обращения - 01.10.2022); Индекс человеческого капитала / Гуманитарный портал: Исследования [Электронный ресурс] // Центр гуманитарных технологий, 2006–2022 (последняя редакция: 18.07.2022). URL: https://gtmarket.ru/ratings/human-capital-index (Дата обращения - 01.10.2022)

Для первых двух индикаторов, приведенных в таблице 1, указаны пороговые значения согласно сложившейся традиции в рамках теории экономической безопасности. Однако общепринятых пороговых значений для прочих индикатор в данное время не существует. Требуется провести отдельное серьезное исследование для определения уровня, безопасного для экономики в контексте применения каждого из них. На данном этапе предлагаем применять в качестве пороговых значений среднее значение по первой десятке в рейтинге стран мира, так как очевидно, что серьезное отставание от лидеров по развитию технологий уже создает значительные угрозы экономической безопасности.

Список использованных источников

1. Абалкин Л.И. Экономическая безопасность России // Вестник РАН. 1997. Т. 67. № 9. С. 771–776.
2. Власова М.С., Степченкова О.С. К вопросу о развитии системы мониторинга технологической безопасности в условиях перехода к высокотехнологичной экономике/ Национальные интересы: приоритеты и безопасность. 2018. т. 14, вып. 9. С. 1680–1692
3. Кальченко О.А. Индексы и показатели управляемого устойчивого развития// Известия ВУЗов. Серия «Экономика, финансы и управление производством». № 02 (28). 2016. С. 27-32

УДК 004.021

Е.А. Блинова, К.С. Марчук, П.П. Урбанович
Белорусский государственный технологический институт
Минск, Беларусь

СТЕГАНОГРАФИЧЕСКИЙ МЕТОД НА ОСНОВЕ РАЗМЕЩЕНИЯ НЕСКОЛЬКИХ КОПИЙ СКРЫТОГО СООБЩЕНИЯ В SVG-КОНТЕЙНЕР

Аннотация. *Приведено описание стеганографического метода многократного встраивания цифрового водяного знака в файлы векторных изображений формата SVG. Предлагаемый стеанографический метод основывается на многократном разбиении кривых Безье методом де Кастельжо.*

Разработано приложение для демонстрации прямого и обратного стеганографического преобразования.

E.A. Blinova, K.S. Marchuk, P.P. Urbanovich
Belarusian State Technological University
Minsk, Belarus

STEGANOGRAPHIC METHOD BASED ON PLACING SEVERAL COPIES OF HIDDEN MESSAGE INTO SVG CONTAINER

Abstract. *The description of the steganographic method of embedding a digital watermark into the vector image files on placing several copies of the SVG format is given. The proposed steganographic method is based on multiple partitioning of Bezier curves by the de Casteljau method. The application has been developed to demonstrate the forward and reverse steganographic transformation.*

Цифровая стеганография – это направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые файлы. Для защиты от копирования в задаче сохранения авторских прав или для обеспечения целостности используются цифровые водяные знаки (ЦВЗ) или идентификационные метки. Обычно ЦВЗ считываются специальным устройством, которое может подтвердить либо опровергнуть его правильность. Технология записи идентификационных меток производителей очень похожа на ЦВЗ, но отличие состоит в том, что на каждое изделие записывается свой индивидуальный номер, по которому можно вычислить уникальность изделия. Такое метод используется обеспечения валидности товаров, для подписей медицинских снимков, нанесения пути на карту. Основными требованиями, предъявляемыми к ЦВЗ и идентификационным меткам, являются надёжность, устойчивость к искажениям, незаметность, способность системы к восстановлению после воздействия [1].

Актуальной является задача создания ЦВЗ для различных типов изображений, в том числе и векторных. Целью настоящего исследования является реализация стеганографического метода скрытия и извлечения ЦВЗ из файлов векторной графики, обладающего устойчивостью к искажениям, для чего сообщение многократно дублируется и помещается во все имеющиеся кривые Безье.

Формат изображений SVG является наиболее распространённым среди векторных изображений. SVG (*Scalable Vector Graphics*) – язык разметки векторной графики, являющийся подмножеством языка разметки XML. Просмотр и изменение файлов SVG возможно выполнять даже в текстовом редакторе. Данный формат файла был

разработан для применения в сети Интернет и расширение SVG является открытым. Файлы SVG могут быть отображены прямо в браузере или внедрены в файлы HTML посредством нескольких методов.

Спецификация SVG 1.1 определяет 14 функциональных областей или наборов функций. Самая главная функция – это путь (*path*). Пути – это контуры простых или составных фигур, которые рисуются изогнутыми или прямыми линиями, которые можно заполнить, обвести или использовать в качестве контура. Пути имеют компактную кодировку и содержатся в атрибуте *d* элемента *path*. Каждая команда начинается с конечной позиции предыдущей команды. Путь может задаваться как абсолютными, так и относительными координатами. Во всех случаях абсолютные координаты следуют за командами с заглавными буквами, а относительные координаты используются после эквивалентных строчных букв [2].

При построении SVG файлов могут использоваться кривые Безье. При построении кубических кривых Безье используются четыре точки: одна начальная P_1, две опорные P_2 и P_3, одна конечная P_4. Встраивание скрытой информации реализуется разделением кубических кривых Безье на участки, каждый из которых является кривой Безье. При этом формируются дополнительные точки, в координаты которых внедряется скрытая информация. Дополнительные точки не отображаются при сравнении с оригиналом изображения, хотя и наличествуют в его текстовом описании. Таким образом в файлах формата SVG можно произвести скрытие данных путем разделения кривых Безье на части согласно методу, предложенному в [3].

Опишем алгоритм скрытия информации в файле формата SVG, содержащем кривые Безье. Для скрытия будем использовать ЦВЗ в виде текста. Перед выполнением алгоритма необходимо выполнить анализ SVG-файла на наличие, количество и вид кривых Безье. Далее скрытие производится в набор кривых Безье.

Шаг 1. Пусть кривые Безье изначального изображения описываются точками M_1, …, M_m, которые являются начальными точками кривых Безье, где m – количество кривых Безье в файле, а точки $C_{j,1}$, …, $C_{j,N}$ – опорные точки j-й кривой. Каждая кривая может содержать любое количество точек, большее трех.

Шаг 2. Проверяем, являются ли координаты точек C абсолютными величинами или относительными. В случае, если координаты точек кривой являются относительными, то их следует преобразовать в абсолютные по следующей формуле:

$$C_{j,i} = M_j + C_{j,i}.$$

В случае, если координаты точек кривой являются абсолютными, в преобразовании нет необходимости.

Шаг 3. Рассмотрим первую кривую и используем первые 4 точки кривой. На данном шаге используются точки M_1, $C_{1,1}$, $C_{1,2}$, $C_{1,3}$. Необходимо произвести операцию построения двух новых кривых из одной изначальной. Для реализации был выбран метод разбиения де Кастельжо [4]. Согласно данному методу, любую кривую можно разделить на две новые в некотором отношении. Для этого на кривой выбирается точка, которую далее будем называть точкой разделения. Для расчёта точки разделения используем параметрическое уравнение кривой Безье третьего порядка:

$$C = (1-t)3P1 + 3(1-t)2tP2 + 3(1-t)t2P3 + t3P4,\ t\in[0,1],$$

где P_i – точки кривой.

Пусть параметр s – отношение разделения, а C – точка разделения. В таком случае формула приобретает следующий вид:

$$C = (1-s)^3 M_1 + 3(1-s)^2\, s\, C_{1,1} + 3(1-s)\, s^2\, C_{1,2} + s^3\, C_{1,3}.$$

Данная точка является конечной для первой создаваемой кривой, и начальной для второй. Опорные точки C_{n12} и C_{n13} для первой новой кривой, и опорные точки C_{n22} и C_{n23} для первой новой кривой вычисляются по формулам:

$$C_{n12} = (M_1 - C_{1,1})\, s + M_1;$$

$$C_t = (C_{1,2} - C_{1,1})\, s + C_{1,1};$$

$$C_{n13} = (C_t - C_{n12})\, s + C_{n12};$$

$$C_{n23} = (C_{1,3} - C_{1,2})\, s + C_{1,2};$$

$$C_{n22} = (C_{n23} - C_t)\, s + C_t.$$

Таким образом получаем 2 новые кривые с точками M_1, C_{n12}, C_{n13}, C для первой кривой и C, C_{n22}, C_{n23}, $C_{1,3}$ для второй кривой.

Шаг 4. Используя полученные координаты опорных точек, внедряем сообщение. Изначально ЦВЗ представлен в виде текста. Многократно дублируем текст так, чтобы разместить ЦВЗ в каждой кривой. Используя преобразование, например, по кодировке Unicode, получаем битовый массив для всего сообщения. Далее преобразуем каждый байт информации в целые числа и последовательно записываем в конце координат опорных точек по аналогии с методом *LSB*. Таким образом одна кривая вмещает в себя до 4 байт информации.

Шаг 5. Если в выбранной кривой больше нет необработанных точек и ЦВЗ полностью записан, переходим к шагу 6. Иначе переходим к шагу 3, используя в качестве начальной точки конечную точку из предыдущей итерации алгоритма, и следующие за ней 3 точки.

Шаг 6. Если в списке кривых ещё остались необработанные кривые, переходим к шагу 3, используя следующую кривую в списке. Иначе возвращаем список кривых и переходим к шагу 7.

Шаг 7. Если изначальная кривая имела относительные координаты точек, преобразуем новые кривые к относительным координатам по следующей формуле:

$$C_{j,i} = M_j - C_{j,i}.$$

Шаг 8. Заменяем все кривые из изначального файла новыми кривыми, содержащими скрытую информацию. В результате получаем новое изображение, которое визуально неотличимо от изначального, но имеет в себе внедрённое сообщение.

При извлечении внедрённой информации используется обратный алгоритм. Два последовательных участка одной кривой рассматривается как одна потенциальная кривая Безье, разделенная в определенном отношении *s*. Если это так, то извлекается значение *s*. Иначе предполагается, что эти участки кривой не задействованы в нанесении ЦВЗ. Из координат опорных точек каждой кривой последовательно извлекается ЦВЗ. Последовательно обрабатывается все кривые, находящиеся в файле, и собирается массив ЦВЗ. В случае, если файл не изменился, то во всех кривых Безье текст ЦВЗ будет одинаков. В случае нарушения ЦВЗ в какой-либо кривой Безье алгоритм возвращает текст ЦВЗ по мажоритарному принципу.

Для демонстрации работы метода было разработано приложение «Центр сертификации изображений» для скрытия данных в изображениях SVG. В качестве СУБД использовалась Oracle Database 12c; для реализации веб-приложения использовалась платформа ASP.Net Core версии 3.1 и язык программирования C#; для регистрации пользователей добавлен SMTP сервер для отправки электронных писем. Интерфейс для клиента реализован с помощью Razor Pages по методологии Ajax. В функциональность данного программного продукта входит регистрация и авторизация пользователей; загрузка изображений на сервер и в базу данных; встраивание скрытого сообщения в изображение; получение скрытого сообщения из изображения. Для каждого пользователя генерируется секретный ключ, на основе которого будет вычислено отношение разделения *s*. Пользователь загружает своё изображение на сервер и вводит

сообщение, которое желает скрыть. Приложением отображается, какая максимальная длина сообщения доступна. В изображение встраивается сообщение и пользователю выдаётся уникальный ключ для извлечения сообщения.

Сообщение дублируется и встраивается в файл от его начала до самого конца. В случае, если некоторая часть файла будет повреждена или изменена, по дубликатам скрытого сообщения можно будет восстановить изначальное сообщение.

Метод может применяться для нанесения ЦВЗ или цифровых меток на графические изображения формата SVG, в которых присутствуют кривые Безье. Поскольку формат SVG является де-факто стандартом векторной графики в Интернете, то предложенный метод может применяться для защиты изображений, размещенных на сайтах, от подделки. Дальнейшие исследования в данном направлении представляют интерес с точки зрения обеспечения заданного уровня стеганографической стойкости метода.

Список использованных источников

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

2. SVG документация [Электронный ресурс] / developer.mozilla.org – Режим доступа: https://developer.mozilla.org/ru/docs/Web/SVG. – Дата доступа: 10.00.2022.

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; 3:68–83.

4. Gerald E. Farin and Dianne Hansford. The Essentials of CAGD (1st. ed.). A. K. Peters, Ltd., USA, 2000, 242 c.

УДК 338,005

А.В. Бунь, А.А. Ледницкая, В.П. Прокопович