УДК 003.26

АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ ДЛЯ ФАЙЛОВ-КОНТЕЙНЕРОВ ФОРМАТА SVG

А. Н. Николайчук

Белорусский государственный технологический университет, Минск
e-mail: nikolaichukalexandra@gmail.com

Обеспечение безопасности цифровых электронных документов является важным аспектом их хранения и передачи. Одним из методов защиты информации выступает использование технологии цифрового водяного знака (ЦВЗ), основанной на применении стеганографического метода, суть которого заключается в скрытом размещении сообщения [1].

Для различных форматов цифровых документов необходимо разрабатывать отдельные методы защиты ввиду уникальности описания и свойств каждого из них. Формат масштабируемой векторной графики (Scalable Vector Graphics – SVG) позволяет легко манипулировать объектами, из которых состоит, благодаря своей структуре, основанной на языке разметки XML, описывающей графические объекты с помощью координат ключевых точек в значениях атрибутов, а также предоставляет широкое разнообразие в выборе контейнера. Для оценки эффективности методов целесообразно провести анализ производительности операции встраивания сообщения.

Рассматривались два известных метода внедрения информации в кривые Безье файла формата SVG с доступным программным обеспечением [2, 3]. Суть первого метода заключалась в разделении кривых Безье, из которых состоит изображение, на сегменты в определенном отношении. Способ разделения кривой Безье, используемый в работе [2], позволяет сформировать дополнительные точки на кривых, в которые внедряется сообщение. Метод в работе [3] дает возможность внедрить данные в пустое пространство изображения, используя уникальность описания фигур векторной графики. Такая графика заключается в том, что объекты, которые создаются вне рабочей области, где находится геометрический объект, не видны пользователю, поэтому данное свойство используется для внедрения скрытого сообщения.

Для исследования были выбраны четыре изображения формата SVG разного размера (424, 814, 1284 и 2568 КБ), в которые внедрялось одно и то же сообщение: «*My Visa Credit Card number is 4539962848122779, CCV number is 483, and Expiration Date is 12/23*». Для каждого изображения проводилась операция внедрения сообщения по 100 раз двумя методами, которые были описаны выше, и высчитывалось время выполнения каждой.

По результатам выполнения операций внедрения для метода [2], представленных на диаграмме рис. 1, где каждая точка обозначает отдельную операцию, наблюдается зависимость между размером файла и временем, которое занимает внедрение сообщения: при увеличении размера файла время, необходимое для выполнения операции, также увеличивается.

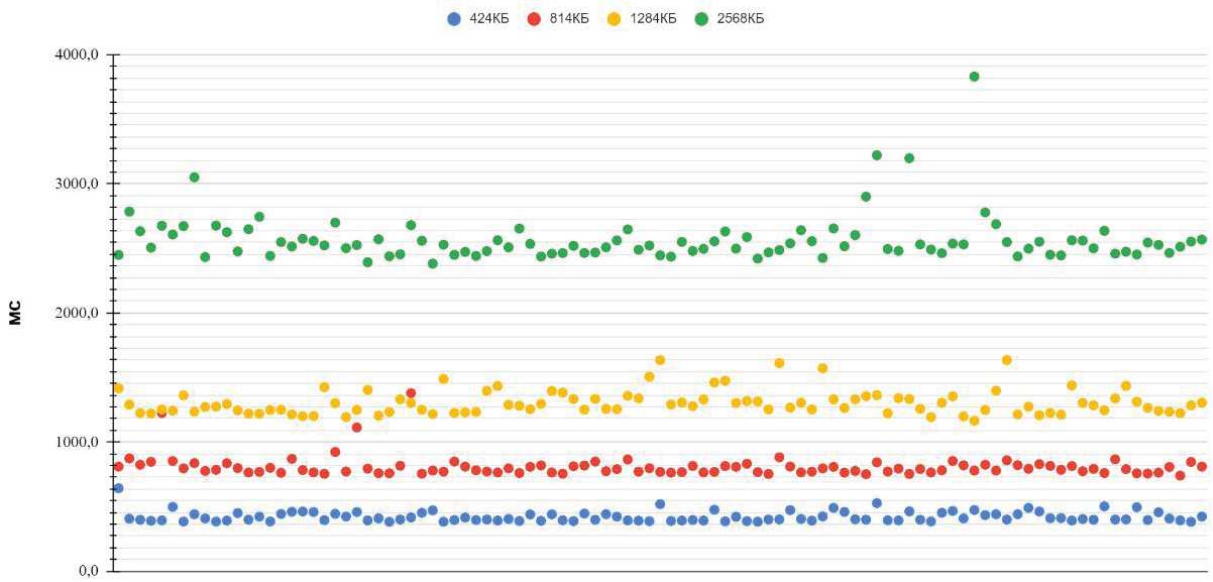

Рис. 1. Диаграмма времени выполнения операции внедрения сообщения методом, использующим разбиение кривой

Используя метод [3], результаты на диаграмме рис. 2 показывают, что время выполнения внедрения не зависит от размера файла.

Такой способ стеганографического осаждения информации в контейнер позволяет размеру сообщения быть независимым от размера самого контейнера или его содержимого и предотвратить модификацию внедренной информации при использовании операции сдвига, которая может рассматриваться как тип несанкционированной модификации стеганоконтейнера.

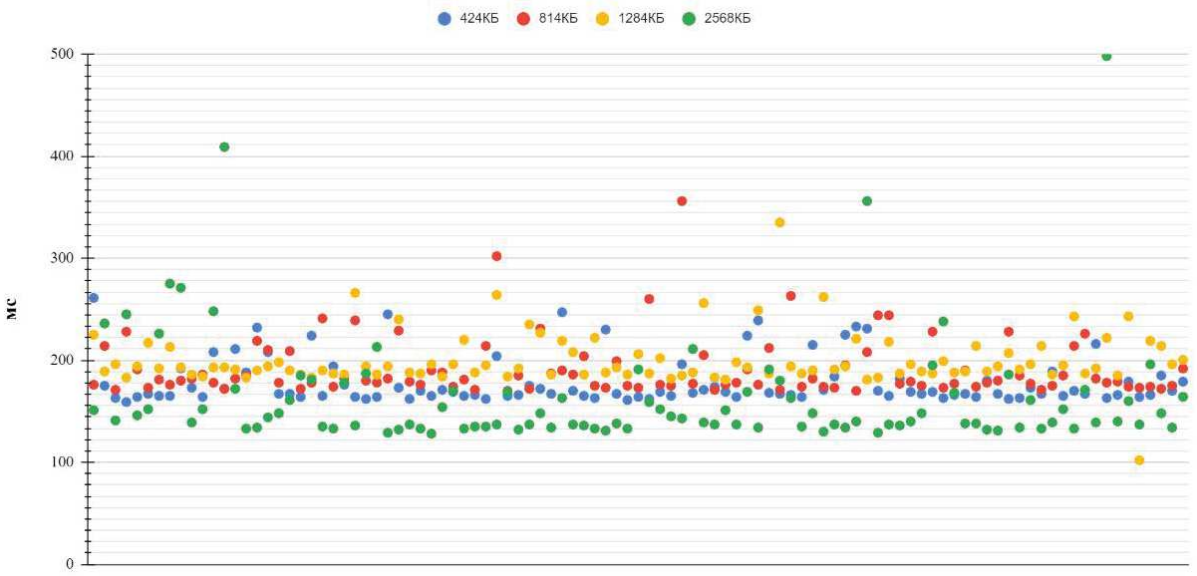

Рис. 2. Диаграмма времени выполнения операции
внедрения сообщения в невидимую область

Согласно полученным данным составлена таблица, показывающая усредненное значение времени выполнения (мс) методов для каждого контейнера.

Среднее время выполнения внедрения сообщения методов
для контейнеров разного размера

Размер контейнера, КБ	Метод, использующий разбиение кривой	Метод внедрения сообщения в невидимую область
424	422,2	179,0
814	809,7	191,9
1284	1305,4	200,4
2568	2568,6	164,18

Поскольку время выполнения операции зависит от устройства, использующего программное обеспечение, стоит оценивать отношение между полученными значениями. Исходя из результатов можно заметить, что время выполнения операции внедрения скрытого сообщения методом [3] остается неизменным для любого контейнера, в то время как выполнение внедрения сообщения методом [2] растет пропорционально увеличению размера контейнера.

Список литературы

1. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации : учеб.-метод. пособие / П. П. Урбанович. – Минск : БГТУ, 2016. – 220 с.

2. Блинова, Е. А. Стеганографический метод на основе встраивания скрытых сообщений в кривые Безье изображений формата SVG / Е. А. Блинова, П. П. Урбанович // Журнал Бел. гос. ун-та. Математика. Информатика. – 2021. – № 3. – С. 68–83.

3. Николайчук, А. Н. Стеганографический метод на основе использования особенностей отображения элементов в формате SVG / А. Н. Николайчук, П. П. Урбанович // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. – 2023. – № 1 (266). – С. 64–70.