ОТЗЫВ

официального оппонента доктора технических наук, профессора
Листопада Николая Измаиловича
на диссертационную работу
Блиновой Евгении Александровны
«Стеганографические методы и алгоритмы защиты авторского права и обеспечения целостности электронных документов на основе языков разметки», представленную на соискание ученой степени кандидата технических наук по специальности 05.25.05 – информационные системы и процессы.

1. Соответствие содержания диссертации специальности и отрасли науки

Целью исследования является разработка и анализ новых эффективных стеганографических методов и реализующих их алгоритмов для решения задач защиты авторского права на электронные текстовые документы, изображения и электронные карты, основанные на языках разметки, а также для обеспечения целостности этих документов.

Поставленная цель достигалась путем проведения теоретических и экспериментальных исследований.

Содержание диссертационной работы Блиновой Евгении Александровны «Стеганографические методы и алгоритмы защиты авторского права и обеспечения целостности электронных документов на основе языков разметки» соответствует отрасли науки – технические и следующим пунктам паспорта специальности 05.25.05 – информационные системы и процессы:

1. Методы и модели описания, оценки, оптимизации информационных процессов и информационных ресурсов, в том числе – контента, а также средства анализа и выявления закономерностей в информационных потоках. Модели информационных систем и процессов, ориентированных на человеко-машинное взаимодействие.

4. Организационное обеспечение информационных систем и процессов, в том числе новые принципы разработки и организации функционирования информационных систем и процессов, применения информационных технологий и систем в принятии решений на различных уровнях управления, в защите прав интеллектуальной собственности на текстовые, графические или иные виды документов. Общие принципы и основы организации информационных служб и электронных библиотек.

2. Актуальность темы диссертации

Широкий круг задач, решаемых с развитием информационных систем и процессов, привело к тому, что сейчас информация является одним из важнейших видов ценностей и по этой причине возникла острая необходимость в защите этой ценности, включая защиту авторских прав и обеспечение целостности передаваемого электронного контента. Для защиты авторских прав и подтверждения целостности цифровых объектов стеганографические методы в настоящее время используются довольно часто. Однако в известных исследованиях стеганографическая система рассматривается как совокупность сообщений, файлов-контейнеров и методов по скрытию сообщений в этих файлах, причем каждый тип объектов рассматривается как единый и неделимый, В этих исследованиях, как правило, отсутствует элемент системности, не в полной мере учитываются или совсем не учитываются взаимосвязи между элементами. Известные подходы используют многие авторы, однако исследования многокомпонентной модели стеганографической системы, учитывающей связи между компонентами, в литературе практически не представлено. Все изложенное свидетельствует об актуальности темы диссертационного исследования и важности решения обозначенной проблемы. В этой связи диссертация Блиновой Е.А., направленная на разработку эффективных стеганографических методов и реализующих их алгоритмов для решения задач защиты авторского права на электронные текстовые документы, изображения и электронные карты, основанные на языках разметки, а также для обеспечения целостности этих документов является важной и представляет несомненный практический интерес.

3. Степень новизны результатов, полученных в диссертации и научных положений, которые выносятся на защиту

Полученные в диссертационной работе Блиновой Е.А. результаты обладают научной новизной, которую можно сформулировать следующим образом:

- впервые с системных позиций сформулирована концепция компонентной стеганографической системы, отличающейся от известных представлением контейнера, ключей и скрытого сообщения в виде набора связанных между собой компонентов, что позволило более корректно описать логические связи между компонентами системы и происходящими процессами;

- новизна предложенного подхода и его математического описания в виде связанных множеств состоит в представлении стеганографической системы в виде совокупности сообщений, файлов-контейнеров, многокомпонентного набора ключей, а также преобразований для разбиения контейнера на компоненты, сообщения – на блоки, вычисления контрольного значения, внедрения и извлечения сообщения, что обеспечило возможность использования различных ключей для скрытия блоков сообщения в разных компонентах;

- обоснованы новые подходы в реализации многокомпонетной стеганографической системы, отличительные особенности которой состоят в дополнении сообщения, осаждаемого в стеганоконтейнер, блоком, представляющим собой вычисленную контрольную сумму осаждаемого сообщения; в поблочном разделении осаждаемого сообщения в соответствии с подобным секционированием исходного стегоконтейнера; в многократном дублировании процедуры размещения сообщения в различных блоках стегоконтейнера;

- новым является предложенная автором идея использования дополнительных пространственно-геометрических параметров электронных текстовых документов, изображений и электронных карт, основанных на языках разметки, модификация которых позволило скрывать тайную информацию для защиты авторского права и контроля целостности электронного контента.

4. Обоснованность и достоверность выводов и рекомендаций, сформулированных в диссертации

Обоснованность и достоверность выводов и рекомендаций, сформулированных в диссертации, основывается на корректном использовании аппарата теории множеств, теории информации, математического описания файлов формата SVG с помощью кривых Безье второго и третьего порядков, применении метода разбиения де Кастельжо для внедрения скрытого изображения.

Достоверность полученных результатов подтверждается представленными в главе 4 примерами применения разработанных программных продуктов SpaceQuoteStego и StegoSVG.

5. Научная, практическая, экономическая и социальная значимость результатов с указанием рекомендаций по их использованию

Научная значимость результатов диссертации состоит в обосновании и

развитии концепции многокомпонентной стеганографической системы, основанной на ключевой информации в виде стегонаборов, отличающейся аналитическим представлением стеганографического контейнера, ключевой информации и скрытого сообщения в виде наборов компонентов, ключевых уровней и блоков, что позволило решать задачи защиты прав интеллектуальной собственности на электронный контент.

Практическая значимость результатов диссертации состоит в разработке и импортозамещающих компьютерных программ, позволяющих практически реализовать скрытие и извлечение цифровых меток из электронных текстовых документов, изображений и электронных карт, основанных на файлах разметки.

Практическая значимость результатов исследования подтверждается актами и справками о внедрены и использовании в Республиканском унитарном предприятии «Научно-производственный центр по геологии», а также в учебном процессе УО «Белорусский государственный технологический университет».

Экономическая значимость результатов состоит в повышении эффективности и снижении затрат на разработку импортозамещающих программных продуктов для защиты права интеллектуальной собственности, для тайной передачи сообщений с возможностью контроля целостности, а также может служить методической и информационной основой для расширения и углубления исследований по решению прикладных задач в данной предметной области.

Социальная значимость полученных результатов состоит в повышении качества подготовки специалистов в области защиты информации и авторских прав на электронные издания, а также защите контента электронных образовательных ресурсов.

6. Полнота опубликования основных положений, результатов диссертации в научной печати

Основные положения и результаты диссертационных исследований в достаточной степени опубликованы в научной печати. По результатам выполненных исследований опубликовано 36 печатных работ, в том числе: 8 статей в научных изданиях, соответствующих требованиям п. 19 Положения о присуждении ученых степеней и присвоении ученых званий, из которых 2 – на английском языке (Scopus), тезисы 28 докладов и материалов конференций, 4 свидетельства о регистрации компьютерных программ. Без соавторов опубликовано 7 работ.

7. Соответствие оформлению диссертации требованиям ВАК.

Оформление диссертации и автореферата соответствует требованиям Инструкции о порядке оформления диссертации, диссертации в виде научного доклада, автореферата диссертации и публикаций по теме диссертаций, утвержденной Постановлением ВАК Республики Беларусь от 28.02.2014 № 3 (в редакции от 22.08.2022 № 5). Разделы «Общая характеристика работы» и «Заключение» автореферата дословно воспроизводят соответствующие разделы диссертации без изъятий и дополнений. Содержание автореферата полностью соответствует положениям и выводам, изложенным в диссертации.

8. Недостатки диссертации

Несмотря на достаточно высокий научный уровень, несомненную новизну и практическую полезность, работа не лишена некоторых недостатков. К ним можно отнести следующие.

1. Глава 2 диссертации посвящена результатам математического моделирования стеганосистемы на основе аппарата теории множеств. Представлены достаточно сложные математические модели компонентной стеганографической системы. В конечном счете стеганосистемма S представлена в виде выражения 2.21, в которое входят 8 взаимосвязанных компонент: множество стеганоконтейнеров, множество сообщений, множество стеганонаборов, набор преобразований для вычисления контрольных чисел, функция сокрытия сообщения и функция извлечения сообщения. Реализация на практике такой стеганосистемы представляется достаточно сложной задачей с учетом всех входящих компонент. В этой связи возникает вопрос эффективности функционирования стеганосистемы, описанной выражением 2.21. Представленные в главе 4 результаты оценки системы, проведенные с участием студентов для некоторых частных случаев, не могут быть основой для обобщающих выводов. При проведении подобных исследований стеганоаналитиком скорее всего выводы были бы несколько другими. В этой связи вопросы эффективности требуют дополнительного, прежде всего теоретического, обоснования: будет ли обеспечена защита авторских прав, если в стеганографической системе 2.21 злоумышленник, например, получит информацию об одном из ключей? Как будет функционировать система 2.21, если будут измены ее другие компоненты? Какой компонент данной системы является наиболее критичным с точки зрения защиты авторских прав и

обеспечения целостности?

2. На стр.41 приводится определение стеганонабора и далее на рис.2.1 представлена общая схема выбора стеганонабора. Ключи K_1, K_2 и K_3 представлены в виде матрицы 3Х4 K_1 и далее матриц 2Х2 K_2 и 2Х2 K_3. Не очень понятно, как были сформированы матрицы и отсюда как производится выбор стеганонабора.

3. В главе 3 достаточно много уделяется внимания кривым Безье, описывается применение метода разбиения де Кастельжо для внедрения скрытого сообщения, показано, как разбивается отрезки, формируются опорные и контрольные точки. При этом вводятся целый ряд обозначений, которые требуют обоснования, Например, на стр.65 мы имеем следующее:

Введем следующие обозначения: $t_0 = 1 - \tau$; $t_1 = t_0^3$; $t_2 = 3t_0^2\tau$; $t_3 = 3t_0\tau^2$; $t_4 = \tau^3$

Обоснований такого введения не представлено, что не позволяет в полной мере оценить достоверность и корректность последующего анализа.

4. В главе 4 и в заключении диссертации упоминается разработанная экспертная система прогнозирования последствий пролива нефтепродуктов, в которой приняты и введены в эксплуатацию стеганографический метод, алгоритмы и процедуры защиты авторских прав и подтверждения целостности электронных карт в базе данных. Из представленной информации не до конца понятно, что же конкретно разработано и внедрено: карты, база данных или может быть вся экспертная система.

5. В работе имеются неточности, например, на стр.61 «Для отображения кривых второго порядка применяются операторы ***Q*** и ***T***, для отображения кривых второго (*видимо, третьего*) порядка применяются операторы ***C*** и ***S***», есть некоторые опечатки.

Вместе с тем приведенные недостатки не влияют на суть положений, выносимых на защиту, а также на научную и практическую ценность полученных результатов, а часть из них может рассматриваться как направление дальнейших исследований.

9. Соответствие научной квалификации соискателя ученой степени, на которую он претендует

Диссертация Блиновой Е.А. является самостоятельной завершенной научно-квалификационной работой, в которой решена важная научно-техническая задача защиты прав интеллектуальной собственности на электронный контент за счет использования многокомпонентной стеганографической системы, отличающейся аналитическим представлением

стеганографического контейнера, ключевой информации и скрытого сообщения в виде наборов компонентов, ключевых уровней и блоков.

Диссертация выполнена на высоком научно-техническом уровне и полностью отвечает требованиям Положения о присуждении ученых степеней и присвоении ученых званий, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук.

Содержательная часть диссертации Блиновой Е.А., сформулированные выводы, положения, выносимые на защиту, и рекомендации по практическому использованию результатов исследования показывают, что соискатель владеет всеми требуемыми навыками, предъявляемыми по специальности 05.25.05 – информационные системы и процессы.

10. Заключение

Диссертационная работа Блиновой Е.А., выполненная под научным руководством доктора технических наук, профессора Урбановича П.П., является законченной научной квалификационной работой.

Исследования автора лежат в области развития теории и практики методов защиты прав интеллектуальной собственности путем использования многокомпонентных стеганографических систем, имеют четкую практическую направленность и полностью соответствуют отрасли наук и специальности 05.25.05, по которой диссертация представлена к защите.

Текст диссертации и автореферат оформлены в соответствии с требованиями ВАК Республики Беларусь к диссертационным работам. Научные конференции и семинары, на которых докладывались и обсуждались результаты исследований, достаточны для объективной оценки этих результатов.

Таким образом, диссертационная работа Блиновой Евгении Александровны «Стеганографические методы и алгоритмы защиты авторского права и обеспечения целостности электронных документов на основе языков разметки» соответствует требованиям, предъявляемым к кандидатским диссертациям. Диссертация обладает внутренним единством, содержит новые научные результаты и свидетельствует о личном вкладе автора в науку.

Автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.25.05 за новые научно обоснованные результаты теоретических и прикладных исследований, обеспечивающих разработку эффективных стеганографических методов и реализующих их алгоритмов для решения задач защиты авторского права на электронные текстовые документы, изображения и электронные карты, включающие:

- математическую модель компонентной стеганографической системы с использованием аппарата теории множеств в виде совокупности сообщений, контейнеров, содержащих выделенные компоненты, трехуровневого ключа, а также преобразований для внедрения и извлечения тайного сообщения, отличающееся от известных более высокой степенью детализации, что обеспечило возможность адаптации системы под решение широкого круга узкоспециализированных задач;

- метод и алгоритмы прямого и обратного стеганографических преобразований информации на основе языков разметки, отличающиеся тем, что встраиваемая в контейнер информация и ее контрольная сумма распределены по компонентам контейнера с учетом его параметров, что позволяет повысить стеганографическую стойкость системы не менее, чем в 4 раза;

- стеганографический метод на основе встраивания дополнительных значений координат в географические электронные карты, позволяющий связать отдельные пространственные области для обеспечения целостности электронных карт, отличающийся от известных тем, что связывает, по аналогии с концепцией блокчейн, пространственные области между собой, что обеспечивает более высокий уровень защищенности электронных карт от несанкционированной модификации.

Официальный оппонент
заведующий кафедрой информационных
радиотехнологий учреждения образования
«Белорусский государственный университет
информатики и радиоэлектроники»,
доктор технических наук, профессор Н.И.Листопад

Поступил в совет 05.11.2024
Э.К. Сенько

Ознакомлена
06.11.2024
Е.А. Белякова