сельскохозяйственной продукции, а также привлечению инвестиций в аграрную сферу и восстановлению производственного потенциала АПК.

Список использованных источников

1. Геттинг Б. Международная производственная кооперация. Роль логистики в усилении конкурентоспособности хозяйственных структур. – М.: Дело, 2000. – 397с.
2. Маркова В.Д. Маркетинг услуг. М.: Финансы и статистика, 1996. - 256с.
3. Барлыбаева Н.А. Национальная инновационная система Казахстана: перспективы и механизм развития -Алматы, 2006.-199с.
4. Портер М. Конкурентное преимущество: Как достичь высокого результата и обеспечить его устойчивость/ Майкл Портер; Пер.с англ. – 2-е изд.- М.: Альпина Бизнес Букс, 2006.- 715с.

УДК 003.26

Д.М. Романенко, О.А. Новосельская,
А.Н. Щербакова, Н.А. Савчук
Белорусский государственный технологический университет
Минск, Беларусь

МЕТОД КОДИРОВАНИЯ ИНФОРМАЦИИ В ВЕКТОРНЫХ ИЗОБРАЖЕНИЯХ

Аннотация. *В статье рассмотрены принципы кодирования цветных векторных изображений, содержащих авторскую информацию для последующей ее идентификации в документах. Приведен базис кода и алгоритм кодирования в векторных изображениях на основании цвета, частоты и типа элементов изображения.*

D. M. Romanenko, O.A. Novoselskaya,
A.N. Stcherbakova, N.A.Savchuk
Belarussian State Technological University
Minsk, Belarus

INFORMATION CODING METHOD OF VECTOR IMAGES

Abstract. *The article discusses the principles of coding color vector images containing author's information for its subsequent identification in documents. The basis*

of the code and the encoding algorithm in vector images based on color, frequency and type of image elements are given.

Система защиты документов предполагает внедрение элементов, содержащих секретную (закодированную) информацию в какой-либо цифровой контейнер, например, изображение. При формировании изображений с защитой следует исходить из вида изображения и возможности его декодирования. С этой целью в рамках настоящего исследования проведен структурный анализ векторных изображений и определены механизмы генерирования кодированных переменных. Следует учитывать, что векторные изображения при их воспроизведении имеют определенные ограничения по типу линий, их цветности, передаваемой частоте. Однако с точки зрения кодирования в цифровом виде наложенные ограничения снимаются, что позволяет представить достаточно большое количество вариантов кодирования различных знаков. Кодирование авторской информации в векторных изображениях может осуществляться в виде набора линий или простых геометрических фигур с разными параметрами (тип линии, толщина линии, цвет линии, расстояние между линиями).

Формальное описание разрабатываемой системы основывается на учете взаимодействия компонентов системы, которые, в общем случае задаются элементами соответствующих множеств [1]: сообщения M ($M \in M$, M – множество всех сообщений); контейнера C ($C \in C$, C – множество всех контейнеров); ключа K ($K \in K$, K – множество всех ключей); заполненного контейнера (или защитного изображения) S ($S \in S$, S – множество всех защитных изображений).

В таком случае алгоритм кодирования авторской информации (данных) составляют два преобразования, задаваемые на основе отображений:

1) прямое преобразование F, сопоставляющее сообщению, пустому контейнеру, ключу заполненный контейнер:

$$M \times C \times K \rightarrow S; \quad (1)$$

2) обратное преобразование F^{-1}, сопоставляющее заполненному контейнеру и ключу исходное сообщение M:

$$S \times K \rightarrow M. \quad (2)$$

Причем

$$F(M, C, K) = S, \quad (3)$$

$$F^{-1} = (S, K) = M, \quad (4)$$

где $M \in \boldsymbol{M}$, $C \in \boldsymbol{C}$, $K \in \boldsymbol{K}$, $S \in \boldsymbol{S}$.

Под системой защиты документов будем понимать систему, формально описываемую выражением вида:

$$\Sigma = (F, F^{-1}, M, C, K), \quad (5)$$

и представляющую собой совокупность сообщений, секретных ключей, контейнеров и связывающих их преобразований.

Под кодированием сообщения с помощью системы Σ в контейнер C понимают применение прямого преобразования F к конкретным M, C и K. Извлечение сообщения, по сути, представляется, как применение обратного преобразования F^{-1} с теми же значениями аргументов, что и при кодировании сообщения.

Предлагаемая система основывается на принципиально новых методах генерации F векторных защитных изображений, описанных в [2]. При этом параметры генерации векторного изображения будут определяться секретным авторским ключом.

Рассмотрим общий вид ключа (K) данной системы, который будет состоять как минимум из следующих блоков, представленных в десятичном виде.

1. Блок K^1, определяющий количество и параметры линий (цвет, тип линии, толщина линии, расстояние между линиями), соответствующий каждой символу сообщений используемого алфавита (каждый отдельный параметр разделяется символом «;».

Цвет линии предлагается описывать в формате (R, G, B). Так, например, (255, 0, 0) будет означать красный цвет линии, а (0, 0, 255) – синий и т.д.

Для определения типа линии целесообразно ввести цифровые идентификаторы, представленные в таблице.

Цифровой идентификатор	Тип линии
0	————————
1	- - - - - - - - - - - - -
2	-·-·-·-·-·-·-·-·-·-
3	—··—··—··—··—

Отметим, что количество типов линий может быть увеличено, т. е. добавлены и другие типы.

Толщина линий и расстояние между линиями будет задаваться в абсолютных величинах, а именно в «пт», т. е. пунктах. При этом шаг изменения данного параметра предлагается установить равным 0,25, т. е. 0,25, 0,5, 0,75, 1 и т.д.

Таким образом, например, если блок K^1 будет иметь следующий вид А–3;(0, 0, 255);0;1;0,75, то это означает, буква «А» в векторном изображении будет представлена тремя синими сплошными линиями толщиной 1 пт и расстоянием между ними 0,75 пт.

Важно учесть при формировании ключа, что какая-либо комбинация линий, соответствующая определенному символу, используемого алфавита не должна быть началом другой комбинации линий, соответствующих другому символу алфавита. В противном случае на стадии декодирования их будет не различить.

2. Блок K^2, определяющий количество повторов сообщения в генерируемом векторном защитном изображении. Данный параметр целесообразно выбирать нечетным, что при декодировании по мажоритарному принципу определять истинное сообщение, даже если в изображении появились ошибки. Также очевидно, что данный блок должен учитывать параметр емкости векторного изображения, выражаемый в максимальном количестве сообщений, состоящих из самого «тяжелого» символа (представлен в первом блоке наибольшей геометрической шириной, зависящей от количества линий, их ширины и расстояния между ними), который может быть закодирован в изображении. Он зависит также и от геометрического размера изображения.

3. Блок K^3, определяющий вспомогательные символы, например, символ, начала сообщения, конца сообщения, повтора сообщения, начала предложения, конца предложения и т. д. Данные символы прежде всего будут выполнять вспомогательную функции для определения от какой линии и до какой необходимо выполнять декодирование (всего сообщения, отдельного предложения и т. д.).

4. В блок K^4 можно определить некоторое число комбинаций линий и их параметров, использующихся для заполнения изображения до и после закодированного изображения. Можно также предусмотреть вариант, при котором закодированное изображение будет рассматриваться как комбинация нескольких изображений (каждому авторскому сообщению в таком случае будет соответствовать одно закодированное векторного изображение), а между ними будут также использованы специальные вспомогательные символы. Данные символы, которые назовем маскирующими, должны будут выполнять задачу дорисовки защитного изображения и при этом решать проблему повышения сложности взлома ключа.

5. Очевидно, что ключ может быть расширен и иными дополнительными параметрами, например, количеством пробельных символов между словами, предложениями или за счет использования в виде отдельного символа комбинации линий с переменными параметрами, например, варьируя толщину линий, расстояния между ними. Также можно использовать линии, например, штриховые, с

варьированием цвета штрихов и т. д., что должно существенно усложнить потенциальный взлом ключа.

Далее перейдем к алгоритму кодирования авторской информации в виде защитного векторного изображения.

Алгоритм в общем случае будет сводится к следующей последовательности действий:

1. Считываются все параметры генерации защитного изображения из секретного ключа автора и определяются (или устанавливаются) геометрические размеры генерируемого векторного защитного изображения.

2. Проверяется соответствие размера одного сообщения и зафиксированного в ключе количества повторов сообщения геометрическому размеру итогового защитного векторного изображения.

3. Если установленные параметры удовлетворяют, то можно переходить к процессу кодирования (генерации) изображения. В противном случае должно быть скорректировано количество повторов сообщения в сторону уменьшения.

4. Если же размер авторского сообщения превышает возможности системы с учетом геометрических размеров генерируемого сообщения и параметров наиболее «тяжелого» символа, то пользователю выводится сообщение о необходимости уменьшения (по количеству символов) кодируемого авторского сообщения.

5. Если все параметры соответствуют требованиям, то начинается процесс генерации изображения путем отрисовки символов алфавита в виде линий, параметры которых указаны блоке K^1 ключа. При этом недостающие части изображения заполняются установленными вспомогательными (маскирующими) символами.

Процесс декодирования сводится к определению по символам начала и конца сообщения (графическое их представление извлекается из секретного ключа автора) графической области закодированного сообщения с последующим выполнением обратных операций.

В заключении необходимо отметить, что предложенный метод позволяет кодировать авторскую информацию в виде векторных изображений с последующим декодированием (извлечением), что позволит в перспективе подтверждать авторство на электронные и печатные документы.

Список использованных источников

1. Шутько, Н. П. Математическая модель системы текстовой стеганографии на основе модификации пространственных и цветовых

параметров символов текста / Н. П. Шутько, Д. М. Романенко, П. П. Урбанович // Труды БГТУ. Сер. VI: Физ.-мат. науки и информатика. – 2015. – № 6. – С. 152–156.

2. Новосельская О. А. Алгоритмы и программное средство для генерации защитных изображений печатных документов / О. А. Новосельская, Н. А. Савчук, А. Н. Щербакова, Д. М. Романенко // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. – 2022. – № 1 (254). – С. 64–72.

УДК 004.78

Д.Р. Нургалиев
Казанский национальный исследовательский
технический университет им. А.Н. Туполева
Казань, Россия

REALM. ОБЪЕКТНО-ОРИЕНТИРОВАННАЯ БАЗА ДАННЫХ ДЛЯ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Аннотация. *В данной статье рассматривается объектно-ориентированная база данных Realm. Проведен обзор и сравнение с другими технологиям, которые используются для хранения данных в мобильной разработке. В заключении показан пример того, как данная технология используется в языке программирования Swift.*

Ключевые слова: *Realm, объектно-ориентированная база данных, мобильное приложение, iOS, язык программирования Swift*

D.R. Nurgaliev
Kazan National Research Technical University
named after A.N. Tupolev
Kazan, Russia

REALM. OBJECT-ORIENTED DATABASE FOR MOBILE APPLICATIONS

Abstract. *This article discusses the object-oriented database Realm. Technologies that are used for data storage in mobile development were reviewed and compared against each other. In conclusion, an example of how this technology is used in the Swift programming language.*

Keywords: *Realm, object-oriented database, mobile application, iOS, Swift programming language.*

Введение

База данных Realm – относительно новый вид мобильной базы данных, которая была создана с нуля для поддержки современных приложений.