ՀՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱ
ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

ԼԱՆԻՆԱ Նատալյա Սեմյոնի

ԹՎԱՅՆԱՑՎԱԾ ՊԱՏԿԵՐՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅԱՆ ԱԼԳՈՐԻԹՄՆԵՐԻ ԵՎ ԾՐԱԳՐԵՐԻ ՀԱՄԱԼԻՐԻ ՄՇԱԿՈՒՄ

Ե.13.05 – “Մաթեմատիկական մոդելավորում, թվային մեթոդներ և ծրագրային համակարգեր” մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսություն

ՍԵՂՄԱԳԻՐ

Երևան – 2011

НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АРМЕНИИ
ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ

ЛАНИНА Наталья Семёновна

РАЗРАБОТКА КОМПЛЕКСА АЛГОРИТМОВ И ПРОГРАММ ЗАЩИТЫ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата технических наук по специальности 05.13.05 – «Математическое моделирование, численные методы и комплексы программ»

Ереван – 2011

Ատենախոսության թեման հաստատվել է Հայ-Ռուսական (Սլավոնական) համալսարանում

Գիտական ղեկավար՝ տ.գ.դ. Դ.Գ. Ասատրյան
Պաշտոնական ընդդիմախոսներ՝ ֆ-մ. գ.դ., պրոֆ. Հ.Գ. Սարուխանյան
տ.գ.թ., դոց. Գ.Ի. Մարգարով
Առաջատար կազմակերպություն՝ Երևանի կապի միջոցների գիտահետազոտական ինստիտուտ

Ատենախոսության պաշտպանությունը կայանալու է՝ 2011 թ. հունիսի 17-ին, ժ. 15^{00} – ին ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող 037 – “Ինֆորմատիկա և հաշվողական համակարգեր” մասնագիտական խորհրդի նիստում, հետևյալ հասցեով՝ Երևան, 0014, Պ.Սևակի փ. 1 :
Ատենախոսությանը կարելի է ծանոթանալ ինստիտուտի գրադարանում:
Սեղմագիրն առաքված է 2011 թ. մայիսի 17-ին:

Մասնագիտական խորհրդի գիտական քարտուղար՝
ֆ.-մ. գ .դ., պրոֆեսոր Մ.Ե. Հարությունյան

Тема диссертации утверждена в Российско-Армянском (Славянском) университете

Научный руководитель: д.т.н. Д.Г. Асатрян
Официальные оппоненты: д.ф-м.н., проф. А.Г. Саруханян
к.т.н. Г.И. Маргаров
Ведущая организация: Ереванский научно-исследовательский институт средств связи

Защита диссертации состоится 17 июня 2011 г. в 15^{00} на заседании Специализированного совета 037 «Информатика и вычислительные системы» Института проблем информатики и автоматизации НАН РА по адресу: 0014, г. Ереван, ул. П. Севака 1.
С диссертацией можно ознакомиться в библиотеке института.
Автореферат разослан 17 мая 2011 г.

Ученый секретарь Специализированного совета
д.ф.-м.н., профессор М.Е.Арутюнян

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность проблемы. Задача защиты информации от несанкционированного доступа, использования и изменения содержания была важной и актуальной на протяжении всей истории человечества. Она продолжает оставаться актуальной и в настоящее время в связи с продолжающимся ростом количества создаваемой, хранимой, обрабатываемой и передаваемой по каналам связи информации. Соответственно интенсивно развиваются теория, методы и средства, применяемые для защиты информации в самых различных областях деятельности человека. При этом требования, предъявляемые к надежности и качеству методов защиты цифрового продукта, становятся все более высокими.

В течение последних без малого двух десятилетий интенсивно развивается область защиты цифровой информации (сигналов, изображений и др.) от несанкционированного доступа и использования, основанная на встраивании в защищаемый объект секретной информации в виде невидимых меток (называемых цифровым водяным знаком – ЦВЗ). При помощи ЦВЗ решаются различные задачи, в частности, восстанавливается секретное сообщение, устанавливается принадлежность защищаемого объекта к заранее определенному классу, проверяется целостность информации и др. Для краткости применяемые при этом методы и алгоритмы удобно называть ЦВЗ-методами, алгоритмами и т.д.

Научная литература, посвященная теории и технике встраивания ЦВЗ в изображение, весьма обширна, а ее объем растет с каждым днем. Причиной тому – возрастание не только объемов цифровой информации, но и разнообразия ее проявлений, видов и применений.

Однако, как показывает анализ научной литературы и запатентованных решений, посвященных ЦВЗ-технологиям, имеется ряд задач, все еще до конца не решенных. Известно, что основные требования, предъявляемые обычно к качеству ЦВЗ-процедуры (например, скрытность, надежность, большой объем встраиваемой информации и др.) взаимно противоречивы, поэтому всякий раз при разработке или применении процедуры приходится идти на определенный компромисс. Более того, пока нет единой теории, позволяющей аналитически исследовать различные свойства ЦВЗ-алгоритмов и выбирать наиболее приемлемую для данной ситуации схему защиты информации. Аналитические методы исследования качества отсутствуют и для большинства известных в литературе ЦВЗ-алгоритмов. По этой причине исследование свойств ЦВЗ-алгоритма обычно проводится на экспериментальном материале, путем компьютерного моделирования, что, конечно, не может гарантировать универсальность и высокое качество предложенных методов.

Настоящая работа посвящена разработке и реализации ЦВЗ-процедуры, основанной на классе адаптивных алгоритмов, позволяющей, в отличие от общеизвестных, не только эффективно реализовать и исследовать систему защиты, но и проводить аналитическое исследование ее свойств.

Целью работы является разработка класса адаптивных ЦВЗ-алгоритмов защиты изображения путем встраивания в него бинарного ЦВЗ, а также методики аналитического и экспериментального исследования качества предложенных процедур.

Задачами исследования являются:

- исследование существующих пространственных адаптивных ЦВЗ-алгоритмов, их достоинств и недостатков, обобщение и формализация задачи;
- исследование свойств визуальной системы человека (ВСЧ) и формирование общего подхода к созданию ЦВЗ-алгоритма, удовлетворяющего основным требованиям качества;
- разработка математической модели и метода аналитического исследования ошибок, возникающих вследствие встраивания ЦВЗ и воздействия атак;
- разработка комплекса алгоритмов и программ для исследования эффективности предложенной ЦВЗ-процедуры;
- численное моделирование различных типов атак и экспериментальное исследование параметров качества ЦВЗ-процедуры.

Методы исследования. В работе применялись:

- современные методы цифровой обработки изображений в пространственной и спектральной областях;
- статистические методы моделирования и исследования случайных последовательностей с заданными свойствами;
- компьютерные технологии и методы регистрации, обработки, отображения и визуализации данных.

Научная новизна работы. В процессе исследования были получены следующие результаты, отличающиеся новизной:

- предложен обобщенный класс пространственных адаптивных устойчивых ЦВЗ-алгоритмов защиты цифрового изображения путем встраивания бинарного ЦВЗ, с учетом свойств визуальной системы человека;
- предложена математическая модель и метод исследования ошибок, возникающих вследствие встраивания и извлечения ЦВЗ, а также воздействия атак;

- получены аналитические выражения, связывающие ошибки процедур встраивания и извлечения ЦВЗ при наличии атак, с параметрами ЦВЗ-процедуры;
- предложен аналитический метод оценивания качества ЦВЗ-процедуры взамен общепринятого графического («магического треугольника»);
- исследована устойчивость предложенной ЦВЗ-процедуры при различных типах атак.

На защиту выносятся следующие научные положения:

- класс пространственных адаптивных устойчивых алгоритмов защиты изображения путем встраивания бинарного ЦВЗ;
- аналитический метод и выражения для исследования ошибок процедур встраивания и извлечения ЦВЗ при наличии атак;
- аналитический критерий оценивания качества класса предложенных ЦВЗ-процедур;
- численные модели и результаты экспериментального исследования устойчивости предложенных процедур;
- комплекс алгоритмов и программ, реализующий предложенную адаптивную ЦВЗ-процедуру и методику исследования качества.

Практическая ценность работы. Достигнуты следующие результаты, представляющие практический интерес:

- создан комплекс алгоритмов и программ, реализующий метод защиты изображения путем встраивания в него бинарного ЦВЗ;
- создана методика для исследования и испытания систем защиты информации в условиях воздействия наиболее распространенных типов атак;
- получены аналитические формулы для оценивания помехоустойчивости и других характеристик адаптивного алгоритма на стадии проектирования системы защиты информации без непосредственного выполнения операций встраивания и извлечения ЦВЗ.

Достоверность научных положений обеспечивается математическим обоснованием полученных результатов, их экспериментальной проверкой путем математического моделирования и численных расчетов.

Апробация работы

Основные положения и материалы диссертации обсуждались на семинарах кафедры математической кибернетики Российско-Армянского (Славянского) университета (РАУ) на научном семинаре ИПИА, и на научном семинаре кафедры ГИУА «Информационной безопасности и программных систем», а также докладывались на научных конференциях:

- на годичных научных конференциях РАУ 2006, 2007, и 2010 гг.;
- на международной научно-практической конференции по вопросам безопасности информационных систем, г. Ереван, 2007;
- на международной научной конференции «Компьютерная наука и информационные технологии – CSIT'2007», 2007;
- на пятой международной конференции «Исследование, разработка и применение высоких технологий в промышленности», Санкт-Петербург, Россия, 2008.

Публикации

Основные результаты исследований отражены в 7 научных публикациях, список которых приведен в конце автореферата.

Структура и объем работы

Диссертация состоит из введения, четырех глав, списка использованной литературы из 108 наименований и основных выводов по диссертации. Основной текст изложен на 118 страницах, включая 21 рисунок и 12 таблиц. Диссертация написана на русском языке.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность и практическая значимость темы диссертационной работы, кратко изложено состояние предметной области, сформулированы цель и основные задачи исследования, выделены научные результаты, отличающиеся новизной, научные положения, выносимые на защиту и практическая ценность полученных результатов.

В первой главе диссертации проанализировано современное состояние проблемы цифровой защиты информации на основе научной литературы, опубликованной в течение последних двух десятилетий. Выполнена классификация задач и типов защиты информации, ЦВЗ-технологий, наиболее распространенных типов атак. Далее, в этой главе рассмотрены предложенные в литературе адаптивные ЦВЗ-алгоритмы, работающие в пространственной области изображения. Рассмотрены свойства ВСЧ, которые можно использовать при разработке ЦВЗ-процедур, с целью обеспечения бóльшей скрытности встраиваемой информации. Подробно описаны алгоритмы, основанные на использовании различных свойств ВСЧ. Выявлены преимущества и недостатки этих алгоритмов. На этой основе обоснована целесообразность разработки нового класса алгоритмов, обладающего большей надежностью и возможностью аналитического исследования качества. Предложено при этом основываться на свойствах ВСЧ, связанных с различной восприимчивостью к изменениям в участках

изображения с различной контрастностью. Исходя из этого сделан обзор формальных мер измерения контрастности изображения, сделан выбор в пользу среднеквадратического отклонения (СКО) интенсивностей пикселов.

В первой главе сделан вывод о том, что в научной литературе практически отсутствуют аналитические результаты общего характера, позволяющие оценивать качество ЦВЗ-процедуры без ее непосредственного применения.

Вторая глава посвящена разработке адаптивного алгоритма встраивания бинарного ЦВЗ в пространственную область изображения.

Рассмотрим изображение-контейнер формата *GrayScale (8 bit),* значения интенсивностей пикселов которого принимают целочисленные значения из множества $\{0,1,...,255\}$. Пусть изображение–контейнер I имеет размеры $M \times N$, и $I = (a_{mn})$, $m = 0,1,...,M-1$, $n = 0,1,...,N-1$.

Ограничимся рассмотрением бинарных ЦВЗ и обозначим матрицу ЦВЗ с размерами $K \times L$, через $W = (w_{kl}), k = 0,1,...,K-1;\ \ l = 0,1,...,L-1$. Необходимо встраивать ЦВЗ W в изображение I, т.е. получить новое изображение $I_W = (a_{mn}^W)$ при помощи некоторого оператора встраивания $E_+(I,W,\alpha,\Xi)$, где $\alpha \geq 0$ – параметр, определяющий силу встраивания ЦВЗ в изображение. Здесь Ξ – секретный ключ, при помощи которого определяется порядок встраивания пикселов ЦВЗ в изображение. Оператор встраивания присваивает новые значения пикселам изображения I в соответствии с фиксированным правилом. При $\alpha = 0$ встраивание не происходит.

При наличии атаки X происходит определенное преобразование изображения I_W, в результате чего оно переходит в изображение $I_{W,X} = (a_{mn}^{W,X})$, которое может отличаться от I_W. При этом под атакой понимается любое преднамеренное или непреднамеренное действие, способное удалить или повредить встроенный ЦВЗ.

Процедура извлечения ЦВЗ из атакованного изображения $I_{W,X}$ производится при помощи оператора $E_-(I_{W,X},I,W,\alpha,\Xi)$. В результате применения оператора извлечения получается, вообще говоря, искаженный образ W_X исходного ЦВЗ W.

Как констатируется в первой главе, в научной литературе универсальных методов построения операторов встраивания E_+ и извлечения E_- не обнаружено. Однако, учитывая ряд факторов и требований, вытекающих из постановки и ограничений общей задачи защиты информации при помощи ЦВЗ-технологий, можно предложить новый подход, позволяющий разрабатывать определенные классы эффективных пространственных ЦВЗ-алгоритмов.

Приведем эти факторы и требования.

- Для устойчивости к атакам процедуры встраивания ЦВЗ в пространственную область необходимо, чтобы размер контейнера был значительно больше размера ЦВЗ.
- Для обеспечения большей скрытности ЦВЗ, необходимо применять малые значения силы встраивания. При этом желательно учитывать свойства ВСЧ.
- Необходимо исходить из положения, что ошибки, возникающие при встраивании ЦВЗ и в результате воздействия атак, принимают малые значения (в противном случае задача защиты изображения теряет смысл).
- Желательно использовать алгоритмы встраивания, не требующие большого объема априорной информации о защищаемом изображении и ЦВЗ (адаптивные алгоритмы).

Приступим к построению процедуры встраивания ЦВЗ.

1. В предположении дифференцируемости процедуры $E_+(I,W,\alpha,\Xi)$, рассматриваемой как функцию от параметра α, представим ее в виде приближения первыми членами ряда Тейлора

$$E_+(I,W,\alpha,\Xi) \approx E_+(I,W,0,\Xi) + \alpha \frac{\partial}{\partial \alpha} E_+(I,W,\alpha,\Xi)\Big|_{\alpha=0}.$$

Тогда можно написать, что

$$I_W \approx I + \alpha S(I,W), \qquad (1)$$

где матрица $S(I,W)$ зависит только от участвующих в процедуре изображений.

2. Исходя из желания использовать те или иные свойства ВСЧ, мы должны подставить в (1) такую матрицу $S(I,W)$, элементы которой зависят от численных значений, характеризующих данное свойство ВСЧ. В первой главе диссертации в качестве подходящего свойства ВСЧ выбрана его избирательная чувствительность к контрастности изображения, а в качестве меры контрастности предложено использовать СКО интенсивностей пикселов рассматриваемого участка изображения.

3. Разделим изображение-контейнер I на $\frac{MN}{KL}$ одинаковых частей (блоков) с размерами $M_K = M/K$ и $N_L = N/L$ (для простоты принято, что K является делителем M, а L - делителем N) и установим взаимно-однозначное соответствие между полученными блоками и битами ЦВЗ.

4. Примем следующую модель для функции $S(I,W)$: пусть w обозначает бит ЦВЗ, подлежащий к встраиванию в некоторый блок B изображения I. Тогда

$$S(B,w) = C(2w-1)S_B, \qquad (2)$$

где $C > 0$ - некоторый масштабный множитель, w - встраиваемый бит ($w = \{0,1\}$), а S_B - мера контрастности блока B (т.е. в данном случае – СКО интенсивностей пикселов блока).

В соответствии с формулой (2), для встраивания бита w в фиксированный блок B необходимо рассчитать среднее значение m_B интенсивностей пикселов b_{ij}, $i = 0,1,...,M_K - 1$; $j = 0,1,...,N_L - 1$ блока и СКО S_B по формулам

$$m_B = \frac{1}{M_K N_L}\sum_{i=0}^{M_K-1}\sum_{j=0}^{N_L-1} b_{ij}\ ,\ S_B{}^2 = \frac{1}{M_K N_L}\sum_{i=0}^{M_K-1}\sum_{j=0}^{N_L-1}(b_{ij}-m_B)^2\ . \qquad (3)$$

Изменение интенсивности пикселов блока со значения b_{ij} на значение $b_{ij}^{'}$ производится в соответствии со следующими правилами:

- если $w = 1$, то $b_{ij}^{'} = b_{ij} + \alpha C S_B{}^{'}$,
- если $w = 0$, то $b_{ij}^{'} = b_{ij} - \alpha C S_B{}^{'}$,

где $S_B{}^{'} = \max(S_B, \beta)$, β - минимальное ненулевое значение СКО по всем блокам. Массив значений m_B запоминается для использования в процедуре извлечения ЦВЗ.

Процедура извлечения ЦВЗ носит обратный характер и применяется, быть может, к атакованному изображению $I_{W,X}$. При этом создаются блоки аналогично тому, как создавались при встраивании ЦВЗ, поэтому при сопоставлении первоначального и анализируемого изображений сначала восстанавливается порядок соответствия анализируемого блока и позиции пиксела в извлекаемом ЦВЗ.

Рассмотрим блок $B^{'}$ изображения $I_{W,X}$ и обозначим через $m_{B'}{}^{'}$ среднее интенсивностей пикселов блока $B^{'}$. Предполагается, что известен массив средних всех блоков, рассчитанных при встраивании ЦВЗ по формуле (3).

Извлечение ЦВЗ выполняется в соответствии со следующими простыми правилами:

- если $m_{B'}{}^{'} > m_B$, то $w^{'} = 1$,
- если $m_{B'}{}^{'} \le m_B$, то $w^{'} = 0$.

Во **второй главе** представлена программная система *WM_Adaptive*, написанная на языке *Visual Basic* и реализующая предложенные процедуры встраивания и извлечения ЦВЗ. Приведены также некоторые результаты экспериментов, выполненных с помощью этой программной системы с соответствующими комментариями. В частности, обсуждены вопросы

выбора параметров ЦВЗ-процедуры и установлены правила визуального и/или формального оценивания качества процедуры.

Третья глава посвящена аналитическому и экспериментальному исследованию ошибок предложенного в главе 2 адаптивного ЦВЗ-алгоритма.

Как следует из постановки задачи защиты изображений, представляют интерес два типа ошибок, которые важны для оценивания качества процедуры встраивания и извлечения ЦВЗ. Первый тип, назовем его *ошибкой встраивания*, характеризует различие между изображениями I и I_W, которое возникает в результате встраивания ЦВЗ. Общая логика защиты изображения требует, чтобы эта ошибка была малой настолько, чтобы изображение со встроенным ЦВЗ визуально не отличалось от оригинала или отличалось в допустимых пределах по заданному формальному критерию.

Второй тип ошибок, назовем его *ошибкой извлечения*, характеризует различие между встроенным ЦВЗ – W и извлеченным ЦВЗ – W_X. Ошибка этого типа также должна быть малой настолько, чтобы извлеченный ЦВЗ был узнаваем визуально. В случае оценивания этой ошибки формальным методом (например, при помощи PSNR), требуется установить уровень минимально допустимой ошибки.

Пусть задана некоторая мера $\|I_1 - I_2\|$ расхождения изображений I_1 и I_2. Тогда можно написать следующее неравенство треугольника

$$\|I - I_{W,X}\| \le \|I - I_W\| + \|I_W - I_{W,X}\|, \qquad (4)$$

где $\|I - I_W\|$ является ошибкой встраивания ЦВЗ, а второе слагаемое характеризует ошибку, вносимую атакой X в защищенное изображение. Из малости второго слагаемого следует малость ошибки извлечения.

Из (4) следует, что для обеспечения близости изображений I и $I_{W,X}$ достаточно, чтобы слагаемые из правой части неравенства принимали малые значения. Поэтому данное неравенство является основной формальной моделью для ошибок любой ЦВЗ-процедуры.

В настоящей работе в качестве меры расхождения изображений $I_1(m,n)$ и $I_2(m,n)$ используется средний квадрат разности интенсивностей пикселов. Устанавливается также общая аддитивная форма для любой ЦВЗ-процедуры и для любого типа атаки

$$I_{W,X} = I_W + X, \qquad (5)$$

имея в виду, что слагаемые в (5) являются матрицами.

Отметим, что при исследовании ЦВЗ-алгоритмов удобно использовать логарифмическую шкалу, и рассматривать их противоположные значения, переведя

соответствующие величины в децибелы. Поэтому вместо ошибки встраивания после такого преобразования будем использовать общепринятый термин «мера необнаруживаемости», а вместо ошибки извлечения – «мера узнаваемости».

Исследуем случай, когда элементы матрицы $X = \{X_{mn}\}$, $m = 0,1,...,M-1$, $n = 0,1,...,N-1$ являются случайными величинами (с неизвестными многомерными распределениями). Соответствующие средние и дисперсии обозначим через $\{\mu_{mn}\}$ и $\{\sigma^2_{mn}\}$.

Рассмотрим важный частный случай, когда элементы матрицы X независимы в совокупности и имеют нулевые математические ожидания, т.е. $E(X_{mn}) = 0$ для всех $m = 0,1,...,M-1$, $n = 0,1,...,N-1$. Тогда для фиксированного блока математическое ожидание среднего квадрата ошибки встраивания равно

$$E[MSE^2(B,X)] = \alpha^2 C^2 S_B{}'^2 + \frac{1}{M_K N_L}\sum_{i=0}^{M_K-1}\sum_{j=0}^{N_L-1}\sigma_{ij}^2 . \qquad (6)$$

В интересном частном случае, когда дисперсии элементов матрицы X одинаковы и равны σ_X^2 для $m = 0,1,...,M-1$, $n = 0,1,...,N-1$, имеем

$$E[MSE^2(B,X)] = \alpha^2 C^2 S_B{}'^2 + \sigma_X^2 . \qquad (7)$$

Назовем эту ошибку *полной ошибкой встраивания с атакой*. В отсутствие же атаки, т.е. при равенстве нулю всех дисперсий $\{\sigma^2_{mn}\}$, выражения (6) и (7) превращаются в среднеквадратическую *ошибку встраивания без атаки*

$$E[MSE^2(B,X)]\Big|_{\{\sigma^2_{mn}=0\}} = \alpha^2 C^2 S_B{}'^2 . \qquad (8)$$

Выражение (8) показывает, что ошибка встраивания без атаки внутри одного блока зависит непосредственно от силы встраивания α и меры контрастности $S_B{}'$. Поскольку мера контрастности изображения является внутренним свойством защищаемого изображения и не может быть изменена, то желаемого уменьшения ошибки встраивания можно добиться выбором соответствующего значения α. Следует отметить интересный факт, что ошибка встраивания не зависит от значения встраиваемого бита и размера блока непосредственно и определяется лишь значением меры контрастности блока, которая, конечно же, является переменной величиной, зависящей от размеров блока.

Перейдя от блоков ко всему изображению, для полной квадратической ошибки $E^2(I,W,X)$ при атаке X и при встроенном ЦВЗ W получим

$$E^2(I,W,X) = \alpha^2 C^2 \overline{S'^2} + \frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\sigma_{mn}^2 , \quad \overline{S'^2} = \frac{1}{KL}\sum_{k=0}^{K-1}\sum_{l=0}^{L-1}S'^2_{kl} .$$

В случае равенства дисперсий имеем

$$E^2(I,W,X) = \alpha^2 C^2 \overline{S'^2} + \sigma_X^2 . \qquad (9)$$

Рассматривая (9), заметим, что полная ошибка встраивания также не зависит от каких-либо характеристик конкретного ЦВЗ W и определяется только свойствами изображения-контейнера I и атаки X. Это замечательное свойство предложенного алгоритма встраивания выгодно отличает его от многих других известных алгоритмов. Поэтому в выражении ошибки $E^2(I,W,X)$ мы опустим аргумент W, т.е. будем применять обозначение $E^2(I,X)$.

Что же касается коэффициентов C и β, фигурирующих в приведенных выше формулах, то без ограничения общности можно принимать, что $C = 1$ и $\beta = 0$. Тогда окончательно получим

$$E^2(I,X) = \alpha^2 \overline{S^2} + \sigma_X^2 . \qquad (10)$$

Несмотря на простоту, формула (10) таит в себе значительные возможности для анализа и регулирования качества процедуры встраивания. Например, при отсутствии атак ошибка встраивания (10) принимает предельно простой вид

$$E^2(I,0) = \alpha^2 \overline{S^2} . \qquad (11)$$

Формула (10) позволяет определять ошибку встраивания ЦВЗ без непосредственного применения самой процедуры встраивания, что важно при проектировании алгоритмов защиты определенного типа изображений.

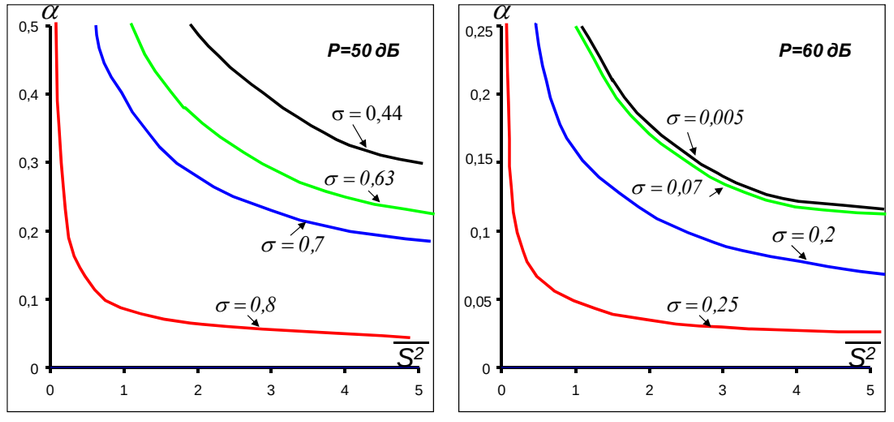


Рис. 1. Зависимость силы встраивания α от $\overline{S^2}$ при различных допустимых значениях ошибки встраивания (11), переведенных в дБ.

В качестве примера укажем на Рис. 1, на котором приведен график зависимости силы встраивания α от средней контрастности изображения $\overline{S^2}$ при максимально допустимых значениях ошибки встраивания (11) в 50 дБ и 60 дБ.

Среднеквадратическая ошибка извлечения ЦВЗ $\|W - W_X\|$ из подконтрольного изображения $I_{W,X}$ имеет вид

$$MSE^2(W,X) = \frac{1}{KL}\sum_{k=0}^{K-1}\sum_{l=0}^{L-1}\left[w(k,l) - w_X(k,l)\right]^2, \qquad (12)$$

где $w(k,l)$ и $w_X(k,l)$ принимают значения «0» или «1». Ошибка извлечения бита с координатами (k_0,l_0) при $w(k_0,l_0)=1$ означает, что $w_X(k_0,l_0)=0$, т.е. произошло событие $m_{kl}^{'} \le m_{kl}$. Вычислим вероятность этого события, основываясь на центральной предельной теореме и полагая, что при достаточно больших размерах блоков

$$m_{kl}^{'} - m_{kl} \sim N\left(\alpha S_{kl}, \frac{\sigma_X^2}{M_K N_L}\right).$$

Тогда вероятность $p(\delta_{kl})$ ошибки извлечения одного бита ЦВЗ равна

$$p(\delta_{kl}) = P\{m_{kl}^{'} - m_{kl} \le 0\} = \frac{1}{2} - \Phi(\delta_{kl}),\ \delta_{kl} = \alpha\frac{S_{kl}}{\sigma_X}\sqrt{M_K N_L} = \alpha\frac{S_{kl}}{\sigma_X}\sqrt{\frac{MN}{KL}}, \qquad (13)$$

где $\Phi(\delta)$ – функция Лапласа. Перейдя ко всему изображению, получим следующее выражение для полной ошибки извлечения

$$E\left[MSE^2(I,X)\right] = \frac{1}{KL}\sum_{k=0}^{K-1}\sum_{l=0}^{L-1} p(\delta_{kl}). \qquad (14)$$

Формула (14) связывает полную среднеквадратическую ошибку извлечения бинарного ЦВЗ со средней вероятностью ошибки извлечения битов по ЦВЗ.

Таблица 1

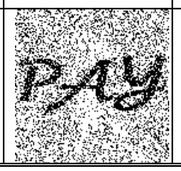
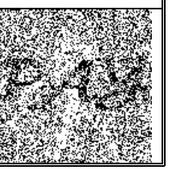
Результаты расчетов теоретической и экспериментальной зависимостей меры необнаруживаемости и меры узнаваемости ЦВЗ от σ_X (изображение Mandrill)

σ_X	**Мера необнаруживаемости, дБ**		**Мера узнаваемости, дБ**	
	Теория	**Эксперимент**	**Теория**	**Эксперимент**
4	35.30	35.45	8.54	9.65
6	32.20	32.27	6.90	7.51
8	29.86	29.89	5.96	6.24
10	27.99	28.03	5.36	5.55

В Таблице 1 приведены результаты расчетов теоретической и экспериментальной зависимостей от σ_X мер необнаруживаемости и узнаваемости ЦВЗ (переведенные в децибелы) для изображения *Mandrill*. Мы видим в целом незначительные расхождения между этими значениями, вполне достаточные для иллюстрации корректности примененной процедуры.

Таблица 2

Сравнительные данные для изображений Mandrill и Cameraman

Изображение	***Mandrill***		***Cameraman***	
σ_X	5	10	5	10
Мера необнаруживаемости	33.75	28.03	33.87	28.22
Извлеченный ЦВЗ				

В Таблице 2 приведены примеры мер необнаруживаемости для двух изображений при относительно больших значениях параметра атаки σ_X ($\alpha = 0.1$). Мы видим, что результаты примерно одинаковы, несмотря на существенно разную структуру рассматриваемых изображений.

Четвертая глава диссертации посвящена исследованию качества предложенного адаптивного алгоритма.

Исследователям ЦВЗ-алгоритмов хорошо известен так называемый «магический треугольник», изображенный на Рис. 2. Смысл данной иллюстрации в том, чтобы показать противоречивость и несовместимость трех основных критериев качества любой ЦВЗ-процедуры.

Рис.2. Иллюстрация противоречивости требований к качеству ЦВЗ-процедуры при помощи «Магического треугольника».

К сожалению, в научной литературе общих аналитических методов исследования качества ЦВЗ-процедуры не обнаружено, поэтому часто приходится довольствоваться только результатами моделирования и качественными рассуждениями.

Однако результаты третьей главы диссертации позволяют для предложенного класса адаптивных ЦВЗ-алгоритмов разработать аналитический метод, основанный на формулах ошибок встраивания и извлечения ЦВЗ.

Введем в рассмотрение следующие три характеристики качества ЦВЗ-процедуры:

1. *Стегоемкость*, означающая количество бит ЦВЗ, приходящихся на один пиксел изображения-контейнера, определим формулой

$$C_0 = \sqrt{KL/MN}\,. \qquad (15)$$

2. *Необнаруживаемость* ЦВЗ, зависящая от значения ошибки встраивания $E^2(I,0) = \alpha^2\overline{S^2}$ в отсутствие атаки, определяем формулой (11). Чем меньше эта ошибка, тем больше необнаруживаемость ЦВЗ. Поэтому необнаруживаемость ЦВЗ целесообразно обозначить через H_0 и определить по формуле

$$H_0 = \frac{1}{\sqrt{E^2(I,0)}} = \frac{1}{\alpha\sqrt{\overline{S^2}}}\,. \qquad (16)$$

3. *Устойчивость процедуры*, которая характеризуется ошибкой извлечения (14). Из формул (13) и (14) следует, что изменение параметров встраивания и влияния атаки приводит к одновременному изменению в ту же сторону всех δ_{kl}. Поэтому исследование поведения (14) можно свести к исследованию δ_{kl} в совокупности. Возведем в квадрат обе части выражения для δ_{kl}, просуммируем по всем $k = 0,1,...,K-1; l = 0,1,...,L-1$ и разделим на KL. Тогда получим

$$\overline{\delta^2} = \frac{1}{KL}\sum_{k=0}^{K-1}\sum_{l=0}^{L-1}\delta_{kl}^2 = \alpha^2\frac{\overline{S^2}}{\sigma_X^2}\frac{MN}{KL}\,. \qquad (17)$$

Устойчивость алгоритма для изображения I при атаке X обозначим через $R(I,X)$ и определим формулой

$$R(I,X) = G_I\sqrt{\overline{\delta^2}} = G_I\alpha\frac{\sqrt{\overline{S^2}}}{\sigma_X}\sqrt{\frac{MN}{KL}}\,, \qquad (18)$$

где коэффициент G_I зависит только от распределения меры контрастности изображения I.

Теперь остается сравнивать (15), (16) и (18) и установить следующее соотношение между ними

$$C_0 \times H_0 \times R(I,X) \times \sigma_X = G_I\,. \qquad (19)$$

Соотношение (19) показывает, что для фиксированного изображения I и параметра атаки σ_X увеличение одного из критериев C_0, H_0 и $R(I,X)$ приводит к уменьшению остальных.

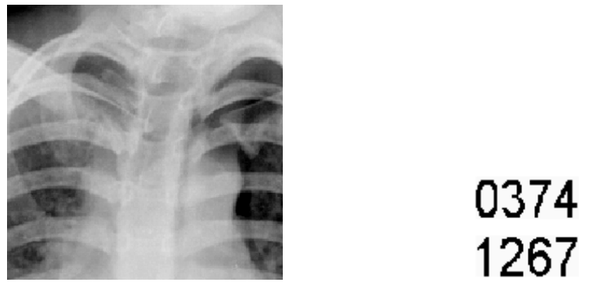
Таким образом, соотношение (19) устанавливает основную функциональную связь между тремя важнейшими критериями оценивания качества при наличии воздействия атаки. При этом характеристики примененного ЦВЗ никак не влияют на соотношение (19). Легко видеть, что все выводы, следуемые из интуитивно обнаруженного правила с «магическим треугольником», также следуют из формулы (19), но со значительно большей убедительностью, наглядностью и возможностью численного сопоставления.

Исходя из вышеизложенного, формулу (19) будем называть *обобщенным критерием оценивания качества адаптивного ЦВЗ-алгоритма.*

Далее, в данной главе методом математического моделирования исследована устойчивость алгоритма при воздействии наиболее известных типов атак. Методика моделирования состоит из следующих основных процедур:

- моделирование случайной атаки. Разработаны программы для моделирования шумов с равномерным и нормальным распределениями и шума типа «соль и перец»;
- реализация атак типа «*StirMark*», в том числе атаки типов «сжатие по стандарту JPEG» и «изменение масштаба изображения»;
- реализация атаки по изменению структуры и содержания изображения.

Ниже приведены примеры с результатами проверки устойчивости при различных типах атак.



а б

Рис. 3. Рентгенограмма грудной клетки человека (а) и ЦВЗ (б).

Пример 1. Устойчивость к случайным атакам. На Рис. 3 показаны защищаемое изображение (а) и ЦВЗ (б), который встраивается при $\alpha = 0.02$.

Представляет интерес зависимость PSNR между изображениями со встроенным ЦВЗ до и после зашумления, т.е., как бы, зависимость от типа распределения шума и параметра σ_X «в чистом виде». Результаты расчетов представлены в Таблице 3. Параметры распределений подобраны так, чтобы дисперсия шума оказалась одинаковой для всех типов шумов. Мы видим, что для всех рассмотренных типов распределений нет значительных расхождений в значениях PSNR.

Результаты извлечения ЦВЗ из зашумленных изображений, представлены в Таблице 4 они подтверждают выводы, которые следуют из Таблицы 3.

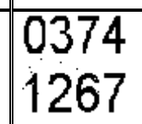
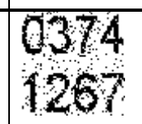
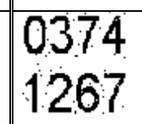
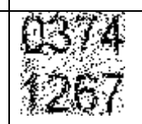
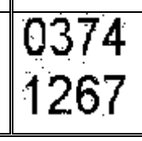
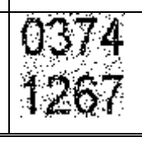
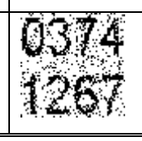
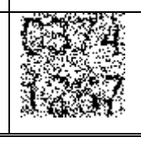
Таблица 3

Зависимость меры необнаружения от типа распределения и параметра σ_X

Тип распределения	σ_X				
	2	4	6	8	10
Равномерное $U(-a,a)$, $a=\sqrt{3}\sigma_X$	43.1	36.0	32.9	30.0	28.3
Нормальное $N(0,\sigma_X)$	41.8	36.0	32.5	30.0	28.1
Распределение «Соль и перец» $p=0.1; b=\sqrt{5}\sigma_X$	42.0	36.5	32.6	30.3	28.1

Таблица 4

Результаты извлечения ЦВЗ из зашумленного изображения

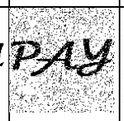
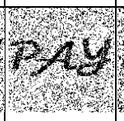
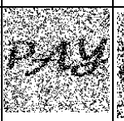
Тип распределения шума	σ_X				
	2	4	6	8	10
Равномерное $U(-a,a)$, $a=\sqrt{3}\sigma$					
Нормальное $N(0,\sigma)$					
Распределение «Соль и перец» $p=0.1; b=\sqrt{5}\sigma$					

Пример 2. В Таблице 5 приведены экспериментальные результаты работы алгоритма после атаки – сжатия в спектральной области с разной степенью по стандарту JPEG. Исходное изображение в данной серии экспериментов – Lenna, 512x512 пикселов. ЦВЗ (текст «РАУ») - с размерами 128x128. ЦВЗ встраивался при $\alpha = 0.1$. При этом значении α получается довольно низкое значение ошибки встраивания (PSNR= 46.01 дБ). В первой строке приведен фактор

сжатия по стандарту JPEG, во второй представлены ЦВЗ, извлеченные из сжатого изображения. Данные Таблицы 5 показывают, что извлеченный ЦВЗ визуально вполне различим, что свидетельствует о высокой устойчивости алгоритма к сжатию изображения в спектральной области.

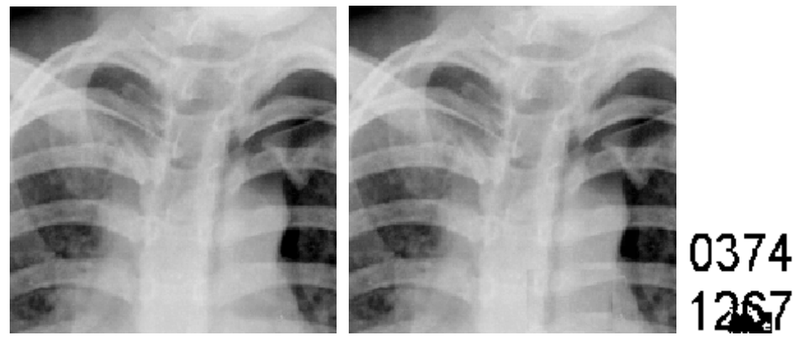
Таблица 5

Результаты исследования устойчивости алгоритма при сжатии в спектральной области по стандарту JPEG

Фактор JPEG	-	60	50	40	30	20
PSNR после сжатия	46.01	25.01	24.98	24.91	24.84	24.71
Извлеченный ЦВЗ						

Аналогичные результаты получаются и при других типах атак, перечисленных выше.

В конце четвертой главы рассмотрено важное приложение разработанного ЦВЗ-алгоритма к задаче контроля целостности и подлинности изображения. В результате анализа встроенного в изображение ЦВЗ необходимо выяснить, изменено ли содержание исходного изображения путем его принудительного искажения.



а б в

Рис. 4. Обнаружение нарушения целостности изображения: а – изображение со встроенным ЦВЗ (см. Рис. 3); б – искаженное изображение; в – извлеченный ЦВЗ, на котором видны следы искажения.

Пример 3. Контроль целостности и подлинности изображения. На Рис. 4 приведено изображение-оригинал (а), искаженное изображение (б) и извлеченный ЦВЗ (в). На Рис.4б. эти

искажения визуально не заметны, однако следы этих искажений видны на извлеченном ЦВЗ (в нижней части ЦВЗ), что доказывает факт принудительного искажения защищенного изображения. Следует отметить важность данного приложения к защите медицинских изображений, учитывая существование понятия врачебной тайны.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ДИССЕРТАЦИОННОЙ РАБОТЫ

1. Предложен обобщенный класс пространственных адаптивных устойчивых ЦВЗ-алгоритмов защиты цифрового изображения путем встраивания бинарного ЦВЗ, с учетом свойств визуальной системы человека.

2. Предложена математическая модель и метод исследования ошибок, возникающих вследствие встраивания и извлечения ЦВЗ, а также воздействия атак.

3. Получены аналитические выражения, связывающие ошибки процедур встраивания и извлечения ЦВЗ при наличии атак, с параметрами ЦВЗ-процедуры.

4. Предложен аналитический метод оценивания качества ЦВЗ-процедуры взамен общепринятого графического («магического треугольника»). Полученные формулы позволяют оценивать качество и другие важные характеристики ЦВЗ-процедуры на стадии проектирования системы защиты изображения без непосредственного выполнения операций встраивания и извлечения ЦВЗ.

5. Исследована устойчивость предложенной ЦВЗ-процедуры при наиболее распространенных типах атак (случайная атака, сжатие в спектральной области, геометрические атаки, принудительное изменение содержания и др.).

6. Создан комплекс алгоритмов и программ, реализующих метод защиты изображения путем встраивания в него бинарного ЦВЗ.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

1 Асатрян Д. Г., Ланина Н. С. Адаптивный алгоритм встраивания цифровых водяных знаков в изображение. Годичная научная конференция РАУ. Сборник научных статей. Ереван, с. 59-65, 2006.

2. Ланина Н. С. Об устойчивости к атакам пространственного алгоритма встраивания в изображение цифровых водяных знаков. Тезисы докладов научно-практической конференции по вопросам надежности и безопасности информационных систем. Армянская технологическая академия Майкрософт АРЭЙ. Ереван, с. 26-29, 2007.

3. Asatryan D., Lanina N., Shahverdyan H. Adaptive Robust Algorithm for Digital Watermarking of Medical Images. Proceedings of 6-th International Conference “Computer Science and Information Technologies – CSIT 2007”, Armenia, Yerevan, 24-28 September, pp.161-164, 2007.

4. Асатрян Д. Г., Ланина Н. С. Исследование ошибок в адаптивном методе цифровой защиты информации. Труды второй годичной научной конференции РАУ, Ереван, сс. 67-74, 2007.

5. Асатрян Д. Г., Ланина Н. С., Шахвердян Г. С. Устойчивые пространственные алгоритмы защиты цифровых изображений. Пятая международная научно-практическая конференция. Россия, Санкт-Петербург, том 12, сс. 49-51, 2008.

6. Asatryan D.G., Lanina N.S. Adaptive Robust Watermarking Algorithm for Image Protection. Vestnik RAU (Herald of the RAU), Armenia, Yerevan, pp. 50-56, 2009.

7. Ланина Н.С. Устойчивость к Stirmark-атакам адаптивного алгоритма защиты изображений. Вестник РАУ. Физико-математические и естественные науки. № 2, сс. 100-104, 2009.

ԱՄՓՈՓՈՒՄ

Չարտոնված օգտագործումից և բովանդակության աղավաղումից թվայնացված պատկերների պաշտպանության խնդիրները համարվել են կարևոր և արդիական մարդկության պատմության ողջ ընթացքում: Դրանք արդիական են նաև մեր օրերում, ի հետևանք ստեղծվող, մշակվող և կապի տարբեր միջոցներով հաղորդվող ինֆորմացիայի ծավալների շարունակական աճի և կիրառական նորանոր խնդիրների առաջացման: Ներկայումս թվայնացված ինֆորմացիայի պաշտպանության տեսությունը, մեթոդները և միջոցները բուռն զարգացում և կիրառություն են ապրում մարդու մտավոր գործունեության ամենատարբեր բնագավառներում:

Վերջին երկու տասնամյակներում ինֆորմացիայի պաշտպանության նպատակով կիրառվում են մեթոդներ, որոնք հիմնված են պաշտպանվող օբյեկտում գաղտնի ինֆորմացիայի ներմուծման եղանակի վրա (այսպես կոչված՝ ջրանշման միջոցով):

Թվային ջրանշման մեթոդներին նվիրված գիտական գրականության վերլուծությունը ցույց է տալիս, որ այդ բնագավառում կան մի շարք խնդիրներ, որոնք դեռևս մինչև վերջ լուծված չեն: Հայտնի է, որ ջրանշման ալգորիթմների որակին ներկայացվող պահանջները իրարամերժ են, ինչն ստիպում է յուրաքանչյուր կոնկրետ խնդրում գնալ փոխզիջման, ընդ որում, արդյունքը գնահատելու համար օգտագործվում է հիմնականում ցուցադրական, գրաֆիկական եղանակը: Բացի դրանից, կարևոր է նաև այն հանգամանքը, որ դեռևս չկա միասնական տեսություն, որը հնարավորություն է ընձեռում ուսումնասիրել առաջարկվող ալգորիթմների որակի բաղադրիչները, ուստի հետազոտողները հիմնականում հենվում են մոդելավորման տվյալների վրա:

Սույն աշխատանքի նպատակն է՝ պատկերի պաշտպանության համար դրանում երկուական ջրանիշի ներմուծման եղանակով ջրանշման ադապտիվ ալգորիթմների դասի, ինչպես նաև առաջարկված ալգորիթմների որակի անալիտիկական և էքսպերիմենտալ հետազոտման մեթոդաբանության մշակումը:

Ատենախոսության **առաջին գլխում** կատարվել է ատենախոսության թեմային առնչվող գիտական գրականության վերլուծություն, ինչի հիման վրա ձևակերպվել են խնդիրները և ուրվագծվել են դրանց լուծման մեթոդները:

Երկրորդ գլխում նկարագրվել է առաջարկված ադապտիվ ալգորիթմների դասը, որը ներառնում է ջրանիշի ներմուծման և արտածման ալգորիթմները: Ցույց է տրվել է մարդու տեսողական համակարգի հատկությունների օգտագործման հնարավորությունը, ինչը լավացնում է ալգորիթմի որակի պարամետրերը:

Երրորդ գլուխը նվիրված է ջրանիշի ներմուծման և հարձակումների հետևանքով առաջացած արտածման սխալների հաշվարկի անալիտիկական մեթոդի մշակմանը և դրանց էքսպերիմենտալ ուսումնասիրությանը: Այդ մեթոդը հնարավորություն է տալիս ստուգելու ալգորիթմի արդյունավետությունը՝ առանց ջրանշման գործընթացի անմիջական կատարման:

Չորրորդ գլխում կատարվել է տարբեր տեսակի հարձակումների նկատմամբ առաջարկված ալգորիթմի կայունության հետազոտություն: Մշակվել է ջրանշման ալգորիթմի որակի ընդհանրացված չափանիշ: Ի տարբերություն լայնորեն կիրառվող գրաֆիկական եղանակի, այս չափանիշը հնարավորություն է տալիս կանխագուշակել ալգորիթմի որակի բաղադրիչները՝ ջրանշման գործընթացը բնորոշող պարամետրերի հիման վրա:

Այսպիսով, ատենախոսության մեջ ստացվել են հետևյալ հիմնական արդյունքները.

1. Առաջարկվել է ջրանշման տարածական ադապտիվ և կայուն ալգորիթմների ընդհանրացված դաս թվայնացված պատկերի պաշտպանության համար:

2. Առաջարկվել է կամայական ջրանշման ալգորիթմում բինար ջրանիշի ներմուծման և արտածման, ինչպես նաև հարձակումների պատճառով առաջացող սխալանքի նկարագրման մաթեմատիկական մոդել և հետազոտման մեթոդ:

3. Ստացվել են ջրանշման ալգորիթմում հարձակման պարագայում ներմուծման և արտածման սխալանքը ալգորիթմի պարամետրերի հետ կապող անալիտիկական արտահայտություններ:

4. Առաջարկվել է ջրանշման ընթացակարգի որակի գնահատման անալիտիկական մեթոդ՝ լայնորեն կիրառվող գրաֆիկական մեթոդի (այսպես կոչված՝ «կախարդական եռանկյունու») փոխարեն: Ստացված բանաձևերը հնարավորություն են տալիս գնահատելու ջրանշման ողջ ընթացակարգի որակը և այլ կարևոր բնութագրերը ինֆորմացիայի պաշտպանության համակարգի նախագծման փուլում՝ առանց ջրանիշի ներմուծման և արտածման գործողությունների անմիջական կատարման:

5. Հետազոտված է առաջարկված ջրանշման ալգորիթմի կայունությունը հարձակումների առավել տարածված տեսակների դեպքում (պատահական հարձակումներ, սպեկտրալ տիրույթում սեղմում, երկրաչափական բնույթի հարձակումներ, բովանդակության հարկադրական փոփոխություն և այլն):

6. Ստեղծվել է երկուական ջրանիշի ներմուծման ճանապարհով պատկերի պաշտպանության մեթոդն իրականացնող ալգորիթմների ու կոմպյուտերային ծրագրերի համալիր:

Lanina S. Natalya

DEVELOPMENT OF A COMPLEX OF ALGORITHMS AND SOFTWARE TOOLS FOR PROTECTION OF DIGITAL IMAGES

SUMMARY

The problems of protection of digital images from the unsupervised access and content forgery were considered as important and actual during the whole human history. These are also topical nowadays due to the continually growing of volume of information, being created, processed and transmitted via various communication channels, and arising of newer applications as well. Nowadays the theory, methods and means for digital information protecting are rapidly developed and applied in various fields of human intellectual activity.

During last two decades the methods for embedding secret information (so-called watermark) in the protecting object were investigated.

The analysis of scientific literature devoted to the watermarking problems shows that there is a whole number of problems not solved yet. It is known that the requirements to any watermarking algorithm are contradictious, which forces to come to a compromise in a concrete problem. In these cases basically a graphical method is used for demonstration of behavior of quality components. Moreover, there isn't any integrated theory, which allows the investigation of the quality components, so the investigators rely on the simulation data.

The goal of present investigation is developing of a class of adaptive watermarking algorithm based on embedding of binary watermark into an image, as well as of a method of the analytical and experimental investigation of the proposed watermarking procedure quality.

In Chapter 1 of the dissertation an analysis of scientific literature related to the theme is done and in this basis some problems have been formulated and solution methods of them are outlined.

In Chapter 2 the proposed class of adaptive algorithms, which includes the watermark embedding and extracting algorithms, is described. The possibility and a method of using the properties of the human visual system to enhance the quality parameters of algorithm are shown.

Chapter 3 is devoted to a method of creating of the analytical calculation end experimental investigation of the errors of a watermark embedding and extracting at the presence of an attack. The method allows checking the effectiveness of the proposed algorithm without any immediate performing of the watermarking procedure.

In Chapter 4 the robustness of the proposed algorithm against various attacks is investigated. A generalized criterion for watermarking procedure quality assessment is created.

Unlike to the widely used graphical method, this method allows forecasting of the quality components on basis of parameters, which describe the watermarking procedure.

Thus, main results in this dissertation are the following.

1. A generalized class of adaptive and robust watermarking algorithms for digitized image protection.

2. A mathematical model and investigation method for describing of the binary watermark embedding and extracting errors by arbitrary watermarking algorithm at presence of an attack are proposed.

3. Analytical expressions for watermark embedding and extracting errors depending on algorithm parameters are obtained.

4. An analytical method for quality assessment of watermarking procedure instead of widely used graphical method (so-called "Magic Triangle") is proposed. The derived formulas allow assessment of the quality and other important characteristics of the whole watermarking procedure on the stage of designing of the information protecting without any immediate performing of the watermark embedding and extracting procedure.

5. The robustness of proposed algorithm against the most propagated types of attack (random attacks, compression in the frequency domain, geometrical attacks, forgery of information content etc) is investigated.

6. A complex of algorithms and software tools, which realize the proposed image protection algorithm by using the embedding of binary watermark, is created.