УДК 004.021

П.В. Бернацкий, Е.А. Блинова
Белорусский государственный технологический университет
Минск, Беларусь

ПРИМЕНЕНИЕ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ ДЛЯ ИЗОБРАЖЕНИЙ ФОРМАТА STEP

Аннотация. *Исследование посвящено применению стеганографических методов для скрытия данных в векторных изображениях файлов стандарта STEP. Обоснована целесообразность использования параметрических структур векторной графики в качестве стеганографических контейнеров для решения задач защиты авторских прав, маркировки и обеспечения целостности цифровых моделей.*

P.V. Bernatsky, E.A. Blinova
Belarusian State Technological University
Minsk, Belarus

APPLICATION OF STEGANOGRAPHIC METHODS FOR IMAGES IN STEP FORMAT

Abstract. *The study is devoted to the use of steganographic methods to hide data in vector images of STEP format files. The feasibility of using parametric vector graphics structures as steganographic containers to solve problems of copyright protection, labeling and ensuring the integrity of digital models is substantiated.*

Стеганография – область науки, занимающаяся методами сокрытия факта передачи информации, часто применяемая для обеспечения конфиденциальности, защиты авторских прав, а также маркировки цифровых данных. Стеганографические контейнеры представлены множеством различных форматов: это векторные и растровые изображения, звуковые и видео файлы, электронные текстовые документы. Для многих документов актуальна задача защиты авторских прав и подтверждения целостности документа [1].

Объектом настоящего исследования являются файлы векторных изображений, содержащих в своем описании объекты в виде совокупности нескольких функций, каждая из которых задана на каком-то множестве значений аргумента, то есть сплайна. Такие файлы широко используются в веб-графике, графическом дизайне, для создания иллюстраций с плавными кривыми, а также инженерных и архитектурных планов. Обработка файлов векторных изображений происходит в программах для векторной графики, таких как Adobe Illustrator, Inkscape, CorelDRAW, в программном обеспечении для

моделирования, например, AutoCAD, Rhino 3D, SolidWorks, Blender и Fusion 360. В работе [2] был предложен стеганографический метод для векторных изображений в формате SVG, содержащих кривые Безье, которые являются частным случаем сплайнов.

Наиболее распространенными видами сплайнов, используемых при описании векторных изображений, могут считаться кривые, описанные *B*-сплайнами (базисный сплайн) и *NURBS* (неоднородный рациональный базисный сплайн). *B*-сплайн описывается формулой:

$$C(u) = \Sigma N_{i,k}(u) \cdot P_i \qquad (1)$$

где $C(u)$ – точка кривой при значении параметра u; P_i – контрольная точка; $N_{i,k}(u)$ – базисная функция степени k, зависящая от узлового вектора.

Сплайн *NURBS* может быть описан следующим образом:

$$C(u) = [\sum N_{i,k} \cdot w_i \cdot P_i] / [\sum N_{i,k}(u) \cdot w_i] \qquad (2)$$

где w_i – вес точки P_i; $N_{i,k}(u)$ – *B*-сплайновая функция; k – степень кривой. Добавление весов w_i позволяет формировать окружности и эллипсы, что делает сплайны *NURBS* стандартом в системах инженерного проектирования. При изменении весов точек форма *NURBS* изменяется без нарушения гладкости, сохраняя локальную структуру данных. На рис. 1 показаны примеры участков кривых, описываемых *B*- сплайнами и *NURBS*.

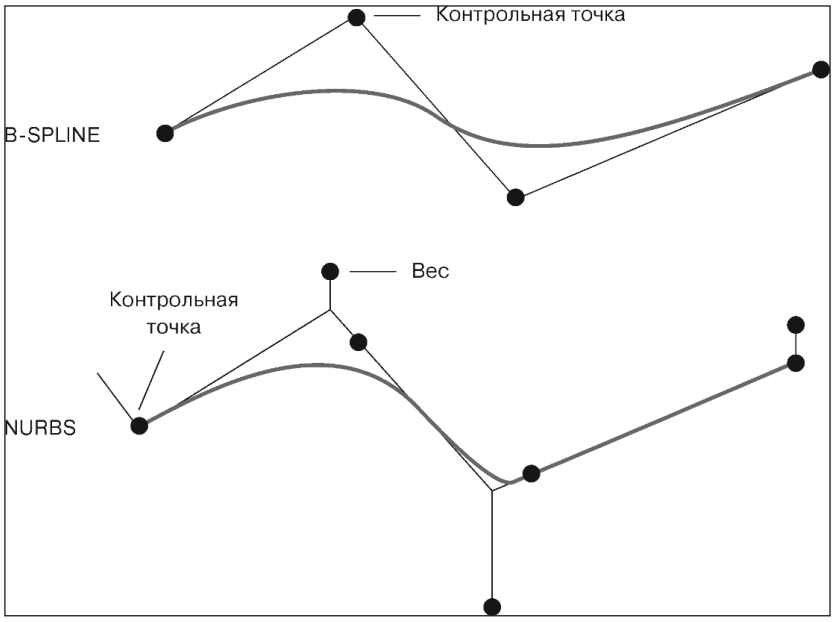

Рис. 1 – Участки кривых, описанных *B*- сплайнами и *NURBS*

Классические стеганографические методы базируются на изменении дискретных характеристик изображения – значений пикселей или коэффициентов частотных преобразований. Однако при различных преобразованиях, таких как сжатие, фильтрация или масштабирование, скрытые данные часто утрачиваются. Поэтому возникает необходимость в поиске новых типов контейнеров, где параметры данных обладают большей устойчивостью и позволяют внедрять метки с возможностью контролировать их изменение или разрушение. Одним из таких направлений является использование векторных изображений, элементы которых могут быть представлены в виде параметрических структур. Для таких изображений целесообразно использовать более сложные и взаимозависимые способы внедрения скрытых данных. Например, для изображений, которые содержат элементы в виде сплайнов, могут генерироваться дополнительные контрольные точки или незначительно изменяться их веса в некоторых отрезках кривой. В расположении таких контрольных точек может быть скрыто секретное сообщение или цифровая метка. Контроль целостности может проводиться путем скрытия контрольных сумм при помощи иных стеганографических методов в других элементах изображения.

Стеганографические преобразования оцениваются по мерам емкости, незаметности и устойчивости. Емкостью является количество бит, которое можно встроить в сообщение с соблюдением условия незаметности. Незаметность описывает требование, чтобы исходный контейнер и полученный стегоконтейнер различались как можно меньше, в том числе и при статистическом анализе. Устойчивостью называется способность противостоять атакам.

Одним из наиболее распространенных форматов в мире инженерии и промышленного дизайна является STEP (Standard for the Exchange of Product model data) – международный стандарт для обмена данными между различными системами инженерного проектирования. Главное назначение формата STEP – сохранить полную информацию о модели без потерь. Формат не является проприетарным, и может свободно использоваться различными приложениями, сохраняет точную геометрию, а также метаданные (материалы, допуски, структуру сборки, историю изготовления). Несмотря на то, что формально файл STEP – это изображение, по сути, это текстовый файл, который описывает модель на специальном языке EXPRESS. Формат поддерживает широкий спектр сущностей для отображения кривых, таких как базисные сплайны (b_spline_curve_with_knots), сплайновые

поверхности (b_spline_surface_with_knots) и более простые элементы, напрмер, окружность, эллипс, составные кривые и ломаные линии.

Основными преимуществами формата STEP являются точность, возможность использования в различном ПО и функциональность, т.к. файл может содержать и атрибутивные данные. В качестве недостатков указываются большой размер файла, отсутствие параметрической истории и сложность.

Полный STEP-файл даже для простой детали содержит сотни строк кода, причем каждая грань, ребро и вершина должны быть явно описаны. Файл формата STEP всегда начинается с секции заголовка, в которой описываются метаданные (время создания файла, автор, ПО и др.). Затем следует секция данных, в которой содержится геометрическое описание объекта. Каждая сущность имеет уникальный номер (#100, #101 и т.д.). Описываются каждая точка и каждая поверхность. В случае, если происходит комбинация элементов, например, кривая принадлежит поверхности или происходит обрезка поверхности по кривой, то описание элемента ссылается на исходный объект. Вся модель в конечном итоге собирается в твердое тело. Формат STEP представляет собой базу данных, содержащую точные математические описания всех геометрических элементов, структуру и взаимосвязи между этими элементами, метаданные.

Таким образом, можно заключить, что файлы формата STEP могут являться эффективным стеганографическим контейнером. Его структура обеспечивает естественную избыточность для внедрения данных, устойчивость к различным преобразованиям и возможность использования нескольких стеганографических методов для контроля целостности. Дальнейшие исследования должны быть направлены на разработку конкретных алгоритмов внедрения и извлечения данных, а также на экспериментальную проверку устойчивости предложенных методов к различным видам атак и преобразований файлов.

Список использованных источников

1. Урбанович П.П. Защита информации методами криптографии, стеганографии и обфускации: учебно-метод. пос. для студ. вузов / П. П. Урбанович. – Минск: БГТУ, 2016. – 219 с.
2. Блинова, Е. А. Стеганографический метод на основе встраивания скрытых сообщений в кривые Безье изображений формата SVG (Steganographic method based on hidden messages embedding into Bezier curves of SVG images) (на англ. языке) / Е. А. Блинова, П. П. Урбанович

// Журнал Белорусского государственного университета. Математика. Информатика – 2022. – № 3. – С. 68–83.

УДК 681.3

М.Ю. Боженков
Белорусский государственный технологический университет
Минск, Беларусь

ГОЛОСОВЫЕ ИИ-ТЕХНОЛОГИИ КАК ДРАЙВЕР ЦИФРОВОЙ ТРАНСФОРМАЦИИ И ЭКОНОМИЧЕСКОГО РАЗВИТИЯ

Аннотация. *В статье анализируется роль голосовых ИИ-технологий как ключевого элемента цифровой трансформации экономики. Рассматриваются принципы работы голосовых систем, их интеграция с профессиональным программным обеспечением и примеры применения в различных секторах, а также процесс обучения таких систем.*

M.Yu. Bozhenkov
Belorussian State Technological University
Minsk, Belarus

VOICE AI TECHNOLOGIES AS A DRIVER OF DIGITAL TRANSFORMATION AND ECONOMIC DEVELOPMENT

Abstract. *The article analyzes the role of voice AI technologies as a key element of the digital transformation of the economy. It examines the principles of operation of voice systems, their integration with professional software, and examples of their application in various sectors, as well as the process of training such systems.*

Информационно-коммуникационные технологии (ИКТ) занимают центральное место в процессе цифровой трансформации современной экономики, обеспечивая непрерывное развитие производственных процессов, управление данными и взаимодействие между различными секторами. В последние годы особую значимость приобретают системы искусственного интеллекта, позволяющие управлять компьютером и программными инструментами посредством голосовых команд. Такие решения формируют новое качество взаимодействия человека и цифровой среды, создавая предпосылки для глубоких изменений в экономических структурах и бизнес-моделях.

Голосовые интерфейсы, интегрированные с искусственным интеллектом, представляют собой качественно новую форму взаимодействия человека и цифровой среды. В отличие от