Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

На правах рукописи

УДК 004.056-028.23

ШЕВЧЕНКО
Кристина Валерьевна

МЕТОДЫ И АЛГОРИТМЫ ЗАЩИТЫ ВИДЕОДАННЫХ

АВТОРЕФЕРАТ
диссертации на соискание степени
магистра техники и технологий

по специальности 1-39 81 01 – Компьютерные технологии
проектирования электронных систем

Минск 2017

Работа выполнена на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **МАТЮШКОВ Владимир Егорович,**
доктор технических наук, профессор, главный инженер ОАО «КБТЭМ-ОМО»

Рецензент: **КАЗЕКА Александр Анатольевич**
кандидат технических наук, доцент, начальник отдела студенческой науки и магистратуры учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Защита диссертации состоится «22» июня 2017 г. года в $10^{\underline{00}}$ часов на заседании Государственной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, Минск, ул. П.Бровки, 6, копр. 1, ауд. 415, тел. 293-20-80, e-mail: kafpiks@bsuir.by

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

ВВЕДЕНИЕ

Информация является одной из ценнейших областей современной жизни. Получение доступа к ней с появлением глобальных компьютерных сетей стало невероятно простым. В то же время легкость и скорость такого доступа значительно повысили и угрозу нарушения безопасности данных при отсутствии мер их защиты. В связи с этим, все чаще возникает вопрос защиты данных от хищения, искажения и незаконного использования. Особый интерес представляет защита видеоданных как одного из самых востребованных в настоящее время видов данных. Системы, в которых хранятся данные видеонаблюдения, становятся все более и более связанными с локальными и глобальными сетями.

Передача видеоданных в компьютерных сетях, включая сеть Интернет, является важнейшей составляющей информационного потока для многих современных мультимедиа-приложений. Они включают в себя различные системы мониторинга, наблюдения, видеотелефонии, персонализированное телевизионное вещание, и многие другие системы.

В зависимости от сферы применения видеоданных, выбираются и соответствующие способы из защиты, поэтому актуальным становится выбор методов для построения конкретной системы защиты.

Для видеоданных проблема защиты от хищения, искажения и незаконного использования имеет свои существенные особенности. Защита видеоинформации требует учета специфики ее структуры, а также алгоритмов, используемых для сжатия и передачи видео.

Одной из основных проблем защиты видеоданных является объём передаваемой информации. При использовании цифровой видеосвязи общая задержка в канале связи не должна превышать 150 мс , причём это суммарная задержка, которая учитывает не только шифрование/дешифрование конфиденциальных данных, но и сжатие – передачу – приём – разжатие – отображение. И чем меньшие накладные расходы вносит шифрование/дешифрование, тем лучше. Таким образом, успешное решение задачи защиты видеоданных возможно с учётом целого комплекса проблем, в том числе и в смежных областях.

С точки зрения безопасности, необходимо также иметь возможность оценить экономический аспект введения защитных механизмов. Не любая информация нуждается в высокой степени защиты, для каждой необходимо подобрать свой уровень конфиденциальности. Под устойчивостью защиты видеоинформации в данной работе понимается способность сохранять состояние защищенности под воздействием случайных и преднамеренных искажений.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Актуальность исследований заключается в решении научно-технической проблемы защиты видеоданных при обработке, хранении, передаче и распространении в условиях угроз, приводящих к потере и модификации информации.

Степень разработанности проблемы

Исследования защиты видеоданных решались на основе построения теоретических моделей с использованием работ российских и белорусских ученых: Грибунин В.Г., Коржик В.И., Оков И.Н., Аграновский А.В., Хади Р.А., а также в работах иностранных ученых Симонс Г., Качин С., Фридрич Дж., Моулин П., Йохансон Т. Встраивание стегосообщения в сжатое видео содержится в работах Коха, Бенхама Д., Лангелаара. Встраиванием стегосообщения в несжатое видео занимались такие авторы, как Куттер М., Питас И.А.

Цель и задачи исследования

Целью диссертации является разработка и исследование методики защиты цифровых видеоданных с использованием цифрового водяного знака и методики перестановки блоков как механизма защиты видеоданных.

Поставленная цель работы определяет следующие основные задачи:

1. Провести обзор и анализ методов и алгоритмов защиты видеоданных, их методы сжатия и шифрования, провести обзор технологий внедрения цифрового водяного знака в видеоданные.

2. Разработать методику защиты видеоданных с использованием цифрового водяного знака, и выявить основные отличия от методики перестановок блоков.

3. Провести сравнительный анализ производительности и эффективности выбранных способов защиты видеоданных, определить пределы применения разработанных методик и сформировать практические рекомендаций для применения.

Область исследования

Содержание диссертации соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-38 81 01 «Компьютерные технологии проектирования электронных систем».

Теоретическая и методологическая основа исследования

В основу диссертации легли работы белорусских и зарубежных ученых в области изучения алгоритмов и методов защиты видеоданных, а также анализ технических нормативных правовых актов по рассматриваемой тематике.

Информационная база исследования сформирована на основе литературы, открытой информации, технических нормативно-правовых актов, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

Научная новизна

Научная новизна и значимость полученных результатов работы заключается в сравнении методики защиты видеоданных с помощью технологий цифрового водяного знака и методики перестановки блоков как механизма защиты видеоданных и выявление основных отличий исследуемых методик.

Теоретическая значимость работы заключается в детальном анализе выбранных методик защиты.

Практическая значимость определяется тем, что предложенные в ней методики защиты видеоданных позволяют обеспечить целостность и защищенность передачи видеоданных в системах связи, а также в возможности создания новых методик защиты видеоданных.

Основные положения, выносимые на защиту

1. Систематизация методов защиты видеоданных, основанная на анализе стандартов сжатия и алгоритмах шифрования, позволившая более детально описать процесс внедрения цифрового водяного знака в видеопоток.
2. Алгоритм шифрования видеоданных на основе перестановки блоков исходных данных по таблице перестановок.
3. Методики скрытого встраивания изображения в видеоданные случайными частями – с помощью логического суммирования и с помощью замены.

Апробация диссертации и информация об использовании ее результатов

Результаты исследований, вошедшие в диссертацию, докладывались и обсуждались на 53-ой научно-техническая конференции аспирантов, магистрантов и студентов БГУИР (Минск, Беларусь, 2017 г.).

Публикации

Изложенные в диссертации основные положения и выводы опубликованы в 4 печатных работах.

Общий объем публикаций по теме диссертационной работы составляет 0,57 авторских листа.

Структура и объем работы

Диссертация состоит из введения, общей характеристики работы, трех глав с краткими выводами по каждой главе, заключения, библиографического списка и приложений.

В первой главе приведен обзор методов сжатия видеоданных, оценки их качества и с состояния проблемы защиты видеоданных.

Во второй главе представлена методика защиты видеоданных с использованием цифрового водяного знака и методика перестановок блоков как механизма защиты видеоданных.

В третьей главе представлен сравнительный анализ производительности и эффективности выбранных способов защиты видеоданных. Определены пределы применения разработанных методик. Сформированы практические рекомендаций для применения предложенных методик обеспечения целостности видеоданных.

В приложении представлены публикации автора и акт внедрения.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы, определяется цель и решаемые задачи, излагаются научная новизна, практическая ценность.

В **общей характеристике работы** показана актуальность проводимых исследований, степень разработанности проблемы, сформулированы цель и задачи диссертации, обозначена область исследований, научная (теоретическая и практическая) значимость исследований, а также апробация работы.

В первой главе рассмотрены основные свойства, присущие современным видеоданным, обозначены задачи обеспечения защиты передаваемой и обрабатываемой информации от несанкционированного доступа. Проанализированы основные алгоритмы сжатия информации, а также конкретные стандарты сжатия видеоданных, селективные методы кодирования видеоинформации. Сделан вывод, что на основе селективных методов создать гарантированно стойкую защиту невозможно. Это связано с тем, что внутренний формат видеоинформации после сжатия сохраняет сложные взаимосвязи между своими элементами. Эти взаимосвязи облегчают злоумышленнику криптоанализ защищенного видеоконтента. При существенном нарушении данных взаимосвязей (для увеличения стойкости), падает степень сжатия видеоинформации, увеличивается количество данных, подлежащих зашифровке, что в свою очередь снижает преимущества применения селективного шифрования.

Был выполнен анализ потенциальных угроз нарушения целостности видеоданных**.** На основе выполненного анализа сформирована модель угроз целостности видеоинформации с классификацией по критериям изображённая на рисунке 1:

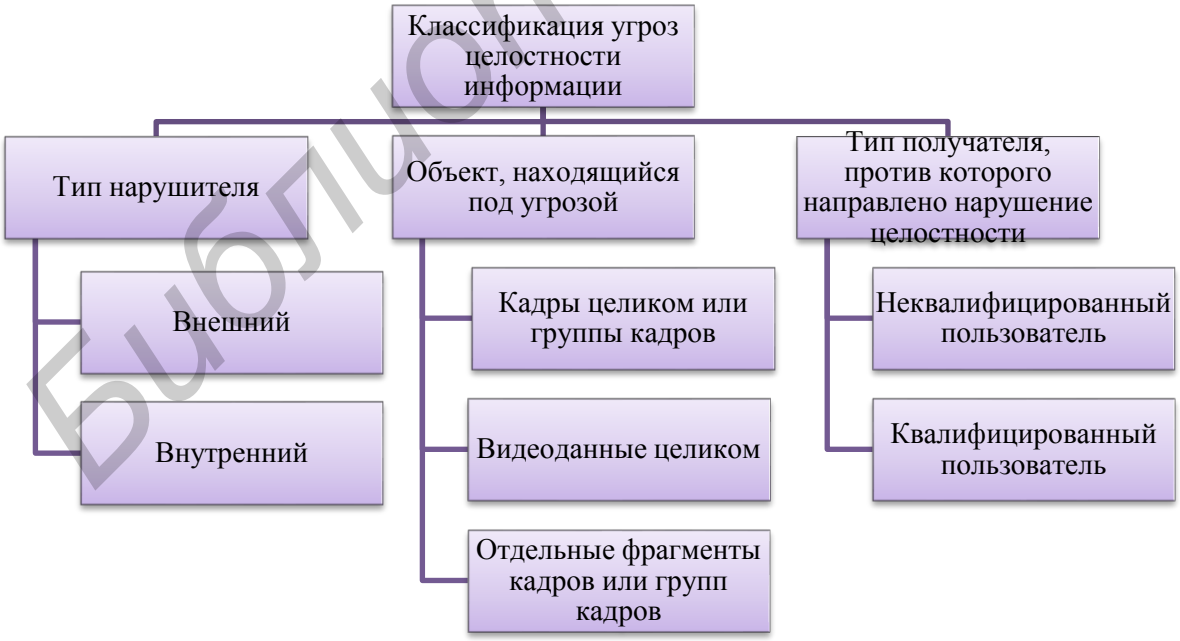

Рисунок 1 – Модель угроз целостности видеоинформации с классификацией по критериям

Проанализирован вопрос качества изображения как одной из характеристик видеоданных. Применительно к сжатию видеоданных, качеством изображения называется характеристика сжатого видеопотока при визуальном сравнении с оригиналом. Возможны два подхода к оценке качества изображений: количественная оценка с помощью использования математических методов (среднеквадратиче-ская ошибка, Lp-норма, меры, учитывающие особенности восприятия изображения зрительной системой человека) и субъективная оценка на основе экспертных оценок. На рисунке 2 изображена классификация оценок качества изображения.

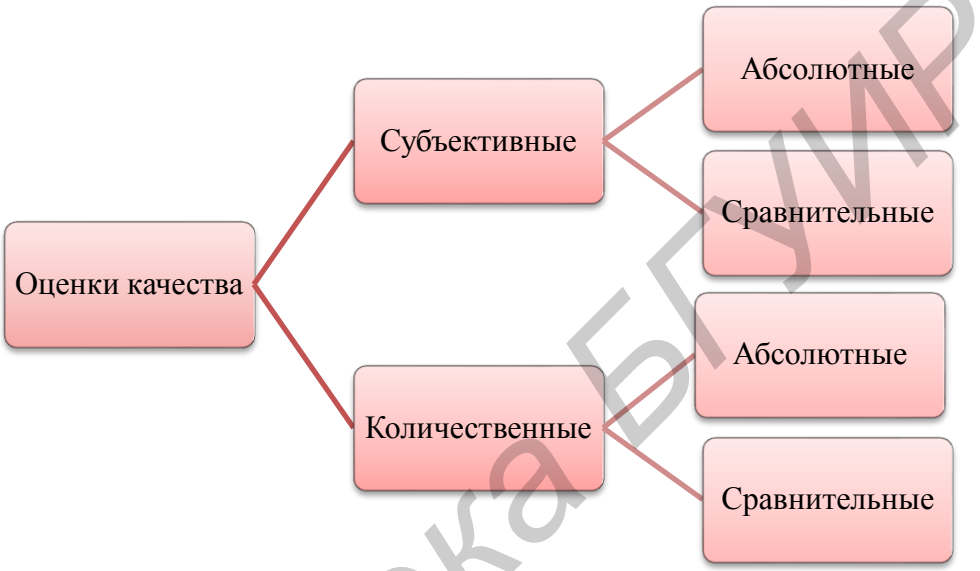

Рисунок 2 – Классификация оценок качества изображения

Проведено исследование существующих известных моделей и методов защиты целостности видеоинформации. В ходе данного исследования была определена требуемая научная задача.

Были рассмотрены понятия, относящиеся к стеганографии как к науке. Приведена их краткая классификация стегосистем и обзор. Рассмотрены основные свойства стегосистемы. Встраивать стегосообщения в видеофайл возможно на нескольких этапах преобразования. Выделяется четыре возможных уровня встраивания стегосообщения.

Первый уровень – скрытое встраивание данных в пространственной области кадров (несжатое видео).

Второй уровень – уровень коэффициентов дискретного косинусного преобразования (ДКП), когда информация скрывается за счет изменения значений коэффициентов либо соотношения между ними.

Третий уровень – уровень квантованных коэффициентов ДКП, встраивание производится после квантования.

Четвертый уровень – уровень кода переменной длины или уровень битовой области.

Во второй главе разрабатываются методики скрытого встраивания изображения в видеоданные случайными частями. Для защиты видеоданных требуется обеспечить низкую робастность водяного знака, чтобы цифровой водяной знак легко удалялся при малейшем воздействии на видео, как-то: сжатие, перерисовка, масштабирование, так как эти воздействия могут служить признаком изменения контента. Водяной знак должен минимально искажать видео, чтобы максимально сохранить его целостность. Система должна обладать определенной стойкостью, обеспечивающей защиту хотя бы от простейшего стегоанализа, такого, как визуальный осмотр контента или побитовый просмотр. Это необходимо для исключения фальсификации уже самого водяного знака.

Встраивание скрытой информации в младшие значащие биты последовательности-контейнера является одним из базовых приемов стеганографии. Новизна методик заключается в осуществлении математических операций между методом младших значащих бит (МЗБ) и псевдослучайной последовательностью таким образом, чтобы минимально изменять распределение МЗБ пикселей каждого отдельного кадра, делая заметным статистические изменения лишь в сумме массивов МЗБ пикселей кадров. Данные статистические изменения служат для декодирования сообщения. Такого рода встраивание делает алгоритм устойчивым к побитовому просмотру видеофайла и к покадровому статистическому стегоанализу. Видеофайл, в который осуществляется встраивание, имеет формат RGB, т.е. каждый его пиксель описывается тремя байтами, каждый из которых соответствует красному, синему и зеленому цвету. Необходимо в данный видеофайл внедрить изображение, не превышающее по геометрическому размеру кадр видеофайла, каждый пиксель которого описывается 1 битом (т.е. черный или белый цвет).

Изменения в младшем значащем бите незаметны для человеческого глаза, поэтому его можно использовать для встраивания информации. В таблице 1 приведено сравнение существующих методов встраивания ЦВЗ.

Таблица 1 – Сравнение существующих методов встраивания ЦВЗ.

Вид ЦВЗ	Мера искажения видео (PSNR)	Робастность к сжатию с потерями
Встраивание в коэффициенты ДКП	54	Да
Встраивание в пространственной области (не МЗБ)	133	Да
Классический метод МЗБ	180	Нет

Для того чтобы встроить изображение в видеоданные, можно применить стандартную модификацию МЗБ. Но существуют программы, позволяющие осуществлять побитовый просмотр изображения. В этом случае возможно несанкционированное обнаружение встроенного изображения. Кроме этой, существуют другие различные методики *стегоанализа — анализа мультимедийного контента в целях обнаружения скрыто встроенных сообщений.*

Рассмотрим последовательность кадров-изображений, каждый из которых можно представить, как совокупность трех матриц цвета с размерностью кадра видеофайла. Цвет для встраивания информации будет синий. Предполагается, что плотность единиц в массиве МЗБ равна 0,5.

Создается маска – случайная часть изображения. Она представляет собой массив из нулей и единиц с размерностью изображения. При этом элементы маски, соответствующие белым точкам (нулевым элементам) изображения, заполняются нулями. А элементы маски, соответствующие черным точкам, заполняются последовательностью, единицы в которой распределены случайным образом, но их плотность в последовательности задается заранее. Для создания маски можно использовать генератор случайных чисел.

Встраивание осуществляется путем осуществления поэлементных битовых операций между МЗБ и масками в месте встраивания изображения. Встраивание осуществляется в группу кадров, число которых мы называем *периодом встраивания.* Для каждого кадра из периода встраивания создается новая маска. Символически процесс встраивания изображен на рисунке 3.

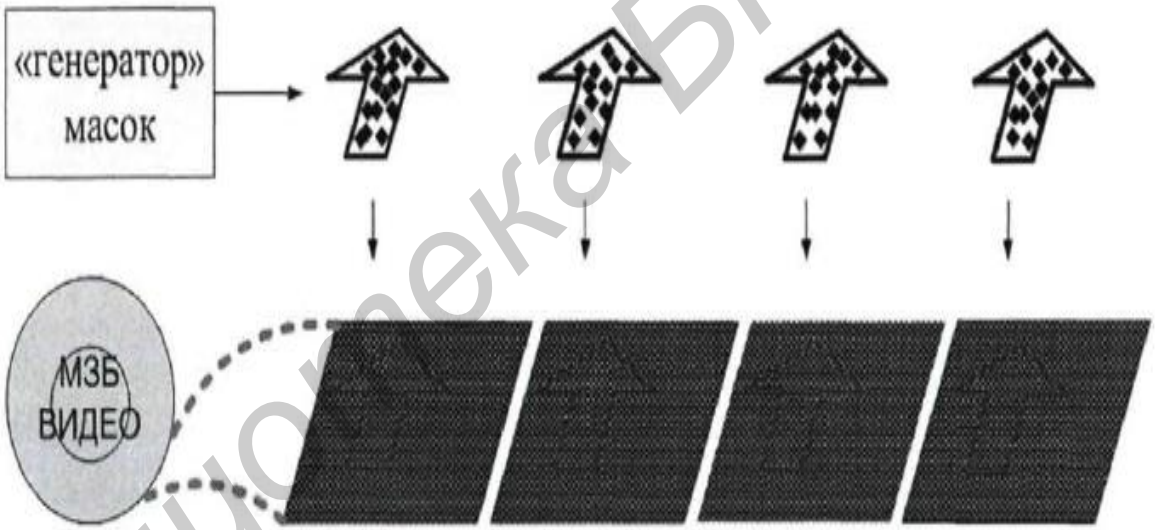

Рисунок 3 – Встраивание ЦВЗ в группу кадров

Выберем место встраивания картинки в кадре. Между каждым битом МЗБ и битом маски, соответствующей данному кадру, в месте встраивания изображения осуществляется операция:

$$Is_{h_0+i,w_0+j} = ms_{i,j} \vee Is_{h_0+i,w_0+j} \qquad (1)$$

Функциональная схема стегосистемы при встраивании изображения случайными частями с помощью логического суммирования изображена на рисунке 4.

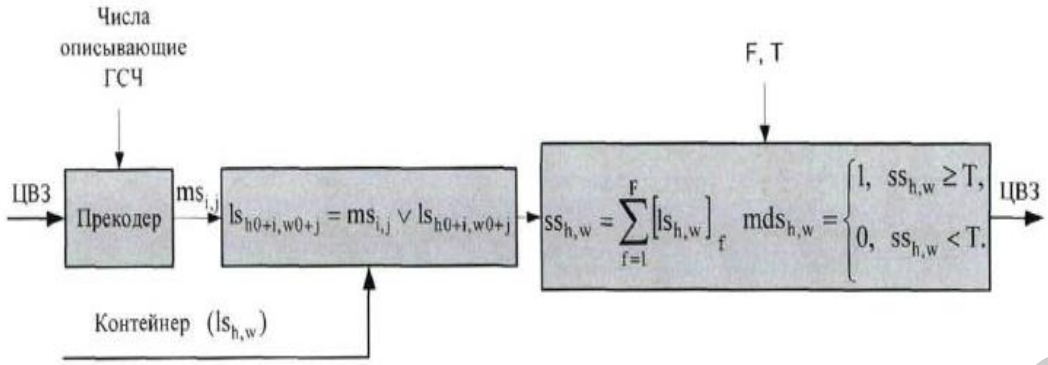

Рисунок 4 – Функциональная схема стегосистемы при встраивании изображения случайными частями с помощью логического суммирования

Второй методикой закрытия видеоданных и в целях предотвращения снижения коэффициента сжатия, предлагается использовать перестановку блоков исходных данных по таблице перестановок.

Таблица перестановок представляет собой одномерный массив индексов, служащий для отображения одного одномерного массива в другой. При этом массив индексов является ключом для восстановления переставленного массива, а сама операция перестановки (как прямой, так и обратной) является очень простой обработкой входных данных, не требующей значительных вычислительных ресурсов.

В отличии от алгоритмов шифрования на базе криптографических алгоритмов, таблица перестановок позволяет вносить определенные ограничения в процесс её формирования, тем самым давая возможность управлять степенью искажения исходного массива. Это конечно, снижает стойкость преобразования, однако придаёт такому преобразованию новые свойства.

При получении таблицы перестановок, можно использовать генератор псевдослучайных чисел, отбрасывая повторные элементы. Однако большинство таких генераторов обладают одним существенным недостатком — при вычислении нескольких элементов последовательности, можно вычислить все последующие, а в некоторых случаях и все предыдущие элементы.

Поэтому для формирования таблицы перестановок, необходимо использовать безопасный генератор псевдослучайных чисел, генерирующий последовательности, зависящие от секретного ключа и затрудняющие восстановление всей последовательности по известной её части. Для этого предложено использовать 2 метода получения псевдослучайных чисел — метод Фибоначчи с запаздываниями и метод использования блочного шифра в режиме счётчика.

При выборе блока изображения, подлежащего перестановке, предлагается использовать (в зависимости от места её выполнения) либо произвольный блок изображения подходящего размера (поиск оптимального размера является отдельной исследовательской задачей), либо блок равный размеру внутреннего BCT-блока алгоритма сжатия.

В третьей главе произведен анализ разработанных методик зашиты видеоданных. Определены пределы применения предложенных в работе методик, описана регулировка степени искажения контейнера, приведены модификации методик встраивания. В процессе определения пределов применения методик разработано достаточное условие обнаружения бинарного сигнала в бинарном шуме посредством корреляционного приемника. Для оценки эффективности предложенных стегосистем необходимо определить, насколько эти системы искажают контейнер.

Суть модернизации метода защиты видеоданных путем встраивания изображения в видеоданные случайными частями заключается во встраивании части изображения не в каждый кадр, а в один из следующих, выбранный случайно. Схема встраивания изображения не в каждый кадр, а в выбранный случайно изображена на рисунке 5.

Рисунок 5 – Схема встраивания изображения не в каждый кадр, а в выбранный случайно

При этом вероятность появления единицы в элементе кадра второго вида при встраивании изображения в видеопоследовательность с помощью логического суммирования будет равна выражению:

$$P_{sis} = \frac{(n \cdot P_{ls} + P_{ms} - P_{ls} \cdot P_{ms})}{n} \qquad (2)$$

Таким образом, не зная ключа, т.е. параметров генератора, определяющего, в какие кадры встраивается изображение, процесс обнаружения перебором значений порога усложняется.

Так же была описана возможность встраивания в видеокодек перестановки блоков перед статистическим сжатием. Для этого рассматривается порядок обработки блоков изображения видеокодеком. Вначале выполняется преобразование цветового пространства (из RGB в YUV, например). Затем производится разбивка на макроблоки - блоки значений компонент каждого цвета определённой размерности, например, 8x8 или 16x16. При этом производится процедура субдискретизации, если это необходимо.

В ходе дальнейшей обработки содержимое макроблоков преобразуется с помощью дискретного косинусного преобразования (ВСТ) и производится операция квантования, когда каждый элемент макроблока • делится на коэффициент квантования. В дальнейшем процессе сжатия происходит поиск оптимальных векторов движения, когда для каждого макроблока в некоторой пространсгвенно-

ограниченной области производится поиск наиболее похожего на него блока и в случае нахождения такого блока, операция квантования производится над разницей между самим блоком и найденным наиболее похожим на него. В результате получается структура данных, которая является промежуточной для дальнейшего сжатия энтропийными кодами.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Выполнен анализ существующих методов защиты видеоданных, приведен обзор методов сжатия видеоданных, оценки их качества и современного состояния проблемы защиты видеоданных.

2. Разработана методика встраивания цифрового водяного знака в видеопоток случайными частями и методика защиты видеоданных с использование перестановок блоков.

3. В результате разработки методик была высчитана эффективность выбранных методик защиты видеоданных, определены приделы применения, сформированы практические рекомендации для применения.

Рекомендации по практическому использованию результатов

Полученные результаты внедрены в учебный процесс на кафедре проектирвоания информационно−компьютерных систем учреждения образования “Белорусский государственный университет информатики и радиоэлектроники” в учебные курсы: «Методы и технические средства обеспечения безопасности» и «Основы защиты информации».

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Тезисы конференций

1. Шевченко К.В. Методы и алгоритмы защиты видеоданных в формате MPEG от несанкционированного доступа / К.В. Шевченко // Новые информационные технологии в научных исследованиях: материалы XXI Всероссийской научно-технической конференции студентов, молодых ученых и специалистов, Рязань, Российская Федерация / ФГБОУ ВО «РГРТУ». – Рязань. 2016. –396–398.

2. Шевченко К.В. Алгоритмы шифрования Data Encryption Standard (DES) и Advanced Encryption Standard (AES) / К.В. Шевченко // Новые информационные технологии в научных исследованиях: материалы XXI Всероссийской научно-технической конференции студентов, молодых ученых и специалистов, Рязань, Российская Федерация / ФГБОУ ВО «РГРТУ». – Рязань. 2016. –398–399.

3. Цырельчук А.И., Методы и алгоритмы внедрения цифрового водяного знака в видеопоток/ А.И. Цырельчук, К.В. Шевченко, // Современные проблемы радиоэлектроники и телекоммуникаций, РТ-2016: материалы 12-я Международной молодежной научно-технической конференции, Севастополь, Российская Федерация / ФГБОУ ВО «СевГУ». – Севастополь. 2016. –161.

4. Шевченко К.В. Методы защиты целостности видеоданных / К.В. Шевченко // Современные проблемы радиоэлектроники и телекоммуникаций, РТ-2016: материалы 12-я Международной молодежной научно-технической конференции, Севастополь, Российская Федерация / ФГБОУ ВО «СевГУ». – Севастополь. 2016. – 160.

РЭЗЮМЭ

Шаўчэнка Крысціна Валер'еўна

Метады і алгарытмы абароны відэададзеных

Ключавыя словы: лічбавы вадзяной знак, метады абароны відэададзеных.

Мэта працы: вывучэнне і вызначэнне актуальных алгарытмаў і метадаў абароны відэададзеных. Для дасягнення названай мэты вырашаюцца задачы дасле-вання асноўных прынцыпаў функцыянавання сістэм перадачы відэададзеных, вы-з'яўляюцца ўразлівасці найбольш распаўсюджаных графічных фарматаў і прад-лага методыка выбару метаду абароны відэаструменю, якая ўлічвае ўласцівасці гэтых фарматаў.

Атрыманыя вынікі і іх навізна: навуковая навізна і значнасць паў-атрыманых вынікаў работы заключаецца ў параўнанні методыкі абароны відэададзеных з дапамогай тэхналогій лічбавага вадзянога знака і методыкі перастаноўкі блокаў як механізму абароны відэададзеных. Сфармуляваны патрабаванні да циф-ровому вадзяніку знаку для абароны відэададзеных. Вывучаны методыкі ўбудавання лічбавага вадзянога знака ў відэаструмень. Вывучаны метады абароны відэаінфарма-цыі з розным узроўнем прыватнасці. Даследаваны метад фарміравання псеўдавыпадковых паслядоўнасці па сакрэтнай ключу, які можа обес-печить абарону ад раскрыцця ўсёй паслядоўнасці па яе часткі і дастаткова хуткай рэалізацыяй.

Ступень выкарыстання: вынікі ўкаранёны ў навучальны працэс на ка¬федре праектавання інфармацыйна-камп'ютэрных сістэм ўстановы обра¬зования "Беларускі дзяржаўны універсітэт інфарматыкі і радиоэлек¬троники ў навучальны курс" ".

Вобласць ужывання: метады і сродкі абароны інфармацыі, інфармацыя-онная безопаасности.

.

РЕЗЮМЕ

Шевченко Кристина Валерьевна

Методы и алгоритмы защиты видеоданных

***Ключевые слова*:** цифровой водяной знак, методы защиты видеоданных.

***Цель работы*:** изучение и определение актуальных алгоритмов и методов защиты видеоданных. Для достижения указанной цели решаются задачи исследования основных принципов функционирования систем передачи видеоданных, выявляются уязвимости наиболее распространенных графических форматов и предлагается методика выбора метода защиты видеопотока, учитывающая свойства этих форматов.

***Полученные результаты и их новизна*:** научная новизна и значимость полученных результатов работы заключается в сравнении методики защиты видеоданных с помощью технологий цифрового водяного знака и методики перестановки блоков как механизма защиты видеоданных. Сформулированы требования к цифровому водяному знаку для защиты видеоданных. Изучены методики встраивания цифрового водяного знака в видеопоток. Изучены методы защиты видеоинформации с различным уровнем конфиденциальности. Исследован метод формирования псевдослучайной последовательности по секретному ключу, который может обеспечить защиту от раскрытия всей последовательности по её части и достаточно быстрой реализацией.

***Степень использования*:** результаты внедрены в учебный процесс на кафедре проектирования информационно−компьютерных систем учреждения образования “Белорусский государственный университет информатики и радиоэлектроники в учебный курс “ ”.

***Область применения*:** методы и средства защиты информации, информационная безопаанности.

SUMMARY

Shevchenko Kristina Valeryevna

Methods and algorithms for protecting video data

Key words: digital watermark, methods of protection of video data.

***The object of study*:** to study and determine the actual algorithms and methods of protecting video data. To achieve this goal, the tasks of researching the basic principles of the operation of video data transmission systems are being solved, you are the vulnerability of the most common graphic formats, and a method is proposed for selecting the method of protecting the video stream, taking into account the properties of these formats.

***The results and novelty*:**the scientific novelty and significance of the obtained results of the work consists in comparison of the method of protection of video data with the help of digital watermark technologies and the technique of permutation of blocks as a mechanism for protecting video data. The requirements to the digital watermark for the protection of video data are formulated. The methods of embedding the digital watermark into the video stream are studied. Methods of protecting video information with different levels of confidentiality have been studied. The method of forming a pseudorandom sequence using a secret key is investigated, which can provide protection against the disclosure of the entire sequence by its part and a fairly fast implementation.

***Degree of use*:** the results are implemented in the educational process on the design of information and computer systems of the institution of education "Belarusian State University of Informatics and Radioelectronics in the training course".

Sphere of application: methods and means of information protection, information security.