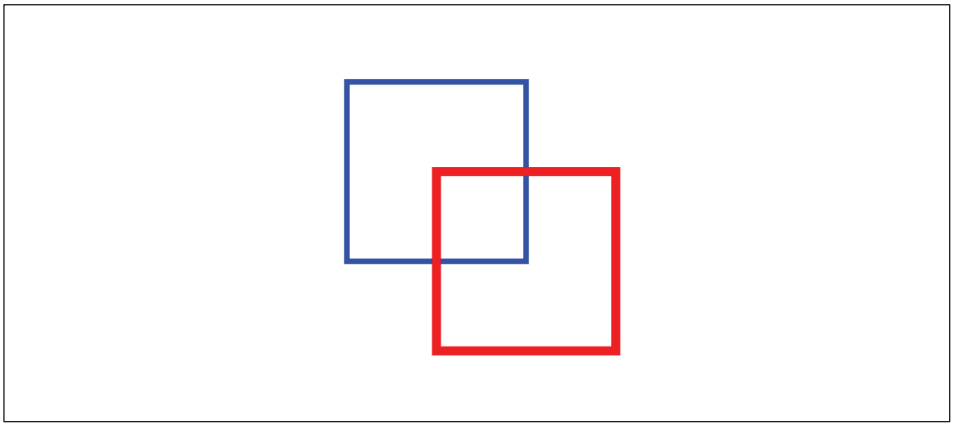

Рис. 2 - Файл SVG с исходными прямоугольниками

Рассмотрим код на рис. 1. Как можно увидеть у фигур отсутствует заливка. При добавлении заливки второй фигуре часть первой фигуры будет перекрыта что представлено на рис. 3.

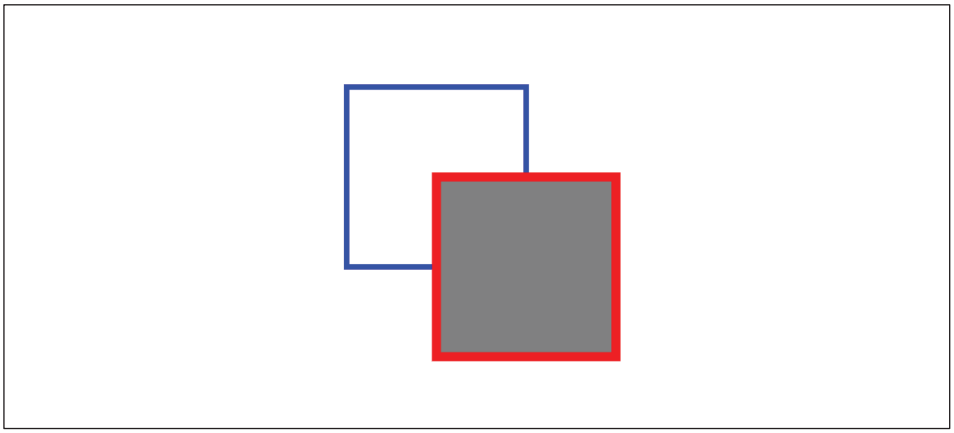

Рис. 3 - Файл SVG с добавленной заливкой второй фигуры

Исходя из представленного выше можно предположить возможность сокрытия информации за фигурами, обладающие заливкой или за линиями с достаточной толщиной. Как пример простейшей реализации можно добавить третий квадрат с зеленой заливкой под второй фигурой, что отображено на рис. 4 и 5.

```
<g>
<rect x="50" y="50" width="100" height="100"
      fill="none" stroke="blue" stroke-width="3"/>
<rect x="120" y="120" width="15" height="15"
      fill="green" stroke="green" stroke-width="5"/>
<rect x="100" y="100" width="100" height="100"
      fill="grey" stroke="red" stroke-width="5"/>
</g>
```

Рис. 4 - Часть текста файла SVG с дополнительным прямоугольниками

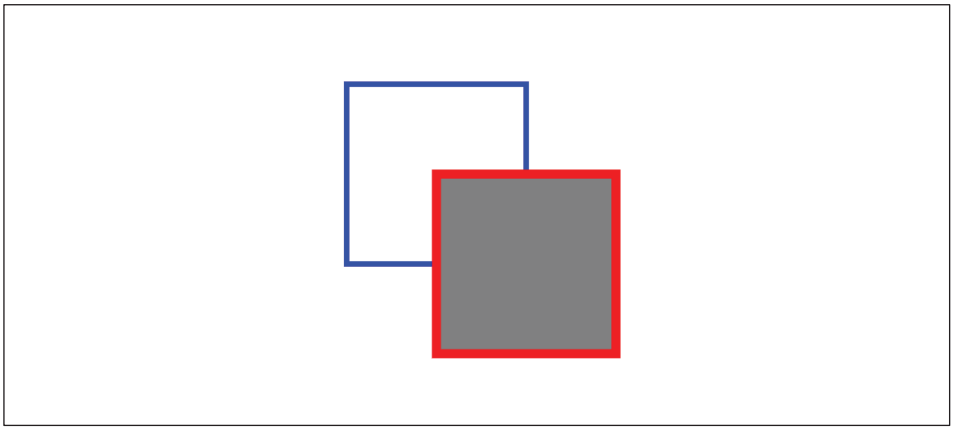

Рис. 5 - Файл SVG с добавленным прямоугольником

Описанный способ позволяет встроить дополнительную информацию в документ без искажения данных. Данный способ целесообразно применять для изображений, содержащих большое число разнообразных геометрических элементов и при некоторой модификации для конвертированных растровых изображений.

Список использованных источников

1. Huber S., Held M., Kwitt R., Meerwald P. Topology-Preserving Watermarking of Vector Graphics. International Journal of Computational Geometry & Applications, 2014, vol. 1, pp. 61–86.
2. Madoš B., Hurtuk J., Čopjak M., Hamaš P., Ennert M. Steganographic Algorithm For Information Hiding Using Scalable Vector Graphics Images. Acta Electrotechnica et Informatica, 2014, vol. 14, no. 4, pp. 42–45
3. Блинова Е.А., Урбанович П.П. Стеганографический метод на основе встраивания скрытых сообщений в кривые Безье изображений формата SVG. Журнал Белорусского государственного университета. Математика. Информатика. 2021, т. 3, с. 68–83.
4. Горбачев В.Н., Метелёв И.К., Кайнарова Е.М., Полякова М.А. Стеганографическая защита изображений из PDF документов на основе конвертора PDF-SVG. GraphiCon. 2017, с. 108–111.