На правах рукописи

Грушо Николай Александрович

МОДЕЛИ И МЕТОДЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ СТАТИСТИЧЕСКОГО ПОИСКА ЗАДАННЫХ ЗАКОНОМЕРНОСТЕЙ В ПОСЛЕДОВАТЕЛЬНОСТЯХ ИЗОБРАЖЕНИЙ В ЗАДАЧАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

Автореферат
диссертации на соискание ученой степени
кандидата физико-математических наук

Автор:

Москва – 2008

Работа выполнена в Институте информационных наук и технологий безопасности Российского государственного гуманитарного университета

Научный руководитель:	доктор физ.-мат. наук, профессор Грушо Александр Александрович
Официальные оппоненты:	доктор технических наук, академик РАЕН, чл.-корр. Академии криптографии РФ Никонов Владимир Глебович
	кандидат физико-математических наук, доцент Применко Эдуард Андреевич
Ведущая организация:	Институт проблем информатики РАН

Защита состоится «24» июня 2009г. в 14:00 часов на заседании диссертационного совета ДМ 212.130.08 в ЦИТиС по адресу:
123557, г. Москва, Пресненский Вал, 19.

С диссертацией можно ознакомиться на сайте МИФИ http://www.mephi.ru и в библиотеке МИФИ

Отзывы в двух экземплярах, заверенные печатью, просьба направлять по адресу: 115409, Москва, Каширское ш., 31, диссертационные советы МИФИ (тел. 323-95-26)

Автореферат разослан «__»_____ 2009 г.

Ученый секретарь
диссертационного совета Горбатов В.С.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. Оценка эффективности поиска заданных закономерностей в последовательностях изображений необходима в решении ряда проблем информационной безопасности.

Защита интеллектуальной собственности может быть построена на встраивании специальных закономерностей в изображения, получивших название «метки» (Watermarks). Например, таки образом защищают права на репродукции картин известных художников из уникальных коллекций. Основное требование к таким меткам – трудность их выявления. Если метка обнаружена и локализована, то ее легко можно изъять из цифрового изображения или видеоряда, чтобы нарушить права интеллектуальной собственности.

Ложные цифровые изображения (или видеоряды), предоставленные в качестве доказательства в суд или в средства массовой информации, требуют выявления признаков фальсификации. Эти признаки, вообще говоря, известны, но мастерство злоумышленника состоит в том, чтобы делать эти признаки малозаметными. Отметим, что указанные признаки проявляются лучше в видеорядах, чем в одинарных изображениях. Например, стабильность печати в заводских условиях значительно выше, чем в кустарных. Поэтому комбинация значений многих характеристик, полученная в кустарных условиях подделок, значительно отличается от изделий промышленного производства.

Известны случаи психологического воздействия на человека через специально сформированные вставки в видеоряды.

Наконец, развивается скрытая передача информации с помощью видеорядов.

Все перечисленные примеры задач выявления закономерностей в видеорядах можно объединить под названием «стеганография в изображениях в широком смысле». Отметим, что термин «стеганография»

обычно трактуется в более узком смысле. Искомые закономерности в последовательностях изображений для краткости будем называть вставками.

Такая стеганография в широком смысле играет все большую роль в проблемах обеспечения информационной безопасности. Методы выявления вставок в последовательностях изображений требуют больших вычислительных ресурсов и их реализация программно-аппаратными комплексами является дорогостоящей. Поэтому предварительно необходима оценка эффективности выявления вставок в последовательности изображений. Разработке методов оценки эффективности статистического поиска вставок различного типа посвящена данная диссертация. Изложенные выше аргументы показывают, что тема диссертации является актуальной.

Предметом исследования в диссертации является обобщенная в указанном выше смысле стеганография в последовательностях изображений или видеорядах.

Объектами исследования являются статистические методы выявления вставок в последовательностях изображений.

Цель диссертационной работы. Цели диссертации – разработать модели и методы оценки эффективности поиска вставок в последовательности изображений.

Направление исследований. Исследования ведутся по нескольким направлениям оценки эффективности статистических методов выявления вставок последовательностях изображений:

- исследуется возможность выявления вставок статистическими методами;
- исследуется взаимосвязь вычислительной сложности алгоритмов выявления и эффективности выявления вставок в последовательностях изображений;
- исследуется техническая реализуемость методов выявления некоторых видов вставок.

При этом в работе ставились следующие задачи.

1. Разработать модели невыявляемости вставок в последовательностях изображений. Определить понятие качества сокрытия вставок в последовательностях изображений. Выразить понятие эффективности поиска вставок через параметры моделей, описывающих методы поиска.
2. Определить условия, при которых поиск вставок в последовательности изображений не эффективен, и условия, при которых хотя бы теоретически есть возможность нахождения вставок.
3. Исследовать вопросы реализуемости поиска и потенциальные потери эффективности, которые возможны при технической реализации и упрощении алгоритмов поиска.

Методы исследований, достоверность и обоснованность результатов. В работе используются методы математического моделирования, опирающиеся на теорию вероятностей, математическую статистику, топологию и теорию сложности. Неэффективность статистического поиска вставок в работе моделируется отсутствием состоятельных последовательностей критериев. Существование таких последовательностей исследуется вероятностными и топологическими методами. Кроме того, работа опирается на эксперименты, подтверждающие техническую реализуемость и целесообразность поиска вставок в последовательностях изображений.

Научная новизна. Большая часть работ по стеганографии направлена на создание методов скрытия информации. При этом под скрытием чаще всего понимаются примитивные оценки или субъективное мнение. Например, при оценке стойкости стеганографических методов с помощью отношения сигнал/шум чаще всего делается предположение о нормальной распределенности сигнала и шума. В видеорядах такие модели совсем неприемлемы. Исследование вопросов существования состоятельных последовательностей статистических критериев в связи со стойкостью скрытых каналов началось с работ Грушо А.А. и Тимониной Е.Е. в 2005-2006

гг. Однако в этих исследованиях не рассматривались условия не существования состоятельных последовательностей статистических критериев. А именно такие условия определяют неэффективность поиска вставок. Поэтому исследования диссертации в этом направлении являются новыми.

Эффективности поиска вставок в последовательности изображений уделялось мало внимания в научной литературе. И хотя методы стеганографии в последовательности изображений разрабатываются, работ, посвященных оценке эффективности поиска вставок в последовательностях изображений, автор диссертации не нашел. Поэтому в диссертации проведены исследования, посвященные существованию и не существованию состоятельных последовательностей статистических критериев для выявления вставок в последовательности изображений.

Взаимосвязь сложности вычисления статистических критериев и состоятельности последовательности статистических критериев на заданном множестве альтернатив в литературе не рассматривались. Поэтому результаты диссертации в этой области являются новыми.

Основные положения, выносимые на защиту. На защиту выносятся следующие основные положения.

1. Определена эффективность поиска вставок, основанная на сложности или невозможности выявления вставок в последовательностях изображений. Это определение конкретизировано в отношении статистических методов выявления вставок в последовательности изображений. Асимптотически невыявляемая статистическими методами вставка характеризуется отсутствием состоятельной последовательности критериев для ее выявления. Для таких задач статистические методы поиска вставок не эффективны.

2. Найдены достаточные условия отсутствия состоятельных последовательностей статистических критериев в дискретных схемах, которые являются моделями вставок в видеорядах.
3. Для аддитивных вставок в последовательности изображений найден полный спектр условий, когда существуют или не существуют состоятельные статистические методы их выявления. Разработан программно-аппаратный макет для реализации эффективного поиска указанных вставок в последовательностях изображений. Это позволило определить около 200 сайтов, в которых могут использоваться вставки в последовательностях изображений.
4. Выявлен эффект фиктивного упрощения статистических процедур выявления вставок в последовательностях изображений. Этот эффект связан с асимптотическим снижением оценок сложности критериев при условии сохранения состоятельности статистических методов выявления вставок. Выработаны рекомендации, позволяющие избегать фиктивных упрощений. Одновременно разработаны методы реального упрощения статистических методов выявления вставок.
5. Построен пример, когда любое реальное упрощение в последовательности статистических критериев приводит к потере состоятельности, т.е. к потере эффективности статистических методов выявления вставок в последовательности изображений.

Практическая полезность работы. Разработанные в диссертации методы оценки эффективности поиска вставок в последовательности изображений будут полезны разработчикам систем защиты от атак на информационные системы с помощью скрытых каналов. Кроме того, эти исследования будут полезны при оценке качества методов, используемых для защиты целостности и защиты интеллектуальной собственности. Полученные в диссертации результаты будут использоваться в учебном процессе в качестве примера оценки эффективности средств защиты.

В работе не ставилась задача по созданию промышленного образца устройства для поиска вставок в последовательности изображений. Проведенная в диссертации работа по технической реализации системы поиска вставок имела целью создание работоспособного программно-аппаратного макета для проверки технической реализуемости. Данный макет также позволил исследовать практические возможности анализа видеорядов с целью поиска признаков вставок в изображениях. С помощью созданного программно-аппаратного макета выявлены сайты Интернет, анимация которых позволяет скрывать вставки рассматриваемых типов. Материалы исследований переданы для использования в НИР «Мозг» Академии криптографии РФ. Созданный макет использовался в учебном процессе на факультете защиты информации в РГГУ.

Апробация работы. Результаты диссертации прошли апробацию на 6 международных конференциях, а также докладывались на семинаре кафедры компьютерной безопасности РГГУ.

Публикации. По материалам диссертации опубликовано 10 работ, при этом основные положения диссертации, выносимые на защиту, опубликованы в 4 статьях в изданиях, рекомендованных ВАК по данной специальности. В работах, написанных в соавторстве, автору диссертации принадлежат результаты, внесенные в диссертацию.

Структура и объем диссертации. Диссертация состоит из введения, трех глав, заключения и списка литературы из 59 наименований. Объем диссертации 104 стр.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении определяется объект исследования, обосновывается актуальность выбранной темы, определяется научная проблема, решаемая в диссертации, и формулируются направления исследований, указываются

методы исследования, а также формулируются положения, выносимые на защиту.

В первой главе приведено обоснование задач диссертации. Рассматриваются проблемы поиска вставок в последовательностях изображений. Очерчен круг смежных вопросов и достижения, опубликованные в зарубежных и отечественных работах. Предложен метод использования стеганографии для защиты целостности сообщений при атаках с помощью внедрения инструкций для программно-аппаратных агентов нарушителя безопасности в шифртексты сообщений. Основная идея метода в следующем.

Пусть легальная информация встроена в некоторый легальный контейнер с помощью метода стеганографии. На приемном конце вставка выделяется из контейнера, а контейнер отбрасывается. Вставка обрабатывается по алгоритму для входящих сообщений и передается пользователю.

Неэффективность поиска закономерностей в видеорядах имеет аналогичную природу с обнаружением вторжений в компьютерные системы. В частности, рассмотрение большого количества различных характеристик влечет большое количество ложных тревог. При отсутствии дополнительной информации такие ложные вставки не дают возможности выделять и эффективно анализировать истинные вставки. Наоборот, вероятность пропуска истинных вставок в таких условиях может приближаться к единице. Эта ситуация формально описывается отсутствием состоятельной последовательности статистических критериев выделения вставок. Поэтому в диссертации неэффективность поиска вставок статистическими методами определяется как отсутствие состоятельной последовательности статистических критериев.

Существует мнение, что вставки необязательно выявлять. Достаточно преобразовать изображение в другой формат и вставки исчезнут. В связи с этим в диссертации предложении новый метод стеганографии в видеорядах,

который является неуничтожаемым при любых преобразованиях изображений в видеоряду, сохраняющих исходные картинки. Метод не меняет структуру каждого из изображений видеоряда, но использует возможности межкадровых изменений изображений. При этом используется модуляция статистических параметров случайных процессов видеоряда. Технически такие вставки легко реализуются, используя векторную модель изображений. Отсюда следует, что преобразование формата изображения не всегда приводит к уничтожению вставок. Даже в простейшем виде характерные признаки рассматриваемого метода стеганографии в видеорядах найдены на многих сайтах и видеофильмах. Эти признаки связаны как с анимацией баннеров на сайтах, так и с помехами, возникающими в результате аналого-цифровых и других преобразований изображений. Работа проведена с помощью макета программно-аппаратного комплекса по поиску вставок в видеоряды. В дальнейшем приведенная модель стеганографических вставок в видеорядах используется для конкретизации теоретических положений и для проверки технической реализуемости.

Рассмотрена проблема алгоритмической реализации поиска вставок в последовательности изображений. В данной работе исследуется переборный алгоритм поиска мерцающих пикселов в предположении о том, что визуальное выявление таких пикселов невозможно, то есть контролер не может визуальным просмотром определить наличие вставки. С целью такого поиска формируемый в компьютере видеоряд запоминается и анализируется в режиме off-line на отдельном компьютере с помощью специального программного обеспечения.

Рассматриваются две задачи. Первая задача состоит в отыскании хотя бы одного мерцающего пиксела, закон изменения значения которого можно отнести к вставке. Вторая задача состоит в выявлении всех мерцающих пикселов с тем, чтобы в последующем решать задачу об интегральном содержании вставки системы.

Для алгоритма последовательного поиска мерцающих пикселов оценены его характеристики. С этой целью используется представление кадра изображения на экране монитора в виде вектора $X = (x_1,...,x_N)$ длины N, компоненты которого являются натуральными числами. Считаем, что для определения факта мерцания одного пиксела требуется наблюдение за этим пикселом в течение l кадров. Поэтому, зафиксировав l кадров видеоряда, можно вести последовательный просмотр изменения значения каждого пиксела в произвольной фиксированной заранее последовательности. Пусть для организации вставки используются m пикселов. В этом случае можно считать, что выбор этих пикселов осуществляется случайно и равновероятно и вероятность любого такого выбора m пикселов равна $\frac{1}{\binom{N}{m}}$.

Асимптотическая оценка среднего числа шагов до первого мерцающего пиксела (при N растущем и m постоянном) равна $\frac{N}{m+1}(1+\mathrm{o}(1))$.

При этих же условиях среднее число шагов для выявления всех мерцающих пикселов оценивается величиной $\mathrm{E}\mu = \frac{Nm}{m+1}\left(1+o(1)\right)$.

В первой главе показано, что поиск вставок является дорогим и трудоемким процессом. Поэтому возникает вопрос об эффективности такого поиска. Отсюда сформулированы основные задачи дальнейших исследований:

- исследовать условия применимости статистических методов к задаче выявления вставок в изображения;
- исследовать связи статистических методов выявления вставок и сложности алгоритмов, реализующих эти методы.

В первом параграфе второй главы приведены некоторые известные в рассматриваемой области результаты и доказано небольшое обобщение

теоремы о существовании состоятельной последовательности критериев для замкнутых подпространств Тихоновского произведения конечных множеств.

Во втором параграфе главы 2 приведены основные результаты автора об условиях не существования состоятельных последовательностей статистических критериев выявления вставок.

Пусть $X = \{x_1,...,x_m\}$ – конечное множество, которое определяет последовательность конечных множеств $X, X^2,...,X^n,...$. На каждом из множеств этой последовательности заданы вероятностные меры

$$\{P_{0,n}(x_{i_1},...,x_{i_n}),\ (x_{i_1},...,x_{i_n}) \in X^n\}, \qquad (2.2.1)$$

$$\{P_{1,\theta,n}(x_{i_1},...,x_{i_n}),\ (x_{i_1},...,x_{i_n}) \in X^n,\ \theta \in \Theta\}, \qquad (2.2.2)$$

Обозначим пространство бесконечных последовательностей

$$X^\infty = \{\alpha = (x_{i_1},...,x_{i_n},...),\ x_{i_n} \in X,\ n = 1,2,...\}.$$

Пусть $(x_{i_1},...,x_{i_n}) \times X^\infty$, $x_{i_n} \in X$, n=1,2,..., – элементарное цилиндрическое множество в X^∞, цилиндрическое множество I_n есть конечное объединение элементарных цилиндрических множеств, а $\mathcal{A}$ –минимальная σ-алгебра, порожденная всеми цилиндрическими множествами.

Пусть вероятностные меры, определяемые формулами (2.2.1) и (2.2.2.), являются согласованными семействами конечномерных распределений. Тогда $\{P_{0,n}(x_{i_1},...,x_{i_n})\}$ определяет единственную вероятностную меру P_0 на измеримом пространстве $\{X^\infty, \mathcal{A}\}$.

Для каждого $\theta \in \Theta$ согласованное семейство конечномерных распределений $\{P_{1,\theta,n}(x_{i_1},...,x_{i_n})\}$ определяет единственную вероятностную меру $P_{1,\theta}$ на пространстве $\{X^\infty, \mathcal{A}\}$.

Рассматривается простая гипотеза $H_0 : P_0$ против сложной альтернативы $H_1 : \{P_{1,\theta},\ \theta \in \Theta\}$. Для задания критерия проверки гипотезы

H_0 против H_1 на пространстве $\{X^\infty, \mathcal{A}\}$ при уровне значимости α необходимо определить критическое множество $S \in \mathcal{A}$ такое, что $P_0(S) < \alpha$. Мощность данного критерия – это функция от θ: $W(\theta) = P_{1,\theta}(S)$.

Рассмотрим последовательность критериев проверки H_0 против альтернативы H_1 с критическими множествами $S_1, S_2, ...$, такую, что

$$\lim_{k\to\infty} P_0(S_k) = 0. \qquad (2.2.3)$$

Определение 2.2.1. Последовательность критериев с критическими множествами $S_1, S_2, ...$, для проверки H_0 против альтернативы H_1 называется состоятельной, если выполняется условие (2.2.3) и для каждого $\theta \in \Theta$:

$$\lim_{k\to\infty} W_k(\theta) = \lim_{k\to\infty} P_{1,\theta}(S_k) = 1.$$

Обозначим через S_k, k=1,2,..., последовательность критических множеств для критериев, проверяющих гипотезу H_0 против альтернативы H_1.

Определение 2.2.2. Последовательность критериев для проверки H_0 против альтернативы H_1 с критическими множествами $S_1, S_2, ...$, удовлетворяет условию (*), если существует $\lim_{k\to\infty} S_k = S$.

Теорема 2.2.1. *Пусть для каждого* $A \in \mathcal{A}$ *такого, что* $P_0(A)$=1 *существует* $\theta \in \Theta$, *что* $P_{1,\theta}(A) > 0$. *Тогда в классе последовательностей тестов, удовлетворяющих условию* (*), *не существует состоятельной последовательности критериев*.

Теорема 2.2.2. *Если существует состоятельная последовательность критериев с критическими множествами* $S_1, S_2, ...$, *для проверки гипотезы* H_0 *против альтернативы* H_1, *то существует состоятельная последовательность критериев, удовлетворяющая условию* (*).

Таким образом, построена состоятельная последовательность критериев, удовлетворяющая условию (*). Отсюда доказана основная теорема.

Теорема 2.2.3. *Пусть для каждого* $A \in \mathcal{A}$ *такого, что* $P_0(A)=1$ *существует* $\theta \in \Theta$, *что* $P_{1,\theta}(A)>0$. *Тогда не существует состоятельной последовательности критериев для проверки гипотезы* H_0 *против альтернативы* H_1.

В частности для случая проверки наличия вставок получаем следующую теорему.

Теорема 2.2.4. *Пусть для каждого* $A \in \mathcal{A}$ *такого, что* $P_0(A)=1$ *существует* $\theta \in \Theta$, *что* $P_{1,\theta}(A)>0$. *Тогда не существует состоятельной последовательности критериев, проверяющих гипотезы* H_{0,n_k} *против альтернатив* H_{1,n_k} *по любой подпоследовательности*.

В параграфе 3 главы 2 теоретические результаты параграфа 2 конкретизированы для случая вставок, встроенных с помощью аддитивного наложения вставки на изображения видеоряда. Здесь удалось получить полный спектр условий, когда существуют или не существуют состоятельные последовательности критериев для выделения таких вставок.

Пусть задано конечное множество $X_1 = \{x_1,...,x_m\}$ допустимых цифровых изображений. Каждое изображение представляет собой слово $x = (y_1,...,y_N)$ фиксированной длины *N*, на каждом месте которого стоит ограниченное целое число $0 < c_2 \le y_i \le c_1$, i=1,...,*N*. Обозначим через $z_n(t)$, t=1,...,*n*, последовательности длины *n* изображений из X_1 и вектора $(z_n(t),\ t = 1,2,...,n) \in X_1^n$. Множество допустимых последовательностей $z_n(t)$, t=1,...,*n*, длины *n* обозначим через μ_n, $\mu_n \subseteq X_1^n$.

Рассмотрим $F_n = \{ f_n(t),\ t = 1,2,...,n \}$ – множество допустимых вставок длины *n* в изображениях. Каждая вставка представляет собой последовательность длины *n* целочисленных векторов $f_n(t) = (u_1^t,...,u_N^t)$

длины *N*. Каждое значение в таких векторах ограничено $\left|u_i^t\right| < c$. Допустим, что вместе с каждой вставкой $f_n(t)$ вставка $-f_n(t) = (-u_1^t,..., -u_N^t)$ входит в F_n. Вставки встраиваются в последовательность изображений $z_n(t)$ аддитивно, то есть если преобразуется последовательность изображений $z_n(t)$ и в нее встраивается вставка $f_n(t) \in F_n$, то преобразованная последовательность получается по формуле

$$\alpha_n(t) = z_n(t) + f_n(t), \quad t=1,...,n,$$

где сложение представляется как сумма целочисленных векторов размера *N*.

Ясно, что для каждой координаты $t=1,...,n$, суммарного вектора $\alpha_n(t)$ являются целыми числами в границах $[c_2 - c; c_1 + c]$.

Предположим, что $c_2 - c > 0$. Обозначим $X = \{v_1,...,v_r\}$ – множество изображений, получаемых из X_1 путем всевозможных вариаций каждой целочисленной компоненты *y* исходного изображения вокруг своего значения в пределах $[y - c; y + c]$. Ясно, что $X_1^n \subseteq X^n$ и

$$\{\alpha_n(t), \quad t = 1,2,...,n\} \subseteq X^n.$$

Обозначим $X^\infty = \{\alpha = (v_{i_1},...,v_{i_n},...), \; v_{ij} \in X, \; i = 1,2...\}$. На пространстве X^∞ рассмотрим цилиндрические множества и σ-алгебру $\mathcal{A}$, порожденную цилиндрическими множествами. Пусть на множествах μ_n, $n = 1,2...$, $\mu_n \subseteq X_1^n \subseteq X^n$, определены согласованные вероятностные меры $P_{0,n}$. Тогда на $(X^\infty, \mathcal{A})$ порождена единственная вероятностная мера P_0, соответствующая допустимым последовательностям изображений. Если рассматривать $\mu_n \times X^\infty = I_n$ как цилиндрическое множество в X^∞, то $I_n \supseteq I_{n+1}$ и существует $\lim\limits_{n\to\infty} I_n = \bigcap\limits_{n=1}^{\infty} I_n = M$. M – измеримое множество в $\mathcal{A}$,

замкнутое в Тихоновских произведениях X^∞ и мера P_0 сосредоточена на последовательностях из M, то есть $P_0\ (M)=1$.

Обозначим $F = \bigcup_{n=1}^{\infty} F_n$ – множество вставок конечной длины и тогда F не более, чем счетное множество. Будем считать, что вставок $f_n(t),\ t=1,2,...,n$, все координаты которых тождественно равны 0, в F нет.

Для каждого $f \in F$ множество $M+f$ является $\mathcal{A}$-измеримым.

Для каждого $f \in F$ пусть $f + \varnothing = \varnothing$. Определим последовательность мер на X^n, если $D_n \subseteq \mu_n$, то

$$D_n + f(t)|_{1,...,n} \subseteq X^n,$$

$$P_{1,f,n}(D_n + f(t)|_{1,...,n}) = P_{0,n}(D_n),$$

$$1 = P_{1,f,n}\left(\bigcup_{D_n \subseteq \mu_n} \left(D_n + f(t)|_{1,...,n}\right)\right).$$

Так как меры $P_{0,n}$ согласованы, то для каждого f меры $P_{1,f,n}$, $n \geq N$, согласованы. Тогда для каждого $f \in F$ определена единственная мера $P_{1,f}$ на $(X^\infty, \mathcal{A})$. Эта мера сосредоточена на множестве $M + f$ и это замкнутое множество в X^∞.

Выполняется равенство для каждого $A \in \mathcal{A}$

$$P_{0,n}(A \cap M) = P_{1,f}\ (A \cap M + f).$$

Рассмотрим несколько случаев. Первый случай, когда $M \cap (M + F) = \varnothing$, то есть любая вставка из F выводит последовательность изображений за класс допустимых. В этом случае показано, что существуют состоятельные последовательности критериев.

Обозначим множество $D = M \cap (M + F)$. Выделим два случая: 1) $P_0(D)=0$, и 2) $P_0(D)>0$. В случае 1) можно построить состоятельную

последовательность критериев. В случае $P_0(D)>0$ нет состоятельной последовательности критериев.

В первом параграфе главы 3 исследована связь эффективности выявления вставок в видеорядах, т.е. состоятельности статистических критериев, и асимптотической сложности их вычисления.

Пусть P_0 – вероятностная мера на измеримом пространстве $(X^\infty, \mathcal{A})$. Кроме того, пусть задано семейство вероятностных мер P_θ, $\theta \in \Theta$, на том же измеримом пространстве.

Рассмотрим проекции введенных вероятностных мер на первые n координат случайных последовательностей из X^∞ и обозначим их соответственно $P_{0,n}$ и $P_{\theta,n}$. Относительно данных мер рассмотрим для каждого n задачу проверки статистической гипотезы $H_{0,n}: P_{0,n}$ против сложной альтернативы $H_{1,n}: \{P_{\theta,n},\ \theta \in \Theta\}$. Критерий T_n уровня значимости α описывается критическим множеством S_n, $P_{0,n} \le \alpha$ и мощностью критерия $W_n(\theta) = P_{\theta,n}(S_n)$.

В этом параграфе использовалось эквивалентное определение состоятельности последовательности критериев T_n, $n = 1,2,....$ Последовательность статистических критериев с критическими множествами S_n называется состоятельной, если для каждого $\alpha > 0$ мощность критерия $W_n(\theta) \to 1$, $n \to \infty$, для каждого $\theta \in \Theta$.

Применение критерия представляет собой работу вычислительного алгоритма. Этот алгоритм по наблюденному вектору на X^n вычисляет, принадлежит ли данный вектор множеству S_n или его дополнению. Если вектор принадлежит S_n, то гипотеза $H_{0,n}$ отвергается. Если наблюденные вектор принадлежит дополнению $X^n \setminus S_n$, то говорят, что наблюдения не противоречат гипотезе $H_{0,n}$, т.е. гипотеза не отвергается, или, иначе, принимается. Таким образом, реализацию статистического критерия можно

описать функцией принадлежности полученного в наблюдении случайного элемента критическому множеству критерия. В дискретных задачах можно говорить о сложности вычисления функции принадлежности некоторого элемента заданному множеству. Таким образом, можно говорить о сложности вычисления статистического критерия. В рассмотренной выше модели мы имеем последовательность статистических критериев для каждого n при $n \to \infty$. Отсюда можно получить асимптотическую оценку сложности последовательности критериев. Оценки сложности определяются количеством операций и объемом памяти, которые необходимы алгоритму, реализующему функцию. Далее рассматриваются оценки количества операций в зависимости от n.

Теорема 3.1.1. *Для любой состоятельной последовательности критериев произвольного уровня* α *с критическими множествами* S_n, n= 1, 2,..., *для проверки* $H_{0,n}$ *против* $H_{1,n}$ *существует состоятельная последовательность критериев уровня* α *с критическими множествами* S'_n, n= 1, 2,..., *сложность которой асимптотически мала по сравнению со сложностью исходных критериев*.

Однако упрощение для последовательности критериев, по сути, оказывается фиктивным. Для того, чтобы не допускать фиктивного упрощения вычисления принадлежности наблюденных значений к критическим множествам в последовательности критериев необходимо накладывать дополнительные ограничения на классы рассматриваемых критериев. Показано, что в случае естественных ограничений любое упрощение вычислений может привести к нарушению свойства состоятельности последовательности критериев. Построенный для этого пример интересен тем, что в нем удалось описать все возможные упрощения вычислений в статистической задаче.

Построены два примера исключения фиктивного упрощения и конструктивной проверки состоятельности

Пусть каждое критическое множество S_n строится исходя из множества S_{n-1} отбрасыванием некоторых последовательностей из множества $S_{n-1} \times X$. Тогда сложность критерия $g(S_n)$, который строится с помощью указанного алгоритма удовлетворяет разностному уравнению $g(S_n)=g(S_{n-1})+ f(n)$, где $f(n)$ – сложность отбраковки последовательностей из множества $S_{n-1} \times X$.

Описан класс альтернатив $\Theta_1 \subseteq \Theta$, для которых последовательность критериев с критическими множествами S_n, $n = 1, 2,...,$ является состоятельной.

Вычисление принадлежности наблюденного значения критическому множеству можно реализовывать с помощью вычисления функции принадлежности к дополнению этого множества. То есть если наблюденное значение не принадлежит к дополнению S_n, то наблюденное значение принадлежит S_n. В некоторых случаях, возможно, что такое вычисление функции принадлежности проще.

Обозначим $D_n = X^n \setminus S_n$, $n = 1, 2,....$ Пусть D_n может быть построено из множества $D_{n-1} \times X$ с помощью исключения некоторых последовательностей и пусть $g(D_n)$ – сложность реализации этого алгоритма. Тогда для некоторой функции $f(n)$ выполняется разностное уравнение $g(D_n) = g(D_{n-1}) + f(n)$, где $f(n)$ характеризует сложность отбраковки последовательностей в множестве $D_{n-1} \times X$..

Выделен класс альтернатив $\Theta_1 \subseteq \Theta$, для которых последовательность критериев с критическими множествами S_n, $n = 1, 2,...,$ является строго состоятельной.

Для случаев, когда критическое множество или его дополнение получается как декартово произведение $S_n = C^n$ некоторого подмножества $C \subseteq X$, то тогда $f(n) = \text{const}$. В этом случае сложность $g(S_n)$ является линейной функцией от n.

В параграфе 2 главы 3 приведены данные об экспериментальном макете, который автор создал для проверки технической реализуемости статистического поиска вставок. Практический поиск вставок существенным образом зависит от класса предполагаемых закономерностей, которые используются во вставках. В видеорядах закономерности связаны с изменением параметров отдельных фрагментов изображений. Таким образом, сначала необходимо реализовать выделение необходимых фрагментов. Решению этой проблемы посвящено много работ. В диссертации не рассматриваются эти вопросы, и предполагается, что в промышленных образцах будут объединены различные разработки по этому направлению. Если фрагменты или их характеристики выделены, то необходимо определить наличие заданных закономерностей в изменениях выделенных параметров. Поэтому в практической реализации выбрана система наблюдения за изменениями характеристик одного или нескольких пикселов.

Рассмотрим видеоряд, состоящий из набора кадров. Рассмотрим один кадр видео ряда *K*. Выберем одну точку кадра *P*. Выберем один цвет точки *C* (красный, синий или зеленый). Теперь рассмотрим последовательность значений *C* в последовательности кадров *K*. Известно, что значение *C* в одной точке *P* во всех кадрах видеоряда *K* не должно меняться, если не происходит никаких изменений изображения. Возникновение же изменений в последовательности *C* означает, что возможно использование стеганографии, например, с идентификаторами. Как показывают результаты главы 2 эффективное выявление возможно только при маловероятных случайных появлениях искомых закономерностей в видеорядах. С этой целью необходимо использовать тракт не создающий дополнительных помех. Кроме того, необходимо было убедиться в том, что искусственные изменения в характеристиках изображений видеорядов действительно существуют. Отсюда возникла задача просмотра Интернет сайтов с целью поиска изменений, которые могут использоваться в стеганографии на видеорядах.

Для реализации системы мониторинга идентификаторов необходимо:

1. Сформировать видео ряд.
2. Обработать видео ряд алгоритмом выявления идентификаторов.
3. Вывести результат обработки для последующей экспертной оценки.

Система распознавания простейших идентификаторов реализована в виде программно-аппаратного комплекса. Аппаратный комплекс состоит из входного, выходного интерфейсов и сигнального процессора. Программный комплекс позволяет в режиме экспертной оценки осуществлять мониторинг потенциальных идентификаторов в кадрах видеоряда.

Программное обеспечение (далее ПО) разработано с целью сбора статистики о меняющихся цветах на сайтах Интернет. Программное обеспечение производит захват изображения с экрана пользователя персонального компьютера и строит график по результатам захвата. На графике по оси абсцисс отсчитываются номера захватов от 1 до 800. По оси ординат производится отсчет интенсивности от 0 до 255 каналов выбранной точки: красного, синего и зеленого. Таким образом, на графике отображаются 3 линии соответствующих цветов. Идентификация мерцаний в заданном диапазоне частот и с заданными ограничениями на длительность может проводиться автоматически.

В макете используется цифровая передача с помощью DVI. Чтобы избежать дрожания, использован стандарт DVI, который обеспечивает стабильность кадров, так как видео изображение, сформированное на видео карте-источнике видео сигнала, не подвергается двойному преобразованию: цифровое в аналоговое на видео карте и обратно на карте видео захвата.

В результате решены следующие технические задачи.

1. Решены проблемы с дрожанием экрана при видео захвате с помощью специальных настроек платы видео захвата.
2. Разработана гибкая система видео захвата с помощью видео карты захвата Accustream 100, которая позволила выделять регионы изображения для анализа.

3. Удобный пользовательский интерфейс, обеспечивающий возможность указания региона для анализа с помощью одного нажатия клавиши мышь.

Основные публикации по теме диссертации.

1. Грушо Н.А. Алгоритмы обнаружения заданных закономерностей в изображениях на экране монитора // Труды XXXIV Международной конференции и дискуссионного научного клуба «Информационные технологии в науке, образовании, телекоммуникации и бизнесе (весенняя сессия)», Украина, Крым, Ялта-Гурзуф, 25 мая – 4 июня 2007 г./ Лаборатория компьютерной графики Запорожского государственного университета. – 2007. – с. 197-199.
2. Грушо Н.А. Асимптотическое распределение времени выявления вставок в изображения на экране монитора // Труды XXXIV Международной конференции и дискуссионного научного клуба «Информационные технологии в науке, образовании, телекоммуникации и бизнесе (весенняя сессия)», Украина, Крым, Ялта-Гурзуф, 25 мая – 4 июня 2007 г./ Лаборатория компьютерной графики Запорожского государственного университета. – 2007. – с. 203-204.
3. Грушо А.А., Грушо Н.А., Тимонина Е.Е. Некоторые применения стеганографии и защищенность стегосхем // Проблемы информационной безопасности. Компьютерные системы. – 2007, № 2. – 3 с.
4. Грушо А.А., Грушо Н.А., Тимонина Е.Е. О проблеме распознавания образов в изображениях // Обозрения прикладной и промышленной математики. – М.: ТВП. – 2007. – т. 15. – вып. 3.
5. Грушо А.А., Грушо Н.А., Тимонина Е.Е. Теоремы о несуществовании состоятельных последовательностей критериев в некоторых дискретных задачах // Дискретная математика, 2008. – т. 20. – № 2.

6. Грушо А.А., Грушо Н.А., Тимонина Е.Е. Существование состоятельных последовательностей статистических критериев в дискретных задачах // Обозрения прикладной и промышленной математики. – 2008. – т.15. – вып. 2. – 3 с.
7. Грушо А.А., Грушо Н.А., Тимонина Е.Е.: Стеганография в видеорядах и технические проблемы распознавания образов // Труды XXXV Юбилейной Международной конференции и дискуссионного научного клуба «Информационные технологии в науке, образовании, телекоммуникации и бизнесе (весенняя сессия)», Украина, Крым, Ялта-Гурзуф, 20-30 мая 2008 г./ Лаборатория компьютерной графики Запорожского государственного университета, 2008. – 3 с.
8. Grusho A., Grusho N., Timonina E. Statistical detection of simulated insertions in sequences of images // Transactions of XXVI International Seminar on Stability Problems for Stochastic Models, Park plaza Hotel Nahariya, Israel. – October 22-26. – 2007. – P. I. – pp 96-99.
9. Grusho A., Grusho N., Timonina E. Complexity and Consistency of Statistical Criteria //Systems and Means of Informatics. Special Issue. Mathematical and Computer Modeling in Applied Problems. – M.: IPI RAS, 2008. – P. 32-39.
10. Grusho A., Grusho N., Timonina E. Asymptotic Complexity of Consistent Sequences of Statistical Criteria in Finite Spaces // Proc. of 2008 Barcelona Conference on Asymptotic Statistics. – Bellaterra: Centre de Recerca Mathematica, 2008. – pp. 70-71.