На правах рукописи

Ренжин Петр Александрович

МЕТОДИКИ ЗАЩИТЫ ЦИФРОВЫХ ВИДЕОДОКАЗАТЕЛЬСТВ ОТ ФАЛЬСИФИКАЦИИ СКРЫТЫМ ВСТРАИВАНИЕМ ИЗОБРАЖЕНИЯ СЛУЧАЙНЫМИ ЧАСТЯМИ

Специальность: 05.13.19 – Методы и системы защиты информации, информационная безопасность.

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Томск 2010

Работа выполнена в ГОУ ВПО «Омский государственный университет им. Ф.М. Достоевского»

Научный руководитель – доктор технических наук профессор
Файзуллин Рашит Тагирович

Официальные оппоненты:

доктор физико-математических наук
Бондарчук Сергей Сергеевич
(Томский государственный педагогический университет)

доктор физико-математических наук
Чернов Владимир Михайлович
(Институт систем обработки изображений РАН,
г. Самара)

Ведущая организация –

ФГУП «Омский научно-исследовательский
институт приборостроения»

Защита состоится 29 июня 2010 г. в 15 час. 15 мин. на заседании диссертационного совета Д 212.268.03 при Томском государственном университете систем управления и радиоэлектроники (ТУСУР) по адресу г. Томск, пр. Ленина, 40, аудитория 203.

С диссертацией можно ознакомиться в библиотеке ТУСУРа.

Автореферат разослан 28 мая 2010 г.

Ученый секретарь
диссертационного совета  Р.В. Мещеряков

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. В настоящее время главной ценностью в человеческом обществе считается информация. Технический прогресс предоставил обществу возможность хранить и обрабатывать информацию в цифровом виде. Одним из примеров являются технологии мультимедиа. Зачастую цифровые средства не только дают возможность хранить и передавать видеоданные, аудиозаписи, изображения, но и являются способом их создания. Но преимущества, которые дает цифровая обработка данных, перечеркиваются легкостью, с которой возможна их фальсификация. В результате с особенной силой встает вопрос о способах и средствах защиты информации как о возможности защитить интеллектуальную собственность. Одним из направлений защиты информации являются технологии цифрового водяного знака.

Особый интерес представляет защита видеоданных как одного из самых востребованных в настоящее время видов продукции. Особенностями защиты видеоданных является большой объем, необходимый для хранения такого рода информации, и, как следствие, широкие возможности встраивания невидимых меток. Информация может быть встроена в сжатое видео, причем разработаны методы встраивания на различных этапах алгоритмов сжатия видеоданных. Также встраивание может осуществляться в несжатое видео за счет различных манипуляций с яркостью. Встраивание стегосообщения в сжатое видео содержится в работах Коха, Бенхама, Лангелаара. Встраиванием стегосообщения в несжатое видео занимались такие авторы, как Куттер, Питас.

В работе правоохранительных органов и судов доказательствами зачастую выступают видеозаписи. Это может быть съемка с места происшествия, запись, сделанная скрытой камерой в банкомате или запись допроса. Такого рода доказательства нуждаются в особой защите. Цифровой водяной знак в данном случае должен являться свидетельством подлинности контента, т.е. отсутствие его по какой-либо причине должно сигнализировать, что запись кто-то изменял. Во-вторых, цифровой водяной знак должен быть устойчив к обнаружению, чтобы исключить его подделку. Кроме того, желательно, чтобы такой знак обладал устойчивостью к монтажу видео.

Основные понятия диссертации. Цифровой водяной знак (ЦВЗ) – последовательность бит, скрыто встраиваемая в другую последовательность, имеющую аналоговую природу. Таким образом, встраивание скрытого сообщения в избыточную служебную информацию файла (изображения, видео или аудио) не явля-

ется цифровым водяным знаком. Цифровым водяным знаком является изменение контента.

Контейнером называется объект, в который осуществляется скрытое встраивание. Контейнером может быть фильм, аудиозапись, цифровое изображение.

Целью работы является разработка и исследование методик защиты цифровых видеодоказательств от фальсификации.

В соответствии с целью были определены **задачи диссертационной работы**:

1. Произвести обзор существующих технологий цифрового водяного знака.

2. Разработать методики цифрового водяного знака, обладающие низкой робастностью и устойчивостью к монтажу.

3. Определить пределы применения разработанных методик.

4. Разработать методику защиты цифровых доказательств от фальсификации.

Методы исследования основаны на использовании стеганографии, теории вероятностей, булевой алгебре, математическом моделировании, программировании.

Достоверность результатов работы обеспечивается строгостью применения математических вычислений, непротиворечивостью полученных результатов, а также внедрением разработанных методик в практику.

Научная новизна заключается в следующем:

– впервые разработаны методики защиты цифровых видеодоказательств от фальсификации с помощью технологий цифрового водяного знака (ЦВЗ);

– впервые предложены технологии ЦВЗ, заключающиеся в покадровом встраивании случайных частей черно-белого изображения в видеопоследовательность. В отличие от известных приведенные методики обеспечивают статистическую взаимосвязь между встроенной информацией в кадрах, что позволяет обнаруживать несанкционированный монтаж (удаление или замену части кадров);

– впервые получено достаточное условие обнаружения бинарного сигнала в бинарном шуме посредством корреляционного приемника.

Практическая ценность. Результаты, полученные в процессе проведенных исследований, используются для защиты цифровых доказательств от фальсификации.

Внедрение и реализация. Получены акты о внедрении результатов диссертационной работы в учебном процессе ГОУ ВПО «Омский государственный технический университет», акт о внедрении методик в качестве средств защиты авторских прав в Учреждении Российской академии наук «Институт систем обработки

изображений РАН», акт об использовании в качестве средств защиты цифровых видеодоказательств от фальсификации в Научно-экспертном центре (ОмГТУ).

Апробация работы. Материалы работы обсуждались на научно-методических семинарах кафедры комплексных систем защиты информации ОмГУ и докладывались на научной конференции «Технологии Майкрософт в теории и практике программирования» (Новосибирск, 2008, второе место), на межрегиональном информационном конгрессе «Роль регионов в реализации стратегии развития информационного общества в Российской Федерации» (Омск, 2008), научной конференции «Технологии Майкрософт в теории и практике программирования» (Томск, 2010) и на всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР» (Томск, 2010).

Публикации. Основные положения диссертации опубликованы в 9 печатных работах [1]–[9], из них две – в изданиях, входящих в Перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёной степени доктора и кандидата наук.

Структура работы. Диссертационная работа состоит из введения, 4 глав, заключения, списка используемых литературных источников из 87 наименований и 1 приложения. Она содержит 107 страниц машинописного текста, 50 рисунков и 3 таблицы.

Личный вклад. В диссертации использованы только те результаты, в которых автору принадлежит определяющая роль. Опубликованные работы написаны самостоятельно и в соавторстве с научным руководителем.

Основные защищаемые положения.

1. Впервые разработаны методики защиты цифровых видеодоказательств от фальсификации скрытым встраиванием черно-белого изображения в видеоданные.

2. Разработано достаточное условие обнаружения бинарного сигнала в бинарном шуме посредством корреляционного приемника.

3. Выполнена программная реализация методик защиты цифровых видеодоказательств от фальсификации.

СОДЕРЖАНИЕ РАБОТЫ

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

В первой главе проведен анализ существующих стегосистем. Приведена их краткая классификация 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.

Для защиты видеоданных от фальсификации требуется обеспечить, во-первых, 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. Во-вторых, водяной знак должен минимально искажать видео, чтобы максимально сохранить целостность доказательства. В-третьих, 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.

Так, встраивание в область преобразования обладает, с одной стороны, высокой стеганографической робастностью, что противоречит предъявляемым требованиям; с другой – оно сильнее искажает сигнал относительно метода младших значащих бит (МЗБ). Заведомо большим искажением обладают и другие, отличные от МЗБ, методики встраивания в пространственную область, так как их можно представить как добавление случайного шума, с амплитудой, отличной от 0.5.

Наконец, классический метод МЗБ в наибольшей мере отвечает требованию низкой робастности и обладает минимальным искажением содержимого видеофайла. Кроме того, выбор МЗБ диктуется еще и следующими соображениями. Встает вопрос, в каком формате сжатия хранить цифровые доказательства. Выбор

любого из алгоритмов, кроме сжатия без потерь, может привести к спорам о том, не утрачена ли информация в процессе обработки. Для исключения данных споров самый удобный способ хранения – это формат RGB, т.е. первоначальный, необработанный контент. Препятствие в виде большого объема хранимых данных снимается современным ростом емкости цифровых носителей и пропускной способности каналов передачи данных.

Однако у классического метода МЗБ есть и ряд недостатков для решения задачи защиты цифровых доказательств от фальсификации. Во-первых, стегосообщение легко декодируется побитовым просмотром или несложным статистическим анализом младших значащих бит. Во-вторых, метод МЗБ не обладает защитой от монтажа независимо от встраиваемой информации. Предложенные в данной работе методики позволяют устранить эти проблемы.

Во второй главе описываются методики скрытого встраивания изображения в видеоданные случайными частями – с помощью логического суммирования и с помощью замены, являющиеся результатом данной работы. Встраивание скрытой информации в младшие значащие биты последовательности-контейнера является одним из базовых приемов стеганографии. Новизна методик заключается в осуществлении математических операций между 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. Приводятся методики выбора параметров для применения данных методик. Устанавливается зависимость между параметрами встраивания и вероятностями ошибок декодирования.

Видеофайл, в который осуществляется встраивание, имеет формат RGB (несжатое видео), 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.

Рассмотрим встраивание изображения в видеофайл случайными частями с помощью логического суммирования. Итак, существует последовательность кадров-изображений, каждый из которых можно представить как совокупность трех матриц цвета с размерностью кадра видеофайла.

Выбирается цвет для встраивания информации. Допустим, это будет синий. Предполагается, что плотность единиц в массиве МЗБ равна 0,5. Выберем место встраивания картинки в кадре.

Пример изображения можно увидеть на рис. 1,а. Создадим «маску» – 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 (рис. 1,б).

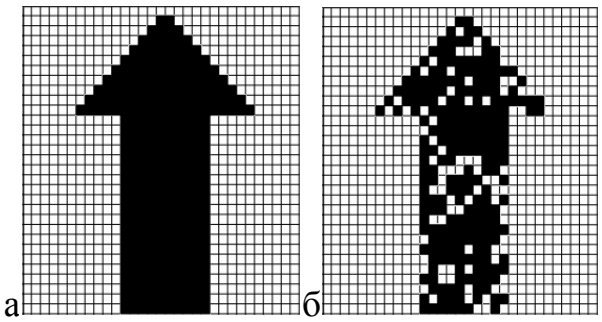


Рис. 1. Примеры входных данных стегосистемы:
а – пример изображения, б – пример маски

Далее маска сравнивается с массивом МЗБ кадра видеофайла в месте встраивания изображения. Если значение ячейки маски равно нулю, то бит кадра остается неизменным. Если единице – бит кадра заменяется битом изображения.

Между каждым битом МЗБ и битом маски, соответствующей данному кадру, в месте встраивания изображения осуществляется следующая операция:

$$ls_{h_0+i,w_0+j} = ms_{i,j} \vee ls_{h_0+i,w_0+j},\ i = 0,...,I-1,\quad j = 0,...,J-1,$$

где i, j – координаты пикселей изображения,

I, J – геометрические размеры изображения,

h_0, w_0 – координаты начала встраивания изображения в матрицу МЗБ,

ls_{h_0+i,w_0+j} – соответствующий бит МЗБ,

$ms_{i,j}$ – соответствующий бит маски.

Но ведь встроена пока только некоторая часть изображения. Чтобы встроить оставшуюся часть, аналогичную операцию проделываем со вторым кадром, затем с третьим и т.д., меняя каждый раз маску. Через определенное количество кадров

все пиксели изображения будут встроены по нескольку раз. Назовем это количество «периодом встраивания». Плотность единиц в маске и период встраивания образуют «параметры встраивания». Процесс встраивания схематично изображен на рис. 2.

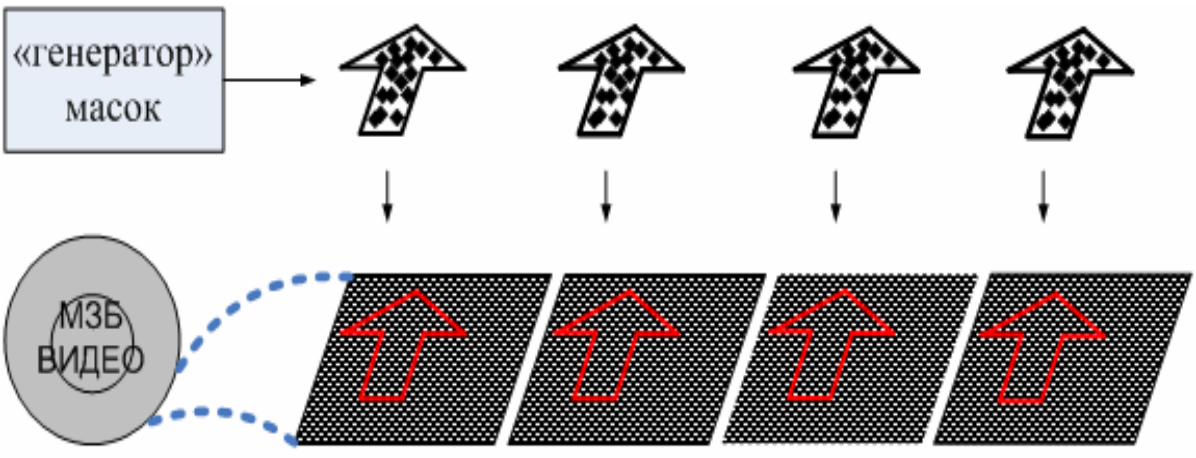


Рис. 2. Процесс встраивания

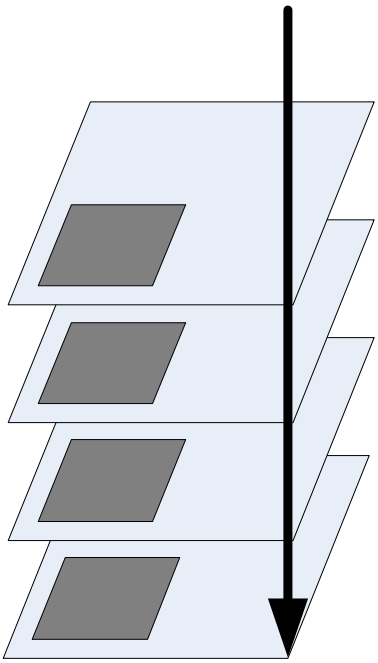


Рис. 3. Процесс декодирования при обычном встраивании изображения в видеоданные случайными частями

Приступим к декодированию изображения. Для этого просто просуммируем массивы МЗБ кадров (рис. 3) всего периода встраивания.

Операция будет иметь следующий вид:

$$Ss = \left[ss_{h,w}\right] ,$$

$$ss_{h,w} = \sum_{f=1}^{F} \left[ls_{h,w}\right]_f , \; h = 1,...,H, \quad w = 1,...,W ,$$

где Ss – суммарная матрица,

h, w – координаты пикселей кадра,

H, W – геометрические размеры кадра,

F – значение периода встраивания,

$\left[ls_{h,w}\right]_f$ – соответствующий бит МЗБ h-го, w-го пикселя f-го кадра.

Подберем пороговое значение ниже значения суммарной матрицы в элементах, соответствующих черным точкам рисунка, но выше, чем в остальных элементах «суммарной матрицы». Соответственно, если значение элемента суммарной матрицы превышает порог, то в результирующей матрице в этом элементе ставится единица, если ниже или равно – то ноль (рис. 4).

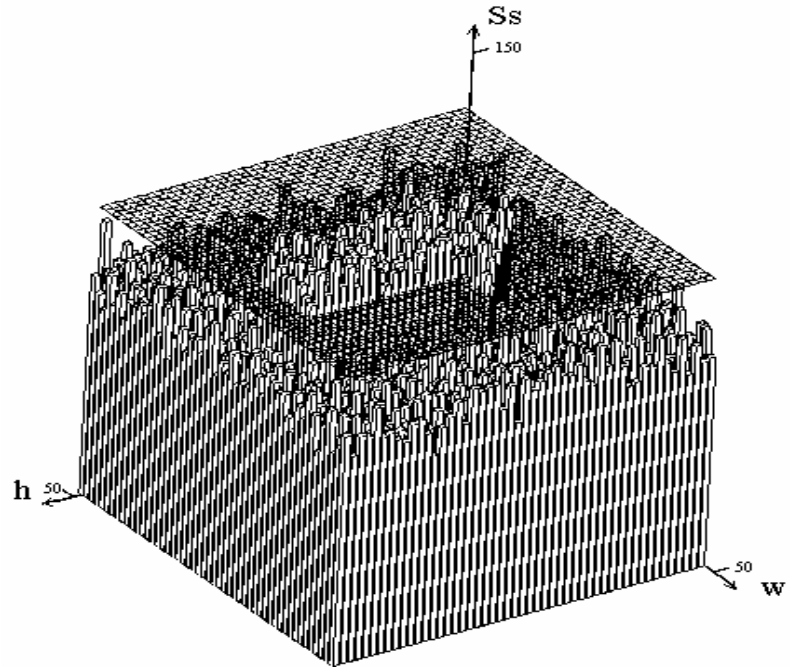


Рис. 4. Суммарная матрица и порог

Методика расчета порога для различных параметров встраивания будет предложена ниже. Результирующую матрицу назовем «матрицей обнаружения».

При встраивании изображения в видеофайл случайными частями с помощью логического суммирования МЗБ кадра разделятся на два вида. Первый – это исходные МЗБ кадра. Как было предположено раньше, $P_{ls} = 0{,}5$. Второй – это элементы, в которых произведено логическое суммирование, т.е. встроена часть стегосообщения (1).

Вероятность появления единицы в точке встраивания выводится на основании взаимной независимости событий существовании единиц в МЗБ кадра и каком-либо элементе маски. Это вероятность суммы двух независимых событий:

$$P_{sts} = P_{ls} + P_{ms} - P_{ls} \cdot P_{ms}, \qquad (1)$$

где P_{sts} – вероятность появления единицы в элементе МЗБ кадра, в котором встроено изображение,

P_{ls} – вероятность существования единицы в исходном МЗБ кадра (элементе первого вида); предполагается, что она равна 0.5.

P_{ms} – вероятность существования единицы в элементе маски.

Соответственно и элементы суммарной матрицы делятся на два вида. Первый вид соответствует исходным МЗБ кадра, второй вид – МЗБ со встроенным стегосообщением.

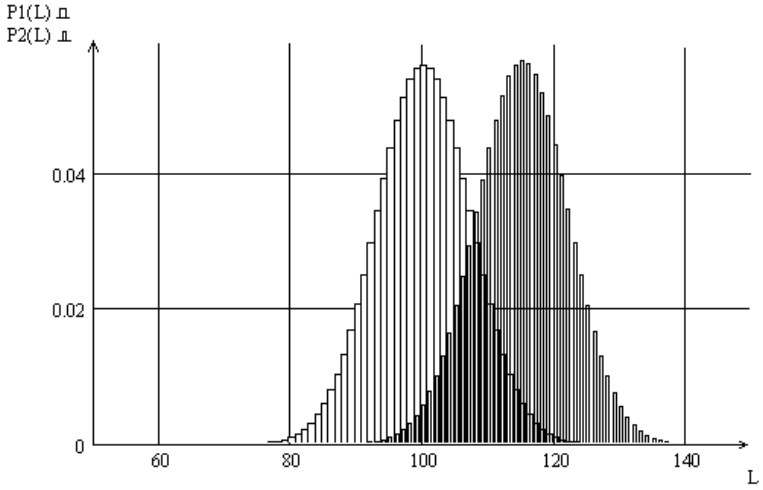


Рис. 5. Ряды распределения значений суммарной матрицы в элементах первого и второго вида при встраивании с помощью логического суммирования

Обозначим символом F период встраивания, а символом L – возможное значение суммарной матрицы массивов МЗБ пикселей кадров, получающейся при обнаружении изображения. По теореме о повторении опытов вероятность какого-либо значения суммарной матрицы в элементе первого вида будет равна выражению (формуле Бернулли):

$$P1(L) = C_L^F \cdot P_{ls}{}^L \cdot (1 - P_{ls})^{F-L}.$$

Аналогично, вероятность какого-либо значения в элементе второго вида можно найти по формуле

$$P2(L) = C_L^F \cdot P_{sts}{}^L \cdot (1 - P_{sts})^{F-L}.$$

Построим на одном графике ряды распределения $P1(L)$, $P2(L)$, $L \in Z$, $L \in (1, F)$ (рис. 5).

Как видно из графика (рис. 5), существуют две четко выраженные области с наибольшей вероятностью появления значений матрицы сумм как в элементах первого вида, так и второго, которые, однако, пересекаются. При установке какого-либо порога появятся вероятности превышения порога в элементах первого вида и появления значений меньше порога в элементах второго вида. Условимся первый вид ошибки (ошибку первого рода) называть ложным обнаружением, второй вид (ошибку второго рода) – пропаданием изображения.

Так как априорные вероятности значений суммарной матрицы и цены ошибок неизвестны, в данной работе для расчета порога применяется критерий минимума суммы условных вероятностей ошибок.

При этом выражение для вычисления порога будет иметь вид

$$T = -F \cdot \ln(1 - P_{ms}) / \ln(-(P_{ms} + 1)/(-1 + P_{ms})),$$

где P_{ms} – вероятность существования единицы в элементе маски,

F – период встраивания.

Задав порог, можно представить вероятность ложного обнаружения как функцию от периода встраивания и плотности единиц в маске

$$P_{fds} = \sum_{l=F}^{T=f(F,P_{ms})} C_l^F \cdot P_{ls}{}^l \cdot (1 - P_{ls})^{F-l},$$

и вероятность пропадания изображения как функцию от периода встраивания и плотности единиц в маске

$$P_{lps} = \sum_{l=1}^{T=f(F,P_{ms})} C_l^F \cdot P_{sts}{}^l \cdot (1 - P_{sts})^{F-l}.$$

Опишем метод встраивания изображения случайными частями с помощью замены.

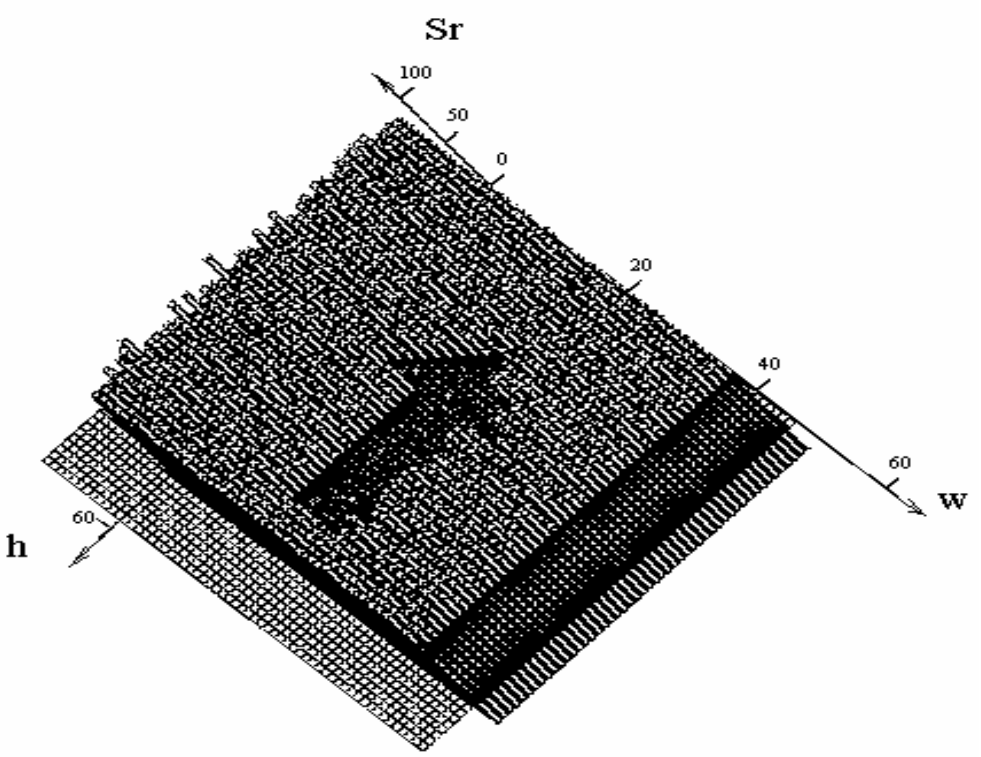


Рис. 6. Установка порога для суммарной матрицы
при встраивании с помощью замены

Создается маска, аналогичная маске на рис. 3, и подобно предыдущему алгоритму встраивание осуществляется в МЗБ кадров периода встраивания, но операция встраивания имеет вид

$$ls_{h0+i,w0+j} = (\overline{mr_{i,j}}) \wedge ls_{h0+i,w0+j},\ i = 0,...,I-1,\quad j = 0,...,J-1,$$

где i, j – координаты пикселей изображения,

I, J – геометрические размеры изображения,

h_0, w_0 – координаты начала встраивания изображения в матрицу МЗБ,

ls_{h_0+i, w_0+j} – соответствующий бит МЗБ,

$mr_{i,j}$ – соответствующий бит маски.

Подобно предыдущему алгоритму декодирование осуществляется с помощью суммирования МЗБ (2).

Процесс установки порога изображён на рис. 6.

$$Sr = \left[sr_{h,w}\right]$$

$$sr_{h,w} = \sum_{f=1}^{F} \left[ls_{h,w}\right]_f \quad h = 1,..., H, \quad w = 1,..., W \qquad (2)$$

где Sr – суммарная матрица,

h, w – координаты пикселей кадра,

H, W – геометрические размеры кадра,

F – значение периода встраивания,

$\left[ls_{h,w}\right]_f$ – соответствующий бит МЗБ h-го, w-го пикселя f-го кадра.

Теперь подберем пороговое значение, которое выше значения суммарной матрицы в элементах, соответствующих черным точкам рисунка, но ниже, чем в остальных элементах суммарной матрицы. Соответственно, если значение элемента суммарной матрицы превышает порог, то в результирующей матрице в этом элементе ставится единица, если ниже или равно – то ноль.

При встраивании изображения в видеофайл случайными частями с помощью замены МЗБ кадра разделятся на два вида. Первый – это исходные МЗБ кадра. Как было предположено раньше, $P_{ls} = 0{,}5$. Второй – это элементы, в которых произведена замена, т.е. встроена часть стегосообщения.

Вероятность появления единицы в элементе встраивания выводится на основании взаимной независимости событий существовании единиц в МЗБ кадра и каком-либо элементе маски. Это вероятность произведения двух независимых событий:

$$P_{str} = P_{ls} \cdot (1 - P_{mr}),$$

где P_{str} – вероятность появления единицы в элементе встраивания стегосообщения (stegomessage),

P_{ls} – вероятность существования единицы в исходном МЗБ кадра (элементе первого вида); предполагается, что она равна 0.5,

P_{mr} – вероятность существования единицы в элементе маски.

Элементы суммарной матрицы также делятся на два вида. Первый вид соответствует исходным МЗБ кадра, второй вид – МЗБ со встроенным стегосообщением. Обозначим символом F период встраивания, а символом L – возможное значение суммарной матрицы массивов МЗБ пикселей кадров, получающейся при обнаружении изображения. По теореме о повторении опытов вероятность какого-либо значения суммарной матрицы в элементе первого вида будет равна выражению (3).

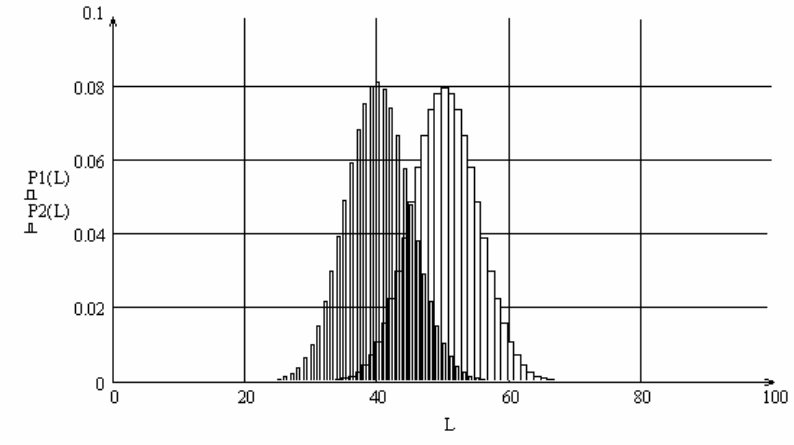


Рис. 7. Ряды распределения значений в элементах первого и второго вида при встраивании с помощью замены

$$P1(L) = C_L^F \cdot P_{ls}{}^L \cdot (1 - P_{ls})^{F-L}. \qquad (3)$$

Аналогично вероятность какого-либо значения в элементе второго вида можно найти по формуле

$$P2(L) = C_L^F \cdot P_{str}{}^L \cdot (1 - P_{str})^{F-L}.$$

Построим на одном графике ряды распределения $P1(L)$, $P2(L)$, $L \in Z$, $L \in (1, F)$ (рис. 7).

Как видно из графика (рис. 7), существуют две четко выраженные области с вероятностью появления значений матрицы сумм как в элементах первого вида, так и второго, которые, однако, пересекаются. При установке какого-либо порога появятся вероятности превышения порога в элементах первого вида (ложное об-

наружение) и появления значений меньше порога в элементах второго вида (пропадание изображения).

Так как априорные вероятности значений суммарной матрицы и цены ошибок неизвестны, в данной работе применяется критерий минимума суммы условных вероятностей ошибок.

После выбора критерия можно записать выражение для вычисления порога:

$$T = F \cdot (\ln(1/(P_{mr} + 1)) / \ln(-(-1 + P_{mr})/(P_{mr} + 1))),$$

где P_{mr} – вероятность существования единицы в элементе маски,

F – период встраивания.

Задав порог, можно представить вероятность ошибки ложного обнаружения как функцию от периода встраивания и плотности единиц в маске

$$P_{fdr} = \sum_{l=1}^{T=f(F,P_{mr})} C_l^F \cdot P_{ls}{}^l \cdot (1 - P_{ls})^{F-l},$$

а также вероятность ошибки пропадания изображения как функцию от периода встраивания и плотности единиц в маске

$$P_{lpr} = \sum_{l=F}^{T=f(F,Pmr)} C_l^F \cdot P_{str}{}^l \cdot (1 - P_{str})^{F-l}.$$

Первая методика защиты видеоконтента от монтажа заключается в выборе параметров встраивания таким образом, чтобы разнести средние значения рядов распределений на рис. 5 и рис. 7 на расстояние «трех сигм» для получения в результате декодирования «чистого», незашумленного изображения. В этом случае при удалении или замене части кадров в матрице декодирования будет появляться шум, свидетельствующий о том, что произведен монтаж изображения.

В третьей главе 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.

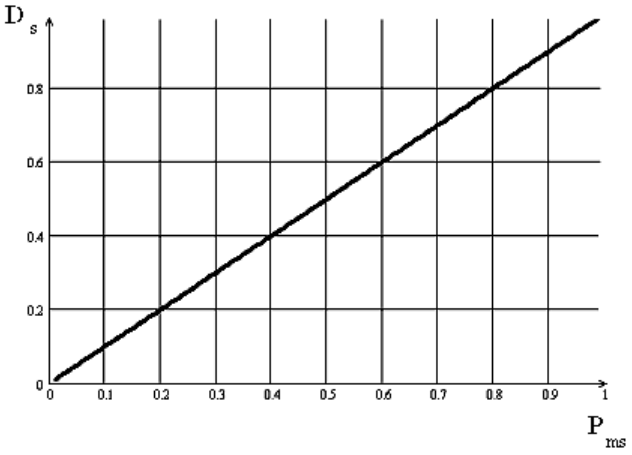
Для оценки эффективности предложенных стегосистем необходимо определить, насколько эти системы искажают контейнер. Меру искажения МЗБ кадра в месте встраивания с помощью логического суммирования можно определить как

$$D_s = \frac{(P_{ms} + P_{ls} - P_{ls} \cdot P_{ms} - P_{ls})}{P_{ls}} = \frac{(P_{ms} - P_{ls} \cdot P_{ms})}{P_{ls}}.$$

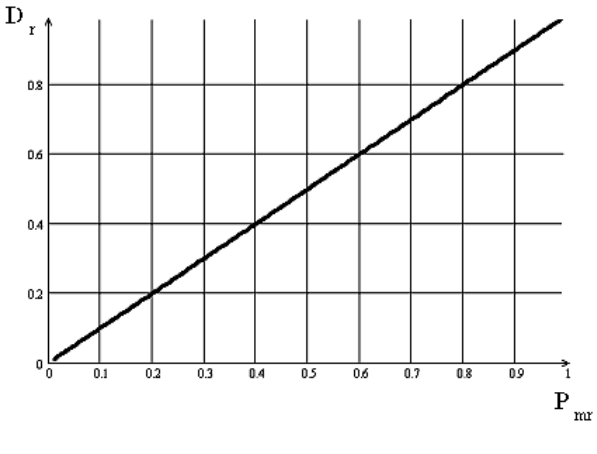
Меру искажения МЗБ кадра в месте встраивания с помощью замены можно определить как

$$D_r = \frac{P_{ls} - P_{ls} \cdot (1 - P_{mr})}{P_{ls}} = P_{mr}.$$

Построим зависимости меры искажения от плотности единиц в маске (рис. 8).



а



б

Рис. 8. Меры искажения массива МЗБ
при встраивании изображения в видеоданные случайными частями:
а – мера искажения при встраивании с помощью логического суммирования,
б – мера искажения при встраивании с помощью замены

Несмотря на различные выражения при $P_{ls} = 0{,}5$, обе меры искажения ведут себя одинаково и равны плотности единиц в маске. Исходя из данной зависимо-

сти, можно говорить о подконтрольной степени искажения видеоданных. Уменьшая степень искажения кадра, можно повышать стегоустойчивость алгоритмов, так как во многих работах по стегоанализу предъявляются требования к минимальному изменению контейнера для обнаружения ЦВЗ.

Достаточное условие обнаружения посредством корреляционного приемника бинарного сигнала в бинарном шуме, разработанное в данном исследовании, позволяет выяснить, когда возможно обнаружение изображения в матрице обнаружения посредством корреляционного приемника.

Очевидно, перед нами встает задача определения условия обнаружения изображения с помощью корреляционного приемника в зависимости от параметров встраивания. Срабатыванием корреляционного приемника назовем событие, когда в точке встраивания изображения мы получаем максимальное значение корреляционной суммы.

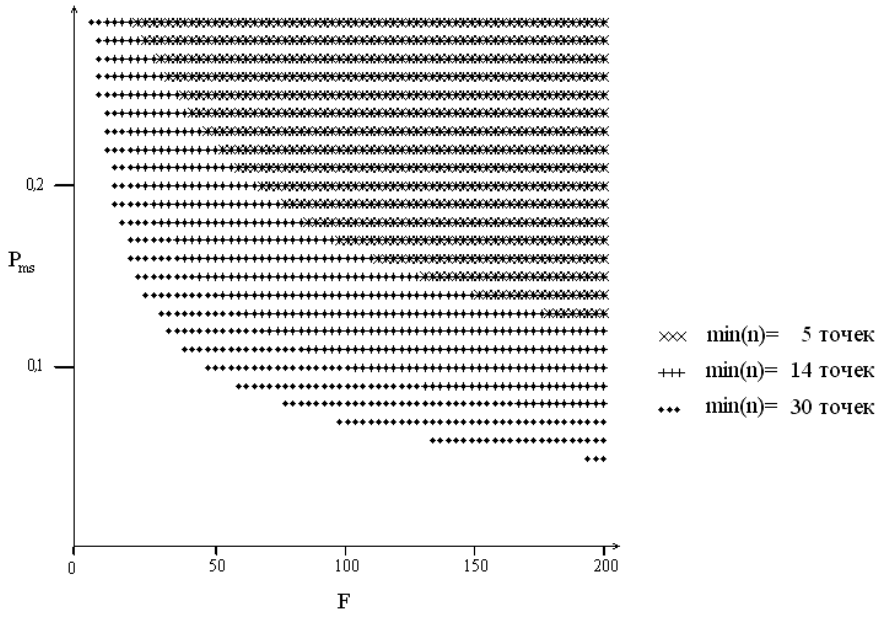


Рис. 9. Зоны возможного обнаружения изображения посредством корреляционного приемника при встраивании изображения случайными частями с помощью логического суммирования

Условием обнаружения изображения с помощью корреляционного приемника является равенство (достаточное условие обнаружения посредством корреляционного приемника бинарного сигнала в бинарном шуме)

$$P_{prev}(\min(n)) = 1 - \varepsilon,$$

где ε задается пользователем, а min(n) – это минимальное количество не совпавших черных точек, которое может получиться при всех возможных сдвигах изображения относительно себя самого.

P_{prev} выражается формулой

$$P_{prev}(n) = \sum_{k=n}^{1} \left[(C_n^k P_{td}^k (1 - P_{td})^{n-k} \cdot [1 - \sum_{i=k}^{n} C_n^i P_{fd}^i (1 - P_{fd})^{n-i})] \right], \qquad (4)$$

где P_{td} – вероятность правильного обнаружения ($(1 - P_{lps})$ или $(1 - P_{lpr})$).

Выражение (4) показывает нам, что условие возможности обнаружения изображения посредством корреляционной функции зависит не только от параметров встраивания, но и от формы встроенного изображения.

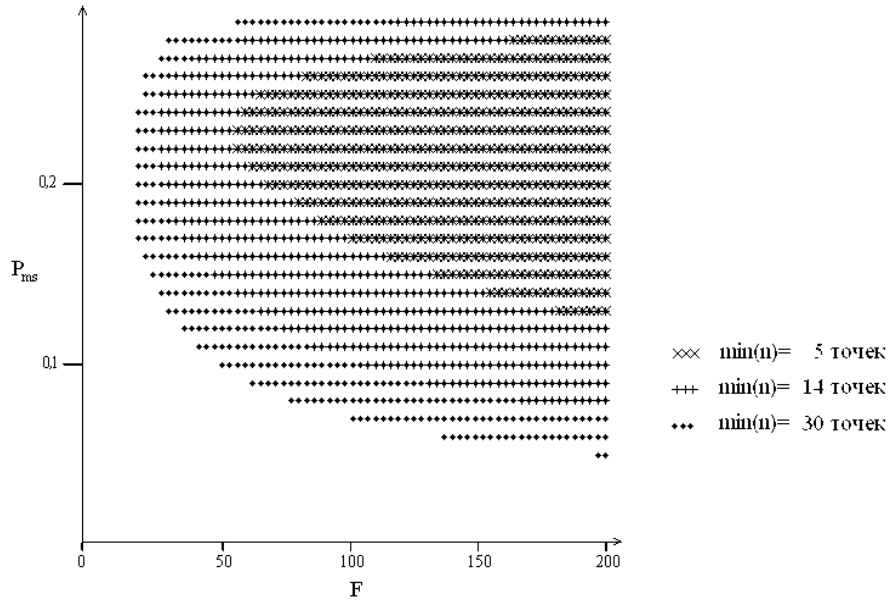


Рис. 10. Зоны возможного обнаружения изображения посредством корреляционного приемника при встраивании изображения случайными частями с помощью замены

Пользуясь данным условием, можно отобразить точками сочетания параметров (рис. 9, 10), при которых возможно обнаружение изображения посредством корреляционного приемника.

Возможно применение данного условия для создания устойчивости к монтажу. Если параметры встраивания взять с границы зон срабатывания, то при вырезании или замене кадров изображение не будет обнаружено корреляционным приемником.

В четвертой главе описана разработанная в данной диссертации методика защиты цифровых доказательств от фальсификации. Описана разработанная в данной работе программа, реализующая методики встраивания изображения в видеоданные случайными частями с помощью логического суммирования и с помощью замены. Описана процедура и приведены таблицы эксперимента, проведенного для тестирования программной реализации.

Для исключения фальсификации записи привлекается эксперт, производящий защиту видеоданных. Запрос на такие услуги может быть сделан любыми заинтересованными лицами, а именно следствием, прокуратурой, стороной обвиняемого. После проведения видеозаписи в присутствии понятых в видеоданные встраивается цифровой водяной знак.

В дальнейшем у заинтересованных лиц могут возникнуть сомнения в подлинности записи. Допустим, кто-то из участников следственного действия может сказать, что не помнит автомобиль, стоявший во дворе дома, или что процесс съемки происходил в другом месте.

В этом случае заинтересованные лица могут сделать запрос на установление подлинности цифровой видеозаписи. Если подлинность видеозаписи не удостоверяется, она исключается из рассмотрения в деле.

Программа, написанная для встраивания, позволяет нарисовать изображение, выбрать файл для встраивания, матрицу цвета, в МЗБ которого будет встраиваться изображение, номер бита (0 – младший, 7 – старший), задать плотность единиц в маске, выбрать период встраивания и место встраивания изображения в МЗБ кадров. Выбирается одна из методик встраивания, отличающихся друг от друга видом битовых операций, осуществляющихся между маской и участками встраивания в МЗБ кадров. Соответственно, декодированное изображение в зависимости от методики имеет различный вид.

Программа написана для операционной системы Windows XP на языке программирования C++, программа занимает 732 КБ и работает с файлами с расширением avi формата RGB.

В заключении представлены основные результаты работы, сформулированы общие выводы относительно выполненной работы и даны рекомендации для дальнейших исследований.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. Впервые разработана методика защиты цифровых доказательств от фальсификации с помощью технологий цифрового водяного знака.

2. Впервые сформулированы требования к цифровому водяному знаку для защиты цифровых доказательств от фальсификации.

3. Разработаны новые методики встраивания цифрового водяного знака:

1) скрытым встраиванием изображения случайными частями с помощью логического суммирования;

2) скрытым встраиванием изображения случайными частями с помощью замены.

Данные методики удовлетворяют сформулированным требованиям к цифровому водяному знаку для защиты цифровых доказательств от фальсификации.

4. Определены пределы применения разработанных методик встраивания цифрового водяного знака. В рамках решения задачи

1) впервые получено достаточное условие обнаружения посредством корреляционного приемника бинарного сигнала в бинарном шуме. В данной работе оно позволяет сформулировать требования к встраиваемому изображению;

2) рассмотрены виды ошибок, возникающие при декодировании изображений, встроенных в видеоданные случайными частями, такие, как ложное обнаружение и пропадание изображения;

3) оценена мера искажения, вносимого в контейнер при использовании данных методик, сделан вывод о регулируемой мере искажения.

4. Разработана программа, реализующая методики скрытого встраивания изображения случайными частями. Экспериментальные оценки ошибок, возникающих при декодировании встроенных изображений, имеют малое расхождение с теоретическими оценками, что говорит о возможности применения методик на практике.

ОСНОВНЫЕ ПОЛОЖЕНИЯ ДИССЕРТАЦИИ ОПУБЛИКОВАНЫ В СЛЕДУЮЩИХ РАБОТАХ:

В изданиях, рекомендованных ВАК:

1. Ренжин П.А. Способ внедрения стегосообщения в видеофайл случайными частями с помощью замены // «Вопросы радиоэлектроники», сер. ОТ. 2008. Вып. 2. С. 153–157.

2. Renzhin P.A. Limits of application of randomized parts embedding of picture in a videodata by logical summation (Ренжин П.А. Пределы применения способа встраивания изображения в видеоданные случайными частями с помощью логического суммирования) // Системы управления и информационные технологии. 2007. № 4.1 (30). С. 189–191.

В остальных изданиях:

3. Информационный образовательный ресурс локального доступа <Программа скрытого встраивания изображения в видеоданные случайными частями> для студентов всех форм обучения специальности <Информационная безопасность>: свидетельство о регистрации электронного ресурса № 15588 / П.А. Ренжин. № 50201000653; заявл. 23.03.2010; опубл. 04.04.2010 // Алгоритмы и программы. 2010. № 4. 1 с.

4. Информационный образовательный ресурс <Основы цифрового водяного знака> свидетельство об отраслевой регистрации разработки № 8169 / П.А. Ренжин. №50200700875, заявл. 02.04.2007, опубл. 09.04.2007 // Инновации в науке и образовании. 2007. №3. 1 с.

5. Ренжин П.А. Вычисление порога обнаружения при внедрении изображения в видеоданные случайными частями с помощью замены // Технологии Microsoft в теории и практике программирования. Новосибирск, 2008. 1–2 марта. С. 48–49.

6. Ренжин П.А. Программа скрытого встраивания изображения в видеоданные случайными частями // Технологии Microsoft в теории и практике программирования. 2010. 23–24 марта. С. 226–227.

7. Ренжин П.А., Файзуллин Р.Т. Методика защиты цифровых видеодоказательств от фальсификации встраиванием цифрового водяного знака // Научная сессия ТУСУР-2010: в 5 ч. Томск, 2010. 4–7 мая. Ч. 3. С. 191–192.

8. Файзуллин Р.Т., Ренжин П.А. Пределы применения способа встраивания изображения в видеопоследовательность случайными частями с помощью замены // Материалы межрегионального информационного конгресса. Омск, 2008. 1–3 октября. С. 262–269.

9. Renzhin P.A. Randomized parts embedding of digital watermarks in a video data by logical summation (Ренжин П.А. Способ встраивания цифрового водяного знака в видеоданные с помощью логического суммирования) // Информационные технологии моделирования и управления. 2007. № 4 (38). С. 450–454.