На правах рукописи

Щерба Евгений Викторович

МЕТОДЫ ЗАЩИТЫ ЦИФРОВОЙ ВИДЕОИНФОРМАЦИИ ПРИ ЕЁ ПЕРЕДАЧЕ В РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Омск 2009

Работа выполнена в Омском государственном техническом университете.

Научный руководитель: доктор технических наук, профессор Файзуллин Рашит Тагирович

Официальные оппоненты:

Ведущая организация:

Защита состоится _____
_____
_____
_____

С диссертацией можно ознакомиться в библиотеке
_____
_____

Автореферат разослан «___» _____ 2009 г.

Ученый секретарь
диссертационного совета

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы

Передача видеоинформации в компьютерных сетях, включая сеть Internet, является важнейшей составляющей информационного потока для многих современных мультимедиа-приложений. Это и различные системы мониторинга, наблюдения, видеотелефонии, регистрирующие и передающие огромные объемы видеоинформации, и персонализированное телевизионное вещание и многие другие системы. Неотъемлемым инструментом видеосистем следующего поколения станет использование потоковой передачи видеоинформации, представленной в цифровом виде. Термином «потоковое видео» обозначают технологии сжатия и буферизации данных, которые позволяют передавать видеоинформацию в реальном времени по локальным компьютерным сетям и через сеть Internet. Согласно статистике исследовательских организаций CacheLogic и Ipoque до 50% всего Internet трафика представляет собой видеоинформацию, передаваемую в распределенных компьютерных сетях. Передача видеоинформации в реальном времени предъявляет повышенные требования к ширине канала, задержкам передачи и допустимым потерям данных. В настоящее время сеть Internet не всегда обеспечивает гарантированное качество обслуживания. Кроме этого, неоднородность структуры сетей и характеристик систем передачи и приема видеоинформации затрудняет передачу в режиме распределенного доступа. Освоение наиболее подходящих стандартов сжатия, преобразования и представления видеоинформации, разработка протоколов и методов передачи составляют важную проблему в области развития информационных технологий.

Наряду с указанными проблемами, при передаче информации по открытому каналу связи неизбежно встает задача защиты её конфиденциальности, целостности и доступности. Под конфиденциальностью видеоинформации обычно понимается субъективно определяемая характеристика видеоинформации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной видеоинформации и обеспечиваемая способностью сохранять указанную видеоинформацию в тайне от субъектов, не имеющих полномочий доступа к ней. Никто сегодня не сможет назвать точную цифру суммарных потерь от компьютерных преступлений, связанных с несанкционированным доступом к информации. С развитием и глобализацией Internet и используемых технологий передачи данных, эта проблема встает наиболее остро, затрагивая и подчиняя себе полный спектр различных решений и разработок. Уникальность глобальной сети Internet в том, что она не находится во владении какого-то физического лица, частной компании, государственного ведомства или отдельной страны. Вследствие этого, практически во всех сегментах сети отсутствует государственное

регулирование, цензура и другие формы контроля как за информацией, циркулирующей в сети, так и за субъектами, пользующихся ее услугами. С другой стороны, Internet сегодня, практически безальтернативный и единственный путь обмена информацией, как на магистральном, так и на локальном уровне. Естественно, данные обстоятельства накладывают дополнительные меры по защите передаваемых данных, так как в незащищенном виде она доступна практически каждому злоумышленнику. Данная проблема широко рассматривается в работах В.А. Герасименко, П.Д. Зегжды, Д.П. Зегжды, А.А. Молдовяна, Н.А. Молдовяна, В. А. Пярина и других авторов.

Учитывая указанные особенности сети Internet, эффективная защита передаваемой информации невозможна на физическом уровне. На сегодняшний день наиболее популярным решением для защиты конфиденциальности на уровне представления является шифрование. Однако в случае потоковой передачи видеоинформации возможности наиболее популярных алгоритмов шифрования могут быть ограничены ввиду их недостаточного быстродействия. За последние годы было предложено множество специализированных алгоритмов шифрования в качестве возможного решения проблемы защиты цифровых изображений и потока видеоинформации. Один из первых широко распространенных подходов к шифрованию цифровых видеоданных заключался в перестановке строк или столбцов кадров видеопотока. Однако большинство таких алгоритмов не обладают достаточной криптостойкостью, и были подвергнуты вскрытию. Вместе с тем, в настоящее время активно ведутся разработки в области визуальной криптографии, которые представляют новую технологию обеспечения защиты конфиденциальности визуальной информации.

Зачастую, вместе с обеспечением защиты конфиденциальности передаваемой видеоинформации, не менее важной задачей является обеспечение её целостности и доступности. Говоря о доступности видеоинформации, подразумевают свойство системы, в которой циркулирует видеоинформация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их видеоинформации. Несомненно, существует достаточное количество методов, призванных обеспечивать целостность и доступность видеоинформации преимущественно на физическом уровне. Среди этих методов можно выделить методы направленные на обеспечение отказоустойчивости (резервирование, дублирование, зеркалирование оборудования и данных) и обеспечение безопасного восстановления (резервное копирование и электронное архивирование видеоинформации). Однако не существует эффективных технических решений способных обеспечивать доступность информации на транспортном уровне и более высоких уровнях при её передаче. Криптографическая защита видеоинформации в определенных случаях может

гарантировать только её целостность, но не может обеспечивать доступность. Таким образом, попытка предложить метод обеспечения доступности видеоинформации, передаваемой в распределенных сетях, основанный на технике визуальной криптографии и системе мультиплексирования трафика, функционирующей на транспортном уровне, наряду с методом обеспечения конфиденциальности, несомненно, также является актуальной.

Цель работы

В связи с этим цель диссертационной работы заключается в обеспечении защиты конфиденциальности и доступности цифровой видеоинформации на уровне содержания при её передаче в распределенных компьютерных сетях. Для достижения поставленной цели решаются задачи разработки и исследования совокупности методов защиты конфиденциальности и обеспечения доступности цифровой видеоинформации при её передаче в распределенных компьютерных сетях, в основу которых положена техника визуальной криптографии и система мультиплексирования трафика. Решение задачи диссертационной работы заключается в следующем:

1. Разработка специализированной системы мультиплексирования трафика для защиты конфиденциальности и обеспечения доступности цифровой видеоинформации при её передаче.
2. Разработка способов сегментации видеоинформации для применения в системе мультиплексирования трафика в качестве схем визуальной криптографии.
3. Разработка архитектуры и реализация экспериментальных программных модулей методов защиты цифровой видеоинформации.
4. Проведение экспериментальных исследований, подтверждающих эффективность разрабатываемых методов.

Методы исследований

В диссертационной работе используются методы математического анализа, теории вероятностей, теории цифровой обработки сигналов и изображений, криптографии и экспериментальных исследований, выполненных с использованием среды программирования Borland C++ Builder и технологии Microsoft DirectShow.

Достоверность

Достоверность результатов работы обеспечивается строгостью применения математических моделей, непротиворечивостью полученных результатов, а также практическим применением разработанных методов.

Научная новизна

В диссертационной работе получены следующие научные результаты:

1. Разработана и реализована специализированная версия системы мультиплексирования трафика для защиты конфиденциальности и обеспечения доступности цифровой видеоинформации при её передаче.
2. Разработан и исследован яркостный способ сегментации изображения как вариант схемы визуальной криптографии в применении к методу защиты конфиденциальности цифровой видеоинформации при её передаче.
3. Доказана эффективность яркостного способа сегментации изображения для решения поставленной задачи относительно других рассматриваемых способов.
4. Исследована и обоснована эффективность способа равномерной сегментации изображения применительно к методу обеспечения доступности видеоинформации, передаваемой в распределенных компьютерных сетях.

Практическая значимость

Разработка и реализация методов защиты получила финансовую поддержку Фонда содействия развития малых форм предприятий в научно-технической сфере (программа У.М.Н.И.К, «Методы защиты и управления качеством при передаче видеоинформации в файлообменных пиринговых сетях»).

Разработанные программные модули зарегистрированы в Отраслевом фонде электронных ресурсов науки и образования (ОФЭРНиО) и могут быть использованы для повышения эффективности защиты конфиденциальности и обеспечения доступности видеоинформации при организации защищенных видеотрансляций в распределенных компьютерных сетях.

Результаты работы используются при преподавании дисциплины «Криптографические методы и средства защиты информации» в Омском государственном техническом университете.

Апробация работы

Результаты работы прошли апробацию в виде выступлений на научных конференциях и семинарах:

1. 39ая Всероссийская молодежная конференция «Проблемы теоретической и прикладной математики» (2008, г. Екатеринбург).
2. VIII Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография – SIBECRYPT-09» (2009, г. Омск).
3. VIII Всероссийский конкурс-конференция студентов и аспирантов по информационной безопасности «SIBINFO-2008» (2008, г. Томск).
4. II Федеральная школа-конференция по инновационному малому предпринимательству в приоритетных направлениях науки и высоких технологий (2006, г. Москва).

5. Конкурс инновационных проектов аспирантов и студентов по приоритетному направлению «Безопасность и противодействие терроризму» (2006, г. Барнаул).
6. Конференция–конкурс работ студентов, аспирантов и молодых ученых «Технологии Microsoft в теории и практике программирования» (2006, г. Новосибирск).

Публикации

Результаты диссертации отражены в 11 публикациях, в том числе 2 публикации в изданиях, рекомендованных ВАК для публикации основных научных результатов диссертации.

Структура и объём работы

Диссертационная работа состоит из введения, четырех глав, заключения, списка литературы и двух приложений. Общий объем работы составляет 98 страниц, в том числе 22 рисунка и 2 таблицы.

Личный вклад

Все исследования, изложенные в диссертационной работе, проведены автором в процессе научной деятельности. Все результаты, выносимые на защиту, получены автором лично. Из совместных публикаций включен лишь тот материал, который непосредственно принадлежит диссертанту, заимствованный материал обозначен в работе ссылками.

Основные результаты, выносимые на защиту

1. Метод защиты конфиденциальности цифровой видеоинформации при её передаче в распределенных компьютерных сетях, основанный на системе мультиплексирования трафика и яркостном способе сегментации видеоинформации, как варианте схемы визуальной криптографии.
2. Метод обеспечения доступности цифровой видеоинформации при её передаче в распределенных компьютерных сетях, основанный на системе мультиплексирования трафика и способе равномерной сегментации видеоинформации, как варианте схемы визуальной криптографии.
3. Архитектура экспериментальных программных модулей, реализующих разработанные методы защиты.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность темы, определяется цель и задачи исследования, излагается научная новизна и практическая значимость работы.

В первой главе рассмотрены существующие методы защиты конфиденциальности и обеспечения доступности цифровой информации, передаваемой в распределенных компьютерных сетях. Большинство из них не может быть задействовано для защиты цифровой видеоинформации в силу различных ограничений. Так, большинство традиционных алгоритмов шифрования не могут применяться для шифрования цифровой видеоинформации в системах реального времени, поскольку их скорость не достаточно высока, особенно в тех случаях, когда алгоритмы реализуются программным обеспечением. К тому же, существование различных алгоритмов сжатия в цифровых видеосистемах делает довольно сложным включение этапа шифрования во всю систему в целом. За последние годы было предложено множество специализированных алгоритмов шифрования в качестве возможного решения проблемы защиты цифровых изображений и потока видеоинформации. Однако большинство таких алгоритмов не обладают достаточной криптостойкостью, и были подвергнуты вскрытию.

Наряду с шифрованием передаваемых данных, сокрытие факта передачи можно выделить как ещё один метод защиты их конфиденциальности. Однако сокрытие внедряемых данных, которые в случае видеоинформации имеют большой объем, предъявляет невыполнимые требования к контейнеру: размер контейнера в несколько раз должен превышать размер встраиваемых данных.

Имитозащита и электронно-цифровая подпись передаваемых данных могут обеспечить контроль целостности, но не обеспечивают их доступность. В то время как методы резервирования каналов и балансировки нагрузки, обеспечивающие доступность передаваемых данных в случае нарушения передачи по одному из каналов, работают в основном на нижних уровнях семиуровневой сетевой модели и не учитывают содержание передаваемых данных.

Это предопределяет необходимость разработки и реализации специализированных методов защиты цифровой видеоинформации, направленных на решение поставленных задач. Было предложено разработать методы защиты конфиденциальности и обеспечения доступности цифровой видеоинформации, которые позволяли бы решать поставленную задачу защиты без применения алгоритмов шифрования, используя аналитическое преобразование исходной последовательности и принципы сокрытия путей передачи между участниками информационного обмена. Решение должно обеспечивать стойкость при несанкционированном доступе к среде передачи на основе имеющихся физических средств.

Вторая глава посвящена разработке методов защиты конфиденциальности и обеспечения доступности цифровой видеоинформации, передаваемой в распределенных компьютерных сетях. В основу методов положена система мультиплексирования трафика (рис. 1), предложенная в работах Файзуллина Р. Т. и Ефимова В. И., позволяющая осуществить

разнесение передачи по нескольким физическим каналам отдельных частей передаваемых данных таким образом, чтобы сложность восстановления исходных данных без какой-либо их части была максимальной или минимальной в зависимости от поставленной задачи.

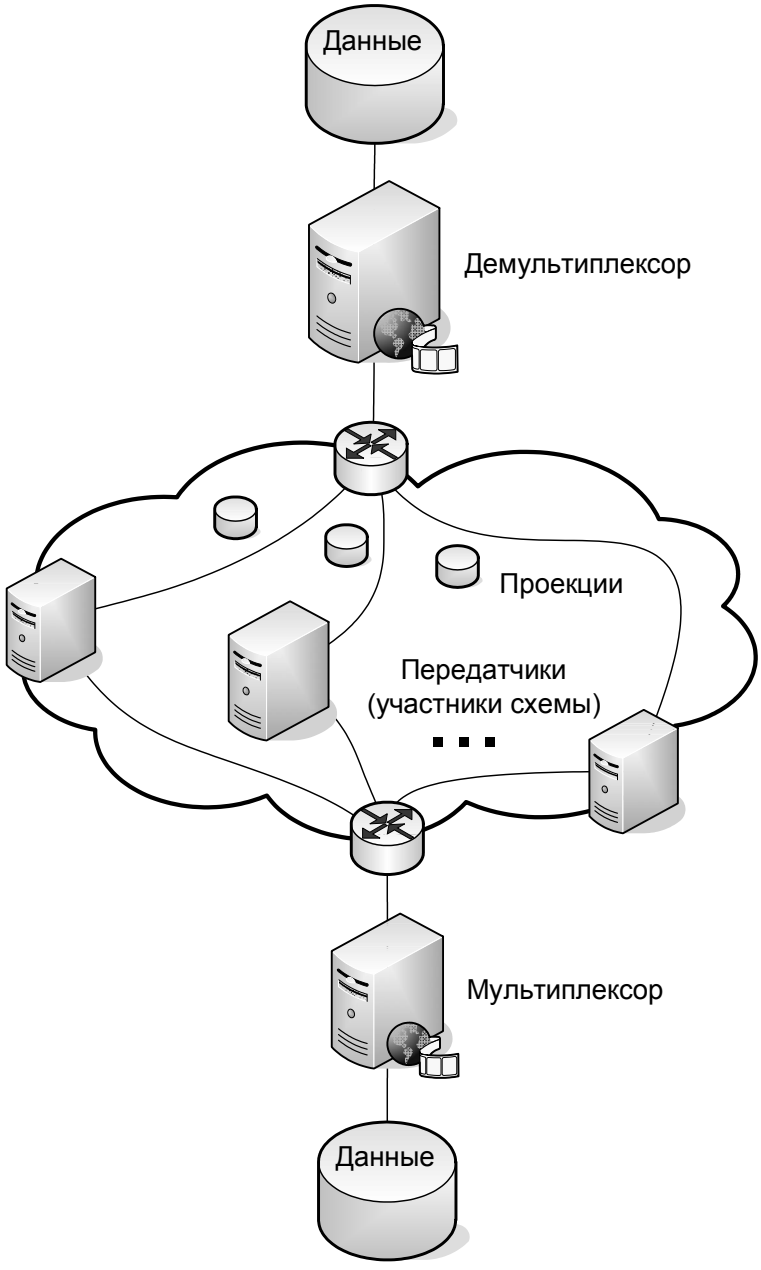


Рис. 1. Система мультиплексирования трафика

Такая модель при работе с видеоинформацией может быть ассоциирована со схемой визуальной криптографии, участниками которой являются промежуточные узлы сети, а проекциям в системе мультиплексирования трафика соответствуют проекции схемы визуальной криптографии, образованные на основе исходного изображения. Классический вариант схемы

подразумевает собой передачу каждому участнику проекции, размер которой равен размеру секрета, но данный способ передачи имеет существенный недостаток. Поскольку размер трафика увеличивается пропорционально числу участников, при передаче больших объемов информации возникает проблема ограниченной пропускной способности канала, поэтому для применения схемы визуальной криптографии в системе мультиплексирования требуется специализированный подход.

В основу алгоритма разделения данных в системе мультиплексирования трафика был положен принцип разбиения множества всех точек изображения на некоторое количество непересекающихся классов. Этот принцип позволяет распределить передачу видеоинформации на несколько физических каналов без увеличения избыточности передаваемых данных, и как следствие, объёма передаваемой по сети информации, что играет большую роль при передаче видеоинформации. Основной недостаток такого подхода заключается в том, что при перехвате одной или нескольких проекций злоумышленник получает некоторую информацию о возможном значении исходного изображения. Задачей в данном случае является поиск такого метода разбиения, при котором практическая ценность перехваченной информации была бы минимальной. В то же время для обеспечения максимальной доступности данных необходимо предложить способ разбиения, обеспечивающий наилучшее восстановление изображения законным получателем, в случае блокирования или модификации одной или нескольких передаваемых проекций нарушителем.

В результате исследований для метода защиты конфиденциальности передаваемой видеоинформации был предложен способ разбиения на основе значения функции яркости точки $f(x,y)$ (яркостный способ сегментации). Каждая проекция в результате разбиения будет включать в себя точки из определенного диапазона яркости. Число диапазонов определяется числом участников. В соответствии со значением функции яркости точки разбиваются на классы. В схеме с 2-мя участниками эти классы выглядят следующим образом:

$$P_0 = \left\{ (x,y) \;\middle|\; f(x,y) < \frac{1}{M_1 M_2} \sum_{x=0}^{M_1-1} \sum_{y=0}^{M_2-1} f(x,y) \right\},$$
$$P_1 = \left\{ (x,y) \;\middle|\; f(x,y) \geq \frac{1}{M_1 M_2} \sum_{x=0}^{M_1-1} \sum_{y=0}^{M_2-1} f(x,y) \right\}. \qquad (1)$$

А для случая произвольного числа $n = 2^k \ (k > 1)$ участников определение классов происходит рекуррентно:

$$P_i = \left\{ (x,y) \,\middle|\, f(x,y) < \frac{2^{k-1}}{M_1 M_2} \sum_{(x,y)\in \bar{P}_j} f(x,y) \right\},$$
$$P_{i+1} = \left\{ (x,y) \,\middle|\, f(x,y) \geq \frac{2^{k-1}}{M_1 M_2} \sum_{(x,y)\in \bar{P}_j} f(x,y) \right\} \qquad (2)$$

Здесь $\bar{P}_j$ - это класс, полученный для схемы с 2^{k-1} участниками, т.е. $j \in \lfloor 0; 2^{k-1} - 1 \rfloor$, а $i = 2j$.

Вместе с тем, для обеспечения максимальной доступности передаваемой видеоинформации был предложен способ равномерной сегментации изображения. Пусть задано цифровое изображение P размерами $M_1 \times M_2$ в виде следующей матрицы:

$$\begin{bmatrix} f(0,0) & f(1,0) & \Lambda & f(M_1-1,0) \\ f(0,1) & f(1,1) & \Lambda & f(M_1-1,1) \\ \text{M} & \text{M} & & \text{M} \\ f(0,M_2-1) & f(1,M_2-1) & \Lambda & f(M_1-1,M_2-1) \end{bmatrix}.$$

Необходимо разбить его на n сегментов так, чтобы для восстановления исходного изображения требовалось минимальное количество сегментов. Для этого очевидным образом необходимо, чтобы в каждый образованный сегмент попали точки, равномерно распределенные по всему кадру, т.е. сегмент будет представлять собой сетку с равноудаленными узлами, а $n = 2^{2k}$, $k \geq 1$:

$$\begin{bmatrix} f(0,0) & 0 & \Lambda & f(\sqrt{n},0) & 0 & \Lambda \\ 0 & 0 & & & & \\ \text{M} & & \text{O} & & & \\ f(0,\sqrt{n}) & & & f(\sqrt{n},\sqrt{n}) & & \\ 0 & & & & 0 & \\ \text{M} & & & & & \text{O} \end{bmatrix}. \qquad (3)$$

При этом восстановить исходное изображение по неполному количеству проекций можно с помощью построения интерполяционной функции

изображения по каждой паре известных соседних точек и расчёте значений в неизвестных точках между ними по построенной функции. Причем, с увеличением количества сегментов полученных пользователем системы, качество полученной оценки исходного изображения должно расти (рис. 2).

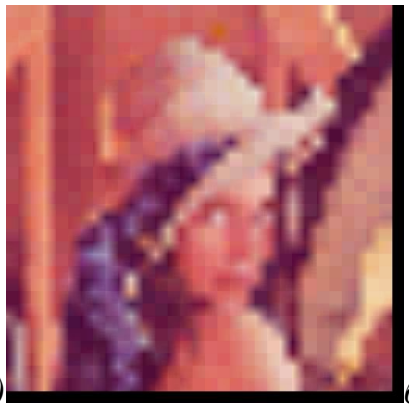
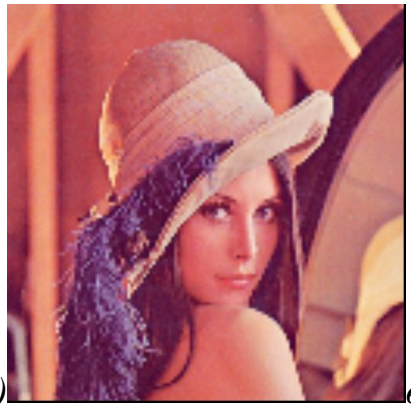
а)  *б)*  *в)* 

Рис. 2. Пример работы метода обеспечения доступности (рис. 2*а* – один сегмент исходного изображения после интерполяции; 2*б* – 16 из 256 сегментов исходного изображения после интерполяции, рис. 2*в* – исходное изображение), $n = 256$.

В третьей главе произведен анализ разработанных методов защиты. В работе сделано следующее допущение: нарушитель может получить несанкционированный доступ к единственному физическому каналу из всего множества каналов задействованных в системе мультиплексирования трафика, и не имеет доступа к остальным каналам. То есть, он имеет возможность для анализа, блокирования и модификации всей информации, передаваемой по этому каналу. В случае передачи видеоинформации задача её анализа естественным образом сводится к задаче анализа отдельных кадров. Но поскольку по каждому из каналов передаётся лишь некоторая проекция исходного кадра, задачей нарушителя станет возможное восстановление исходного кадра на основе перехваченной им проекции. В случае если нарушитель сможет успешно справиться с этой задачей, он фактически получит доступ и ко всему потоку видеоинформации в целом, что приведет к нарушению конфиденциальности передаваемой видеоинформации.

Блокирование и модификация одного из сегментов видеоинформации нарушителем в свою очередь может повлечь нарушения целостности и доступности видеоинформации. Таким образом, возникает вопрос, насколько устойчив разработанный метод обеспечения доступности видеоинформации к атакам нарушителя.

Для получения ответа на поставленный вопрос, были исследованы возможные методы восстановления исходного кадра на основе его произвольной проекции. Для того чтобы использовать методы цифровой

обработки изображений для решения поставленной задачи восстановления исходного кадра была предложена следующая аналогия (рис. 3).

В случае метода защиты конфиденциальности, сам метод представляет искажающую систему, а в задачи нарушителя входит восстановление исходного изображения, в то время как для метода обеспечения доступности уже действия нарушителя представляют искажающую систему, в задачи законного получателя входит восстановление исходного изображения.

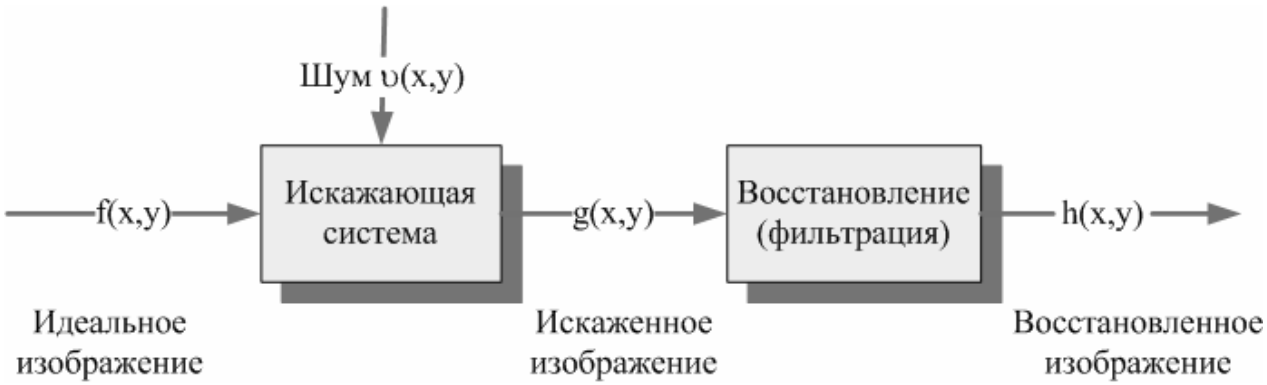


Рис. 3. Модель искажения и восстановления изображений.

Для оценки эффективности методов восстановления и как следствия методов защиты были выбраны следующие критерии:

- Критерий минимума квадрата средней квадратичной ошибки восстановленного изображения:

$$\varepsilon^2 = \frac{1}{M_1 M_2} \sum_{x=0}^{M_1-1} \sum_{y=0}^{M_2-1} \left(h(x,y) - f(x,y)\right)^2 \to \min$$

- Психовизуальный критерий качества.

В качестве методов восстановления изображения рассматривались методы билинейной интерполяции, бикубической интерполяции сплайнами и экстраполяции линейным прогнозированием. В результате исследований были получены следующие результаты:

- Бикубическая интерполяция сплайнами позволяет добиться минимума ε^2 при интерполяции проекций равномерной сегментации.
- Была построена зависимость роста ε^2 при увеличении относительного размера разрыва (рис. 4)
- В некоторых случаях искомый результат можно получить экстраполяцией разрывов, однако в случае проекций, образованных яркостной сегментацией, экстраполяция разрывов неэффективна.

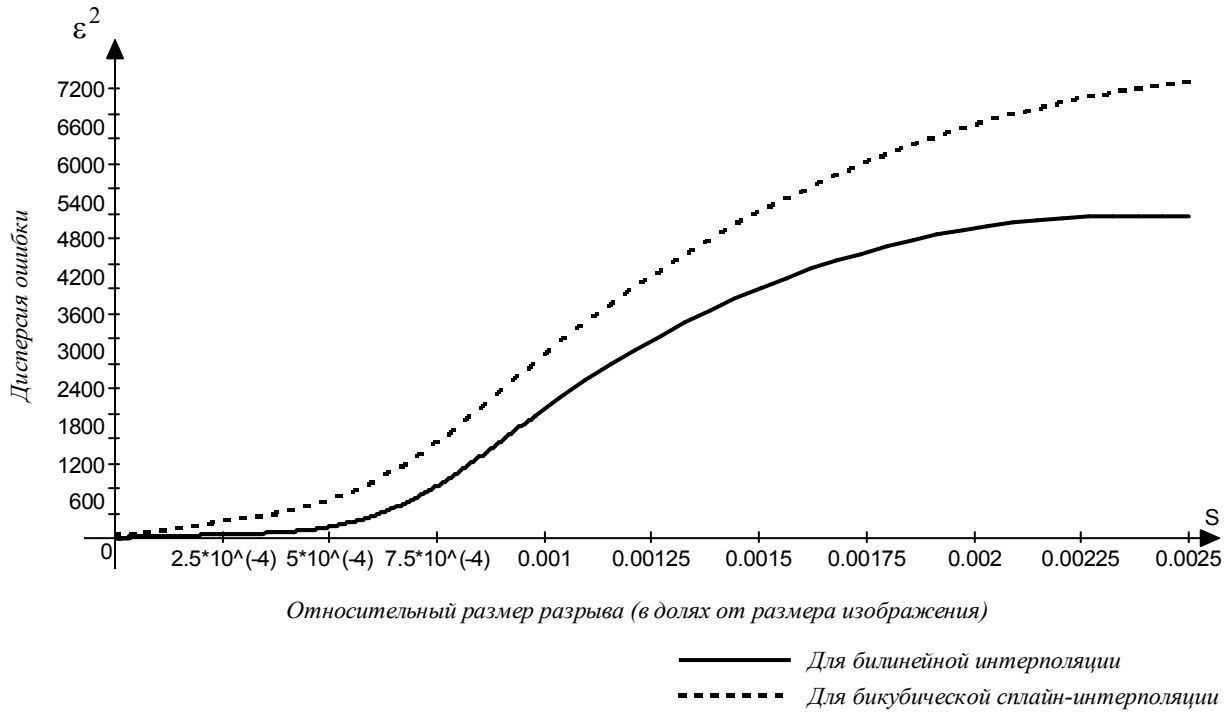


Рис. 4. Результаты интерполяции случайного одиночного разрыва в среднем по стандартному набору из 24 изображений Kodak Lossless True Color Image Suite, 256 градаций яркости.

Данные результаты хорошо согласуются с психовизуальным критерием качества восстановления (рис. 5).

а)  *б)* 

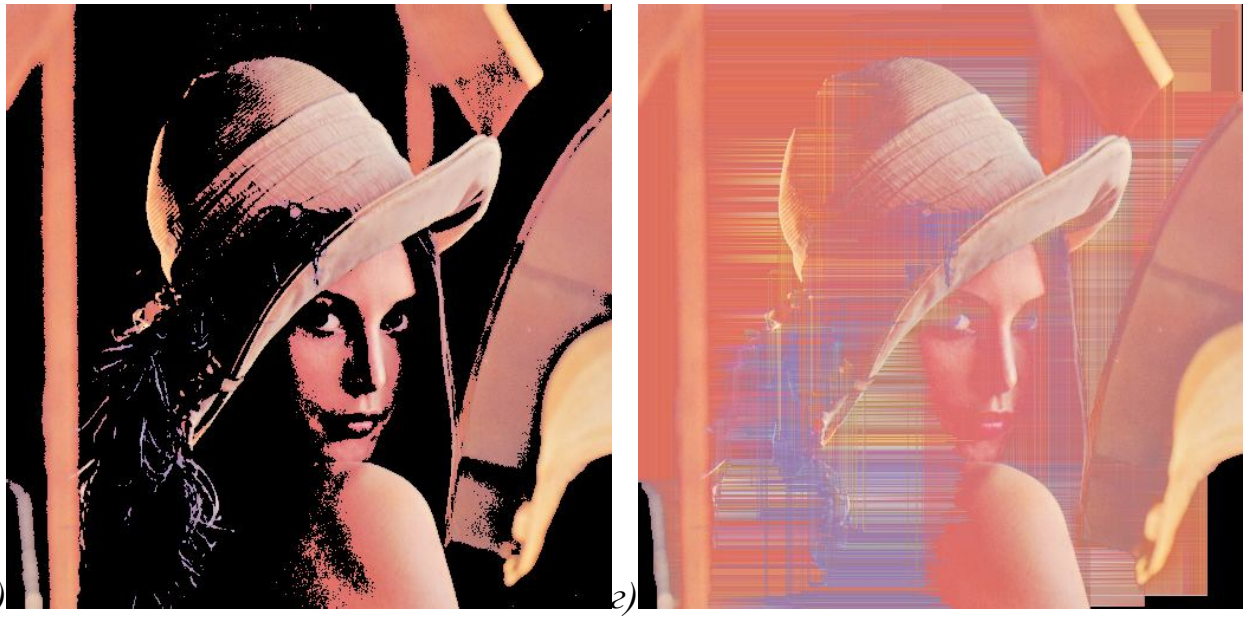


Рис. 5. Пример билинейной интерполяции разрывов (рис. 14*а* – проекция случайной сегментации, рис. 14*б* – результат интерполяции проекции 14*а*; 14*в* – проекция яркостной сегментации, рис. 14*г* – результат интерполяции проекции 14*в*), $n = 2$.

Кроме того, была построена и доказана следующая теорема, которая также позволяет обосновать преимущества яркостного способа сегментации перед остальными способами для применения в системе мультиплексирования трафика. Поскольку яркостная сегментация максимизирует разницу между значениями $\bar{f}_i$, значения выражения $\left(\bar{f} - \bar{f}_i\right)^2$ в этом случае также будут максимизированы.

Теорема 1. Пусть исходное изображение $f(x,y)$ сегментировано на n проекций $f_1(x,y), \text{K}, f_n(x,y)$ с помощью яркостного способа сегментации. Тогда средняя квадратичная ошибка ε_i восстановленного изображения $h_i(x,y)$ на основе произвольной проекции $f_i(x,y)$ методами интерполяции имеет оценку снизу: $\varepsilon_i^{\,2} \geq \left(\bar{f} - \bar{f}_i\right)^2$, где $\bar{f}_i$ – среднее значение $f(x,y)$ для проекции i, а $\bar{f}$ – среднее значение $f(x,y)$ для исходного изображения.

Доказательство данной теоремы произведено с применением метода математической индукции и перехода от $h_i(x,y)$ к $f_i(x,y)$.

В четвертой главе представлена программная реализация разработанных методов защиты конфиденциальности и обеспечения доступности цифровой видеоинформации при её передаче в распределенных компьютерных сетях, а также проведены экспериментальные исследования этих методов. Для программной реализации описанной системы была выбрана технология

Microsoft DirectShow, как ключевая технология Microsoft для создания компонентов обработки видеоданных. В результате работы были созданы фильтры, ответственные за преобразование кадра исходного видеопотока в проекцию производного видеопотока. В основу фильтра, реализующего метод защиты конфиденциальности, положена процедура генерации заданной проекции с помощью способа яркостной сегментации изображения, в то время как фильтр, реализующий метод обеспечения доступности использует для генерации проекций равномерную сегментацию изображения. На вход фильтров при этом подается исходный поток видеоинформации, а поток доступный на выходе представляет собой видеопоследовательность образованных проекций с заданными свойствами.

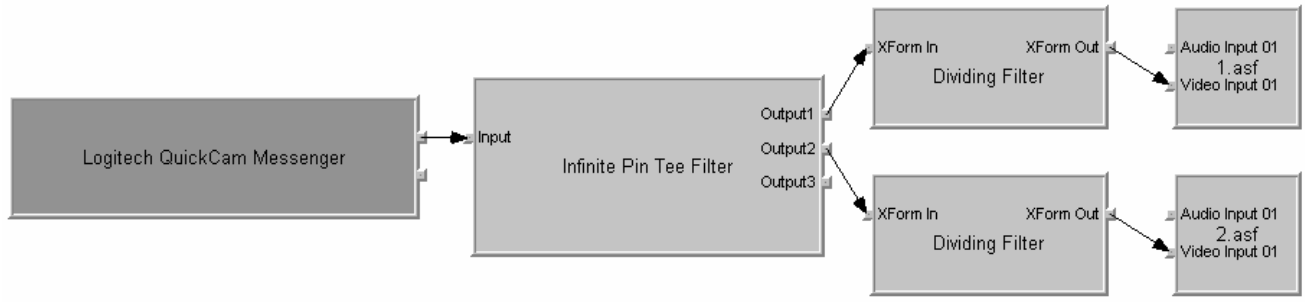


Рис. 6. Граф фильтров

Разработанные фильтры были успешно интегрированы в граф фильтров, построенный для процесса организации и передачи производных потоков видеоинформации по сети (рис. 6). В качестве источника исходного видеопотока могут выступать фильтры любых устройств захвата видеоизображений, а также фильтр, обеспечивающий чтение видеопотока из файла. Следующий фильтр (Infinite Pin Tee Filter) создает необходимое количество копий исходного потока в соответствии с числом участников схемы мультиплексирования трафика. Далее каждая копия исходного потока видеоинформации с помощью разработанных фильтров подвергается последовательной сегментации в соответствии выбранной задачей и заданным порядковым номером класса сегментации, т.е. номером участника системы, которому впоследствии с помощью фильтра ASF Writer будет передан преобразованный поток видеоинформации. Участники схемы мультиплексирования трафика, транслируют входящий поток непосредственно исходному получателю потока видеоинформации, который, принимая входящие потоки, строит на их основе исходный поток видеоинформации.

Были проведены экспериментальные исследования работы представленной системы с переменным числом участников (от 2-х до 32-х) в действующей компьютерной сети крупной организации (сеть Fast Ethernet 100 Мбит/с, процессоры рабочих станций Intel Pentium IV 3 GHz). В задачи исследования входило определение зависимости максимально допустимого

числа участников системы от размера кадра исходного потока видеоданных, зависимости эффективности методов защиты от числа участников системы (рис. 7, 8) и выбора оптимального числа участников системы на основе этих двух зависимостей. Поскольку обработка большого объёма видеоданных в системе мультиплексирования трафика накладывает определенные ограничения ввиду не всегда достаточного быстродействия рабочей станции, в ходе исследования были получены следующие результаты (табл. 1).

Таблица 1. – Максимальное допустимое число участников системы при осуществлении сегментации исходного потока на рабочей станции с процессором Intel Pentium IV 3 GHz.

Размеры кадра исходного видеопотока (24bit, 24 к/с)	Максимально допустимое число участников системы
1920x1080	2
1280x720	4
720x576	8
640x480	8
320x240	32

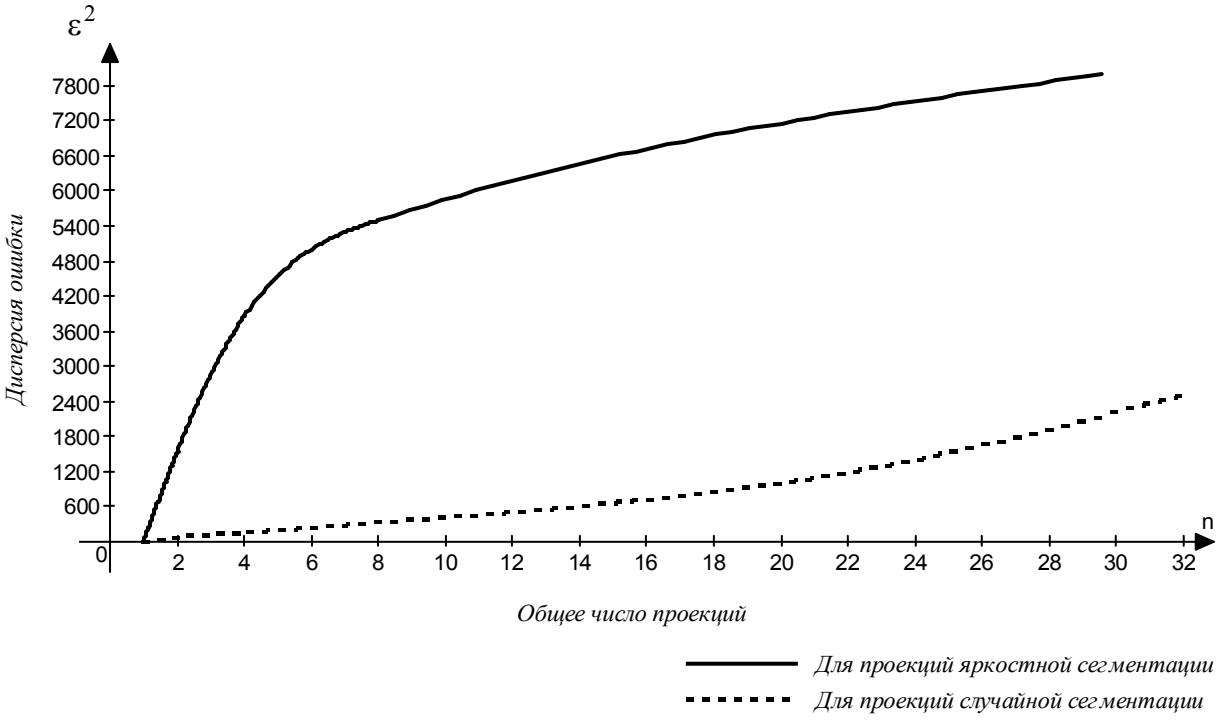


Рис. 7. Усредненные результаты билинейной интерполяции для двух видов проекций, образованных по стандартному набору из 24 изображений Kodak Lossless True Color Image Suite

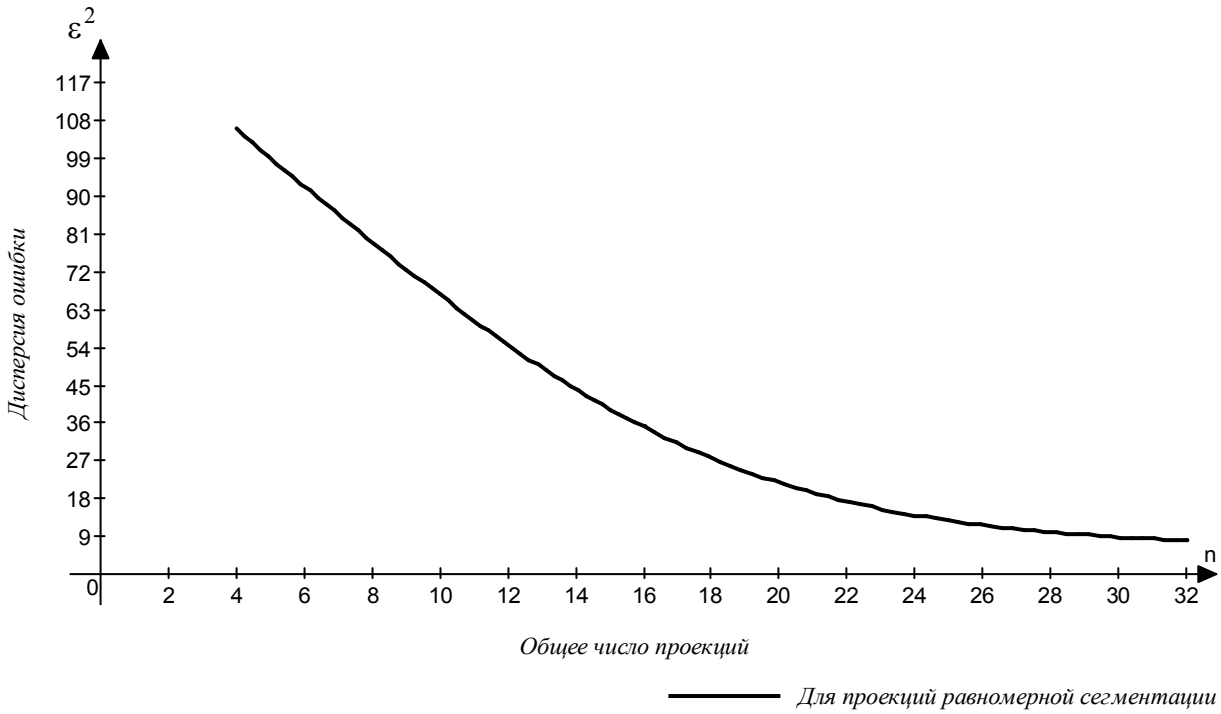


Рис. 8. Усредненные результаты бикубической интерполяции сплайнами для проекций равномерной сегментации, образованных по стандартному набору из 24 изображений Kodak Lossless True Color Image Suite, 256 градаций яркости.

На основании полученных зависимостей можно сделать вывод о том, что применение системы мультиплексирования трафика с числом участников не менее 8 является наиболее обоснованным, в случае, когда требования как разрешению кадра передаваемого потока видеоинформации не определены.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В результате проведенных исследований получены следующие основные научные и практические результаты:

1. Обобщены и систематизированы основные подходы к защите цифровой видеоинформации, передаваемой в распределенных компьютерных сетях. Указаны их ограничения.
2. Разработаны методы защиты конфиденциальности и обеспечения доступности передаваемой видеоинформации на основе системы мультиплексирования трафика и варианте схемы визуальной криптографии.
3. Предложены способы сегментации кадров потока видеоинформации для применения в разработанных методах защиты.
4. Приведено исследование представленных способов, сравнение с другими способами сегментации и обоснована эффективность выбранных способов сегментации.

5. Представлена модульная реализация разработанных методов защиты на основе технологии Microsoft DirectShow.
6. Проведены экспериментальные исследования разработанных методов, представлены рекомендации относительно параметров их применения.

Разработанные методы защиты обладают следующими отличительными особенностями:

- Основываются на свойстве структурной избыточности распределенных сетей.
- Обеспечивают защиту на уровне содержания информации.
- Позволяют решать поставленную задачу без применения криптографических алгоритмов.
- Используют бесключевое преобразование информационного потока.
- Программная реализация представленных методов предъявляет минимальные требования к вычислительным ресурсам.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Щерба Е.В. Атака на систему мультиплексирования разнесенного TCP/IP трафика на основе анализа корреляции потоков / Е.В. Щерба, В.И. Ефимов // Информационные технологии моделирования и управления. – 2005. – Выпуск 6(24). – С. 859-863.
2. Щерба Е.В. Разработка Microsoft DirectShow фильтра для защиты канала передачи видеоинформации / Е.В. Щерба // Технологии Microsoft в теории и практике программирования. Конференция–конкурс работ студентов, аспирантов и молодых ученых. – Новосибирск: 2006. – С. 144.
3. Щерба Е.В. Применение системы мультиплексирования TCP/IP трафика для защиты канала передачи видеоинформации / Е.В. Щерба // Конкурс инновационных проектов аспирантов и студентов по приоритетному направлению «Безопасность и противодействие терроризму». Каталог поданных проектов. – Барнаул: АлтГТУ, 2006. – С. 67.
4. Щерба Е.В. Применение системы мультиплексирования TCP/IP трафика для защиты канала передачи видеоинформации / Е.В. Щерба // Федеральная школа–конференция по инновационному малому предпринимательству в приоритетных направлениях науки и высоких технологий. – М.: РГУИТП, 2006. – С. 161–164.
5. Щерба Е. В. Комплекс программ защиты видеоданных / В.И. Ефимов, М.В. Корытова, Г.С. Ржаницын, Е.В. Щерба // Научная сессия МИФИ – 2007. Сборник научных трудов. – М.: МИФИ, 2007. – Т.16: Компьютерные науки. Информационные технологии. – С. 143-144.
6. Щерба Е.В. Некоторые аспекты применения протокола BitTorrent при

организации учебного процесса / Е.В. Щерба, Л.П. Щерба // Актуальные проблемы развития техники и экономики в условиях Крайнего Севера: сб. науч. тр. / отв. ред. В.Е. Щерба. – Омск: изд–во ОмГТУ, 2007. – С. 104–109.

7. **Щерба Е.В. Метод защиты канала передачи видеоинформации на основе мультиплексирования трафика / Е.В. Щерба // Вопросы защиты информации. – 2008. – № 1(80). – С. 55–60.**
8. Щерба Е.В. Метод управления качеством при передаче видеоинформации в файлообменных пиринговых сетях / Е.В. Щерба // Проблемы теоретической и прикладной математики: Труды 39й Всероссийской молодежной конференции. – Екатеринбург: УрО РАН, 2008. – С. 418–422.
9. **Щерба Е.В. Анализ применимости методов интерполяции и экстраполяции для решения задачи восстановления изображения / Е.В. Щерба // Компьютерная оптика. – 2009. – Том № 33, №3. – С. 336–340.**
10. Щерба Е.В. Метод защиты цифровой видеоинформации при её передаче в распределенных компьютерных сетях / Е.В. Щерба // Прикладная дискретная математика. – 2009. – Приложение № 1. – С. 60–62.
11. Щерба Е.В. Учебно-исследовательский программный модуль Y-Sharing 1.0 для сегментации входящего потока видеоинформации на основе значения яркости – М.: ЦИТиС – №50200900627. – 2009.