ՀՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱ
ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

ԱՍԱՏՐՅԱՆ ՆԱԻՐԱ ՍԱՄՎԵԼԻ

ՄՈՒԼՏԻՄԵԴԻԱԿԱՆ ԻՆՖՈՐՄԱՑԻԱՅԻ ՊԱՇՏՊԱՆՈՒԹՅԱՆ ՀԱՄԱԿՑՎԱԾ ԱԼԳՈՐԻԹՄՆԵՐԻ ՄՇԱԿՈՒՄ

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

ՍԵՂՄԱԳԻՐ

Երևան – 2013

НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АРМЕНИИ
ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ

АСАТРЯН НАИРА САМВЕЛОВНА

РАЗРАБОТКА КОМБИНИРОВАННЫХ АЛГОРИТМОВ ЗАЩИТЫ МУЛЬТИМЕДИЙНОЙ ИНФОРМАЦИИ

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

Ереван – 2013

Ատենախոսության թեման հաստատվել է Հայ-Ռուսական (Սլավոնական) համալսարանում

Գիտական ղեկավար՝	տ.գ.դ.	Դ.Գ. Ասատրյան
Պաշտոնական ընդդիմախոսներ՝	տ.գ.դ.	Գ.Հ.Խաչատրյան
	տ.գ.թ.	Վ.Գ. Մարկարով

Առաջատար կազմակերպություն՝ Երևանի կապի միջոցների գիտահետազոտական ինստիտուտ

Ատենախոսության պաշտպանությունը կայանալու է 2013թ. Մայիսի 10-ին, ժամը 16.00–ին ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող 037 "Ինֆորմատիկա և հաշվողական համալիրներ" մասնագիտական խորհրդի նիստում, հետևյալ հասցեով՝ Երևան, 0014, Պ.Սևակի փ. 1:

Ատենախոսությանը կարելի է ծանոթանալ ինստիտուտի գրադարանում:
Սեղմագիրն առաքված է 2013թ. Ապրիլի 10-ին:

Մասնագիտական խորհրդի գիտական քարտուղար, ֆ.-մ. գ .դ. Հ.Գ. Սարուխանյան

Тема диссертации утверждена в Российско-Армянском (Славянском) университете

Научный руководитель:	д.т.н.	Д.Г. Асатрян
Официальные оппоненты:	д.т.н.	Г.Г.Хачатрян
	к.т.н.	В.Г.Маркаров

Ведущая организация: Ереванский научно-исследовательский институт средств связи

Защита диссертации состоится 10 мая 2013г. в 16.00 часов 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 10 апреля 2013г.

Ученый секретарь Специализированного совета, д.ф.-м.н. А.Г. Саруханян

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность проблемы

Проблема защиты информации от несанкционированного доступа, использования и изменения, которая сопровождала человечество на всем протяжении его истории, стала особенно актуальной со второй половины двадцатого века. Картины, фотографии, музыка, фильмы и другие продукты интеллектуальной деятельности в течение веков сохранялись на физических носителях. С развитием компьютерных технологий многие произведения стали оцифровывать и информацию стало удобно хранить, воспроизводить и распространять, но, в то же время, возникла возможность неразрешенного копирования, использования и изменения ее содержания.

В последние два десятилетия для защиты мультимедийной продукции от подобного рода действий стали разрабатывать и успешно применять специальные цифровые технологии. В частности, к ним также относятся технологии, основанные на алгоритмах встраивания в защищаемый объект цифрового водяного знака (ЦВЗ) и обеспечивающих возможность последующего его извлечения. Наличие ЦВЗ в спорном объекте доказывалось сравнением встроенных и извлеченных данных.

Основными требованиями к ЦВЗ-алгоритмам являются незаметность встраиваемых меток с точки зрения аудиовизуального восприятия человека, устойчивость процедуры к атакам разного рода и объем данных, который возможно встраивать в защищаемый объект по данному алгоритму.

С развитием данного научного направления стали разрабатываться методы, позволяющие реализовать встраивание и извлечение ЦВЗ, представляющих собой разнотипную мультимедийную информацию, что позволило применять ЦВЗ-технологии и для сокрытия информации, скрытого аннотирования с целью совместного хранения общедоступных и секретных данных и др. В связи с этим возникла необходимость исследования возможности встраивания ЦВЗ как можно большего объема при обеспечении требуемого качества объекта со встроенным ЦВЗ и приемлемой устойчивости к атакам. Анализ многочисленных научных публикаций указывает на отсутствие сколько-нибудь универсальных методов, позволяющих значительно увеличить объем встраиваемой информации.

Настоящая работа посвящена разработке и реализации ЦВЗ-метода, который позволяет встраивать в произвольное изображение ЦВЗ большого объема при сохранении приемлемой устойчивости к атакам и необнаруживаемости ЦВЗ.

Разработанный подход основан на предложенной нами концепции увеличения объема встраиваемых данных, позволяющей встраивание большого объема информации при достаточной узнаваемости извлеченной информации независимо от того, искажения этой информации произошло от атак или вызваны самим процессом встраивания.

Целью работы является разработка метода защиты изображения при одновременном сокрытии в нем данных большого объема с хорошими показателями качества путем комбинирования пространственных и частотных ЦВЗ-алгоритмов, а также создание методики аналитического и экспериментального исследования достигаемых при этом эффектов.

Для достижения указанной цели в диссертации решены следующие **задачи**:

• изыскание эффективного подхода комбинирования пространственных и частотных ЦВЗ-методов для реализации концепции увеличения объема встраиваемой информации;

• разработка и исследование комбинированного алгоритма;

• разработка математической модели ошибок встраивания и извлечения, и соответствующей методики аналитического и экспериментального исследования качества ЦВЗ-процедуры;

• разработка комплекса алгоритмов и программ для реализации комбинированного алгоритма;

• приложение разработанного комплекса алгоритмов и программ к практическим задачам.

Методы исследования

В работе применялись:

• современные методы цифровой обработки изображений в пространственной и спектральной областях;

• статистические методы моделирования и численного анализа;

• компьютерные технологии и методы регистрации, обработки, визуализации и отображения данных.

Научная новизна работы

В процессе исследования были получены следующие результаты, отличающиеся новизной:

• разработан адаптивный линейный ЦВЗ-алгоритм защиты серотонного изображения при помощи встраивания серотонного ЦВЗ;

• предложена математическая модель и аналитический метод исследования ошибок линейного алгоритма, возникающих вследствие встраивания и извлечения ЦВЗ-изображения, при воздействии атак;

• предложена концепция увеличения объема встраиваемых данных и разработан соответствующий подход для комбинирования пространственных и частотных ЦВЗ-методов;

• разработан, реализован и исследован комбинированный ЦВЗ-алгоритм с одновременным сокрытием в нем данных в объеме, значительно превышающем объем защищаемого изображения;

• теоретически и экспериментально исследована возможность применения преобразования Арнольда для повышения качества ЦВЗ-процедуры.

• создан комплекс программ, реализующий предложенные линейный и комбинированный алгоритмы защиты изображения.

• предложены варианты решения практических задач, связанных с защитой цветного изображения, обнаружения подделки изображения и др. с помощью применения разработанного комплекса.

На защиту выносятся следующие научные положения:

• концепция увеличения объема встраиваемых данных и соответствующий подход для комбинирования пространственных и частотных ЦВЗ-методов;

• класс комбинированных пространственно-частотных алгоритмов для защиты изображения и одновременного сокрытия в нем данных большого объема;

• математическая модель и аналитический метод исследования ошибок линейного алгоритма, возникающих вследствие встраивания и извлечения ЦВЗ-изображения, при воздействии атак;

• численные модели и результаты экспериментального исследования объемов встраиваемых данных, устойчивости к атакам и других параметров качества предложенной ЦВЗ-процедуры;

• комплекс алгоритмов и программ, реализующий предложенную методику защиты изображения и исследования характеристик качества.

Практическая ценность работы

Получены следующие результаты, представляющие практический интерес:

• создан комплекс алгоритмов и программ, реализующий устойчивый метод защиты изображения;

• создан комплекс алгоритмов и программ, реализующий метод защиты изображения и одновременного сокрытия в нем данных объемом, в несколько раз превышающим его собственный;

• получены аналитические выражения для предварительной оценки устойчивости и других характеристик комбинированного алгоритма 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.

Основные результаты диссертационной работы **внедрены** в учебный процесс Российско-Армянского (Славянского) университета (РАУ) и опубликованы в учебно-методическом пособии Асатрян Д.Г., Асатрян Н.С., Ланина Н.С., Таирян С.В. Основы цифровой защиты мультимедийной информации. Изд. РАУ, Ереван, 104 с., 2011.

Апробация работы

Основные положения и материалы диссертации обсуждались на семинарах факультета прикладной математики и информатики и кафедры Математической кибернетики Российско-Армянского (Славянского) университета (РАУ), докладывались на следующих научных конференциях:

- на годичных научных конференциях РАУ, 2009, 2010;
- на международных научных конференциях «Компьютерная наука и информационные технологии – CSIT», 2009, 2011;
- на научном семинаре кафедры «Информационной безопасности и программного обеспечения» ГИУА.
- на Первом армянском международном конгрессе «ARMTELEMED: Road to the Future», 2011.

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 104 наименований и основных выводов по диссертации. Основной текст изложен на 104 страницах, включая 16 рисунков, 7 графиков и 7 таблиц.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность проблемы, научная новизна и практическое значение полученных результатов, сформулированы цель и задачи работы, а также основные положения, выносимые на защиту.

В первой главе приведены обзор научной литературы, изданной преимущественно за последние 5 лет, и анализ современного состояния рассматриваемой проблемы. Кратко изложена история развития систем защиты авторских прав, основанных на ЦВЗ-технологиях, рассмотрены основные требования к ЦВЗ-алгоритмам, их основные области приложения.

На примерах нескольких алгоритмов исследуются недостатки, присущие пространственному и частотному подходам к разработке ЦВЗ-алгоритмов, и положительные эффекты, возникающие в результате их комбинирования. В частности, указывается на возможность увеличения объема встраиваемых данных и повышения устойчивости к атакам. Анализируются недостатки известных в литературе комбинированных алгоритмов.

Специально рассматривается литература по медицинским ЦВЗ-технологиям. Приводятся основные требования, предъявляемые к таким алгоритмам, связанные со спецификой медицинских задач. Указывается, что ЦВЗ-алгоритмы, применяемые для

аннотирования медицинских изображений, должны обеспечивать высокое качество получаемого изображения и при этом позволять встраивание информации большого объема. Указывается, что недостатком уже существующих методов является небольшой объем встраиваемой информации.

Отмечается, что в некоторых статьях зарубежных исследователей, опубликованных после выхода в свет работ автора настоящей диссертационной работы, был проанализирован предложенный нами подход, выполнены эксперименты и сравнительные исследования, показывающие его эффективность. В этих работах указано, что использование разработанного нами комбинированного пространственно-частотного алгоритма дает возможность существенно увеличить объем встраиваемой информации и в то же время обеспечить достаточно высокое качество извлеченной информации.

Вторая глава посвящена разработке линейного алгоритма встраивания ЦВЗ в пространственную область изображения-контейнера. Линейный алгоритм является основной процедурой, используемой в разработанном в следующей главе комбинированном алгоритме.

Приведем описание линейного ЦВЗ-алгоритма. По данному алгоритму в серотонное изображение-контейнер (или в один из цветовых каналов цветного 24-битового изображения) $I = \{a_{mn}\}$ размерами $M \times N$, $m = 0,1,...,M-1$, $n = 0,1,...,N-1$ встраивается серотонное ЦВЗ-изображение $W = \{w_{kl}\}$ размерами $K \times L$, $k = 0,1,...,K-1$, $l = 0,1,...,L-1$.

Пусть, для простоты, K и L кратны M и N соответственно. Изображение I разбивается на $K \times L$ непересекающихся блоков I_ξ размерами $(M/K)\times(N/L)$, $\xi = 0,1,...,(K \times L)-1$. Каждый из блоков изображения I ставится во взаимно-однозначное соответствие с пикселами ЦВЗ W. Для увеличения секретности может быть применен алгоритм перемешивания координат пикселов с помощью определенного псевдослучайного правила.

Пусть w_ξ – пиксел ЦВЗ W, встраиваемый в блок $I_\xi = \{a_{m_\xi n_\xi}\}$

Встраивание ЦВЗ осуществляется по формуле

$$a^W_{m_\xi n_\xi} = (1-\alpha)a_{m_\xi n_\xi} + \alpha w_\xi, \qquad (1)$$

где $a_{m_\xi n_\xi}$ – соответствующий пиксел изображения со встроенным ЦВЗ I^W при фиксированном для всех блоков изображения-контейнера значении $\alpha > 0$. Таким образом, в каждый из MN/KL пикселов блока I_ξ встраивается один и тот же пиксел ЦВЗ – w_ξ и по одному и тому же правилу.

Процедура извлечения ЦВЗ основана на методе наименьших квадратов (МНК) для оценки неизвестного параметра w^X_ξ с помощью значений пикселов $a^{W,X}_{ij}$ блока ξ, возможно подвергнутого атаке, изображения $I^{W,X}$, где X обозначает атаку.

Используя (1) можно получить МНК-оценку параметра w_ξ^X

$$\hat{w}_\xi^X = \frac{\mu_\xi^{W,X} - (1-\alpha)\mu_\xi}{\alpha},$$

где μ_ξ и $\mu_\xi^{W,X}$ средние значения интенсивностей пикселов ξ - го блока изображения-контейнера до и после встраивания ЦВЗ с последующей атакой.

$$\mu_\xi = \frac{KL}{MN}\sum_{m_\xi}\sum_{n_\xi} a_{m_\xi n_\xi},\ \mu_\xi^{W,X} = \frac{KL}{MN}\sum_{m_\xi}\sum_{n_\xi} a_{m_\xi n_\xi}^{W,X}.$$

Далее исследованы ошибки, возникающие при встраивании и извлечении ЦВЗ по линейному алгоритму при различных типах атак.

Об эффективности алгоритма при фиксированном объеме ЦВЗ можно судить исходя из степени искажения защищаемого изображения, вследствие встраивания ЦВЗ и по степени узнаваемости ЦВЗ в данных, извлеченных из защищаемого изображения, возможно атакованного.

Эффективность большинства известных ЦВЗ-алгоритмов устанавливается экспериментально. В данной работе для измерения расхождения между изображением со встроенным ЦВЗ и исходным изображением, встроенным и извлеченным ЦВЗ, использовались критерии, основанные на среднеквадратическом отклонении сравниваемых изображений (СКО, MSE).

Для двух изображений $I_1(m,n)$ и $I_2(m,n)$ с одинаковыми размерами $M \times N$, $m = 0,1,...,M-1$, $n = 0,1,...,N-1$ средний квадрат отклонения этих изображений определяется по формуле

$$MSE = \sqrt{\frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\left|I_1(m,n) - I_2(m,n)\right|^2}.$$

Для оценивания качества ЦВЗ-процедуры используется также пиковое отношение сигнал/шум

$$PSNR = 10\log_{10}\left(\frac{MAX^2(I_1,I_2)}{MSE^2}\right) \text{ дБ},$$

где $MAX(I_1,I_2)$ – динамический диапазон расхождения между пикселами изображений I_1 и I_2. В отличие от MSE, $PSNR$ характеризует степень сходства изображений I_1 и I_2.

Далее в работе приведены описание и результаты экспериментов, показывающие устойчивость линейного алгоритма к наиболее распространенным типам атак.

Приведем пример. В серотонное изображение Lena[*)] размерами 512×512 пикселов встраивался ЦВЗ, представляющий собой серотонное изображение Cameraman размерами 128×128 пикселов, с коэффициентом, определяющим силу встраивания $\alpha > 0.03$. Затем изображение со встроенным ЦВЗ подвергалось атаке. Извлеченное из атакованного изображения ЦВЗ сравнивалось с изображением Cameraman путем расчета значения $PSNR$. Типы атак, применяемых к изображению со встроенным ЦВЗ, извлеченные ЦВЗ-изображения и полученные значения $PSNR$ представлены на Табл. 1.

Таблица 1.Результаты экспериментов по исследованию устойчивости линейного алгоритма к наиболее распространенным типам атак

Сжатие JPEG с параметром качества 60	Сжатие JPEG2000 с параметром 20	Увеличение значений пикселов	Комб. атака: «гауссовский шум+JPEG»
			
PSNR=20.46дБ	PSNR=24.65дБ	PSNR=11.09дБ	PSNR=17.60дБ

Как визуальный анализ извлеченных ЦВЗ-изображений, так и приведенные количественные оценки их качества показывают, что линейный алгоритм устойчив к наиболее распространенным типам атак.

В работе также разработан метод аналитического расчета ошибок встраивания и извлечения ЦВЗ, который позволяет определять параметры ЦВЗ-процедуры без непосредственного осуществления этих операций.

Обозначим через $E_{emb.}$ среднеквадратичную ошибку встраивания ЦВЗ, характеризующую степень искажения оригинального изображения в результате встраивания.

Предполагается, что в результате атаки значения пикселов изображения со встроенным ЦВЗ изменяются случайным образом, в соответствии с формулой

$$a^{W,X}_{m_\xi,n_\xi} = (1-\alpha)a_{m_\xi n_\xi} + \alpha w_\xi + x_{m_\xi n_\xi},$$

где $x_{m_\xi n_\xi}$ – элемент случайной выборки из X, со средним 0 и дисперсией σ^2_X.

В диссертации показано, что в случае атаки рассматриваемого типа (без учета ошибок визуализации)

$$E^2_{emb} = E\left[\frac{1}{MN}\sum_\xi\sum_{m_\xi}\sum_{n_\xi}\left(a^{W,X}_{m_\xi n_\xi} - a_{m_\xi n_\xi}\right)^2\right] = \frac{\alpha^2}{KL}\sum_\xi\left(w_\xi - \mu_\xi\right)^2 + \frac{\alpha^2}{KL}\sum_\xi S^2_\xi + \sigma^2_X, \quad (2)$$

[*)] Здесь и далее используются названия изображений, широко известных в литературе по обработке изображений

где

$$\mu_\xi = \frac{KL}{MN}\sum_{m_\xi}\sum_{n_\xi} a_{m_\xi n_\xi},\ S_\xi^2 = \frac{KL}{MN}\sum_{m_\xi}\sum_{n_\xi}\left(a_{m_\xi n_\xi} - \mu_\xi\right)^2.$$

Второй тип ошибки – средняя ошибка извлечения $E_{extr.}$ – относится к устойчивости метода и определяет качество извлеченного ЦВЗ в случае наличия атаки.

Ошибка извлечения вычисляется по формуле

$$E_{extr}^2 = E\left[\frac{1}{KL}\sum_{\xi}\left(\hat{w}_\xi^X - w_\xi\right)^2\right] = \frac{KL}{MN}\frac{\sigma_X^2}{\alpha^2}. \quad (3)$$

Как видно из формулы (3), средняя ошибка извлечения в случае атаки не зависит от изображения-контейнера, но пропорциональна отношению σ_X / α. Этот факт можно использовать при планировании стратегии защиты изображения и выбора необходимых параметров ЦВЗ-процедуры.

Величина KL/MN может быть интерпретирована как объем информации, которую возможно встраивать по линейному алгоритму, т.к. равна среднему количеству байтов ЦВЗ, встраиваемых в один байт изображения-контейнера. Устойчивость метода обеспечивается при $(KL/MN)<1$, т.е. алгоритм устойчив, если размер ЦВЗ, по крайней мере, в два раза меньше размера изображения-контейнера.

Во второй главе исследуется также ошибка, возникающая из-за неизбежного округления значений интенсивностей пикселов до целочисленного значения данных для их визуализации на экране монитора. Дается количественная оценка расхождения теоретически рассчитанных ошибок встраивания и извлечения ЦВЗ с экспериментальными. Показывается, что если предположить, что ошибки округления интенсивностей пикселов являются независимыми случайными величинами, распределенными равномерно на интервале $(-0.5;0.5)$ с дисперсией $\sigma_{round}^2 = 1/12$, то результирующее сходство между гипотетическим (с нецелочисленными значениями интенсивностей) и визуализированным (с целочисленными значениями) при отсутствии атаки (т.е. при $\sigma_X^2 = 0$) будет составлять около 60 дБ. Таким образом, когда речь идет об изображении со встроенным ЦВЗ, то искажения, вызванные визуализацией, можно рассматривать как последствия некой атаки. Поэтому извлеченный ЦВЗ даже в отсутствие атаки не является точной копией встроенного ЦВЗ и при разработке ЦВЗ-алгоритмов надо закладывать несколько избыточную степень устойчивости к атакам.

Далее во второй главе рассматривается вопрос о зависимости качества ЦВЗ-процедуры от правила установления взаимно-однозначного соответствия пикселов ЦВЗ к блокам изображения-контейнера. Для увеличения секретности часто применяется

псевдослучайное правило, позволяющее перемешивать случайным образом соответствующие пикселы изображения.

Из выражений для вычисления ошибки встраивания (2) видно, что при перемешивании пикселов изображения-контейнера или ЦВЗ может измениться первое слагаемое, поэтому ошибка зависит от процедуры перемешивания.

В настоящей работе в качестве модели перемешивания пикселов применяется преобразование Арнольда. При этом рассматриваются две задачи.

1. Оценить ошибку встраивания, когда преобразование Арнольда применяется к ЦВЗ n_{iter} раз при фиксированном изображении-контейнере. Можно ли рассчитывать на уменьшение ошибки встраивания в зависимости от количества итераций преобразования Арнольда?

2. Преобразование Арнольда применяется к изображению контейнеру n_{iter} раз и осуществляется встраивание ЦВЗ в преобразованное изображение. Полученное в результате этих процедур изображение подвергается $(T - n_{iter})$ итерациям преобразования Арнольда, где T - период. Можно ли рассчитывать на уменьшение ошибки встраивания в зависимости от количества итераций преобразования Арнольда?

В работе показано, что

1. Ошибка встраивания $E_{emb.}$ в этом случае можно рассчитывается по формуле (2) при интерпретации результата применения преобразования Арнольда как случайную величину. В результате получаем, что $E_{emb.}$ не зависит от числа примененных итераций.

2. Применение преобразования Арнольда может, как увеличить, так и уменьшить ошибку встраивания, но в обоих случаях незначительно. На Рис.1 в качестве примера приведен график зависимости качества изображения со встроенным ЦВЗ, выражаемого через экспериментально полученные значения $PSNR$, от числа итераций преобразования Арнольда, примененного к ЦВЗ-изображению.

Рис.1. График зависимости качества изображения с ЦВЗ от числа примененных итераций преобразования Арнольда.

Видно, что для данной конкретной пары изображение-контейнер и ЦВЗ применение преобразования Арнольда привело к улучшению качества защищаемого изображения.

Таким образом, нами как аналитически, так и экспериментально доказано, что применение преобразования Арнольда в линейном алгоритме незначительно влияет на качество изображения с ЦВЗ.

Третья глава посвящена разработке и исследованию комбинированного ЦВЗ-алгоритма. В начале главы предлагается концепция увеличения объема встраиваемой информации, основанная на предварительном сжатии ЦВЗ с допустимым уровнем искажений и приемлемой степенью устойчивости к атакам.

В качестве ЦВЗ-модели применяется линейный алгоритм, предложенный во второй главе, с учетом использования в качестве ЦВЗ сжатого спектра встраиваемой информации.

Сжатие, встраивание и извлечение ЦВЗ-изображения. Сжатие осуществляется при помощи Дискретного Косинусного Преобразования (ДКП) в соответствии со следующим алгоритмом:

- ЦВЗ $W = \{w_{kl}\}\ (k = 0,1,...K-1; l = 0,1,...,L-1)$ разбивается на блоки размерами $b \times b$ пикселов, где b может принимать значения 4, 8 или 16 в зависимости от размеров ЦВЗ-изображения и от конкретной задачи.
- для каждого блока рассчитывается матрица ДКП $DCT = \left(DCT_{ij}\right)$ $\left(i = 0,1,...b-1,\ j = 0,1,...,b-1\right)$.
- сохраняются только $t \times t$ коэффициентов ДКП каждого блока, остальные отбрасываются;
- сохраненные коэффициенты всех блоков объединяются в «сжатую» матрицу $DCT^{comp.} = \left(DCT^{comp.}_{k'l'}\right)$ размерами $K' \times L'$ $\left(k' = 0,1,...K'-1, l' = 0,1,...,L'-1\right)$;
- каждому элементу матрицы $DCT^{comp.}$ ставится в соответствие целочисленное значение из промежутка [0,255] по правилу

$$w'_{k'l'} = 255\frac{DCT^{comp.}_{k'l'} - Min}{Max - Min},$$

где Max, Min - соответственно максимальное и минимальное значения интенсивностей пикселов матрицы $DCT^{comp.}$, являющиеся частью информации, которая в случае необходимости используется для восстановления ЦВЗ-изображения из извлеченных данных.

Схема преобразования ЦВЗ по комбинированному алгоритму дана на Рис.2.

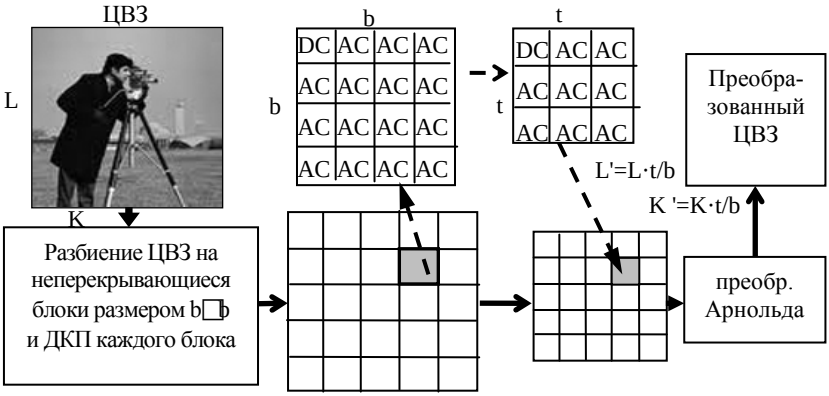
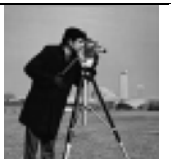


Рис.2. Схема преобразования ЦВЗ по комбинированному алгоритму.

Для исследования качества предложенного комбинированного алгоритма крайне важным является изучение качества информации после описываемых выше преобразований ЦВЗ. Поэтому проведены следующие численные эксперименты: серотонное изображение сжималось описанным выше способом. Каждый раз сохранялся определенный процент коэффициентов (25%, 6.25%, 1.25%). Полученная путем отбрасывания коэффициентов сжатая матрица ДКП $DCT^{comp.}$ дополнялась нулями до размеров исходного изображения и подвергалась обратному ДКП и преобразованию в изображение. В Таблице 2 приведен пример, показывающий зависимость качества полученных изображений от процента сохраняемых при сжатии коэффициентов ДКП.

Таблица 2. Результаты экспериментов по сжатию ЦВЗ

	100%	25%	6. 25%	1. 25%
Получен-ное изобр.				
PSNR	∞	40.01 дБ	27.84 дБ	22.73 дБ

Эксперименты показали, что даже при достаточно сильном сжатии до 25% от первоначального объема, изображение, полученное в результате обратных преобразований, визуально неотличимо от оригинального ($PSNR = 40.01$ дБ).

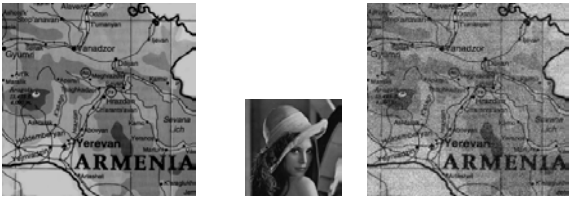
Таким образом, предложенный метод предварительного преобразования ЦВЗ может быть использован в ЦВЗ-алгоритмах с целью искусственного уменьшения объема

встраиваемых данных, что в конечном итоге позволяет встраивать ЦВЗ-изображение бóльшего размера.

Заметим, что описанная ЦВЗ-процедура применима для защиты произвольного мультимедийного объекта при надлежащем представлении участвующих в процедуре объектов.

Иллюстрация концепции увеличения объема встраиваемой информации (экспериментальное исследование свойств комбинированного алгоритма). Проведены эксперименты по встраиванию ЦВЗ бóльшего размера (Рис. 3a) в изображение меньшего размера (Рис. 3b). ЦВЗ-изображение преобразовано по комбинированному алгоритму (сохранено только 6.25% коэффициентов ДКП) и встроено по линейному алгоритму. Полученное изображение со встроенными данными подвергнуто атаке типа «сжатие».

Было установлено, что при этом обеспечивается степень устойчивости, позволяющая использовать извлеченное из атакованного изображения ЦВЗ по назначению (см. Рис. 3c), в данном случае в качестве карты



a b c

Рис.3. Результаты эксперимента по встраиванию ЦВЗ большого размера в изображение меньшего размера

Исследование компромисса между степенью сжатия ЦВЗ по комбинированному алгоритму и устойчивостью ЦВЗ-процедуры. При применении комбинированного подхода кроме ошибок извлечения, возникающих в результате атаки на контейнер с ЦВЗ, добавляются ошибки, возникающие вследствие предварительного преобразования ЦВЗ-изображения. Представляет интерес исследование зависимости устойчивости комбинированного алгоритма от соотношения объемов ЦВЗ-изображения до и после сжатия. Результаты экспериментов иллюстрируются графиком, приведенным на Рис.4.

Наличие максимума на кривой связано с тем, что уменьшение объема встраиваемых данных путем сжатия уменьшает ошибку встраивания и, следовательно, улучшает качество извлеченного ЦВЗ. В то же время при увеличении степени сжатия оно само становится причиной ухудшения качества извлеченной информации. Эти две противодействующие тенденции приводят к возникновению максимума, что и наблюдается в данном эксперименте.

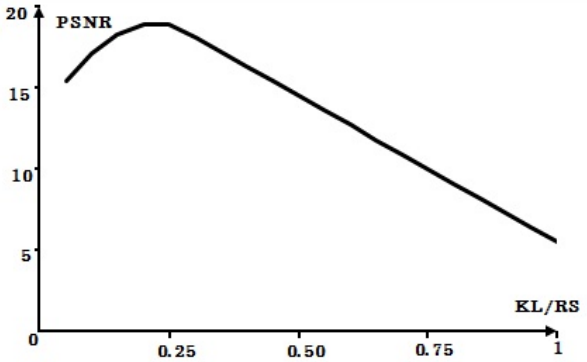


Рис.4. Зависимость качества извлеченного ЦВЗ от степени его сжатия.

Таким образом, варьируя параметр сжатия, можно добиться необходимой степени устойчивости процедуры при данном объеме оригинала ЦВЗ.

Сравнение с другими ЦВЗ-алгоритмами. Проведен сравнительный анализ комбинированного и других ЦВЗ-алгоритмов схожего типа. Представлены результаты экспериментальных исследований, полученные как нами, так и зарубежными исследователями, позволяющие утверждать, что комбинированный алгоритм конкурентоспособен, а по некоторым параметрам, например, по устойчивости к наиболее распространенным типам атак, по количеству информации, которую возможно встраивать по данному алгоритму, превосходит другие алгоритмы.

В Табл. 3 приведена зависимость числа ошибок при установления факта наличия ЦВЗ в исследуемом изображении от типа атаки[*)] при использовании различных алгоритмов.

Таблица 3.Результаты сравнительного анализа различных алгоритмов

Тип атаки	Комб. алгоритм	Метод Mohanty	Метод Rahmani
Атака отсутствует	0/2500	0/2500	0/2500
Сжатие JEPG (10,40)	**1/2500**	6/2500	3/2500
Гауссовский шум	**2/2500**	3/2500	3/2500
Увеличение резкости	**1/2500**	4/2500	3/2500
Размывание изображения	**2/2500**	**2/2500**	**2/2500**
Обрезка (40%, 50%, 60%)	**1/2500**	20/2500	**1/2500**

Видно, что наименьшее количество ошибок зафиксировано в случаях, когда ЦВЗ был встроен по комбинированному алгоритму.

[*)] Rahmani H., Mortezaei R., Moghaddam M. E. A New Robust Watermarking Scheme to Increase Image Security. EURASIP Journal on Advances in Signal Processing. Vol. 2010, Article ID 428183.

Выбор наиболее подходящего цветового канала для встраивания ЦВЗ. Известно, что предпочтение тому или цветовому каналу при встраивание ЦВЗ в цветное изображение обычно отдается на основе экспериментальных результатов, т.к. отсутствуют аналитические формулы, позволяющие получать количественные оценки основных характеристик ЦВЗ-алгоритма. Мы предлагаем перед осуществлением встраивания ЦВЗ по комбинированному алгоритму разлагать цветное изображение на цветовые каналы различных цветовых моделей и для каждого канала по формуле (2) рассчитывать значение ошибки встраивания. Затем встраивать ЦВЗ в цветовой канал, для которого было получено наименьшее значение MSE^2. Таким образом, выбор канала для осуществления процедуры встраивания осуществляется на основе расчетов и не требует осуществления процедур встраивания и извлечения.

В четвертой главе рассматриваются различные приложения комбинированного пространственно-частотного алгоритма встраивания ЦВЗ.

Предварительно дается краткое описание программной системы, состоящей из модулей, реализующих встраивание и извлечение ЦВЗ по линейному и комбинированному алгоритмам, моделирующих атаки типа «наложение шума» с различными распределениями, моделирующих преобразование Арнольда, а также прямое и обратное преобразования ЦВЗ-изображения.

В программной системе предусмотрена возможность визуализации изображений, получаемых на каждом этапе экспериментов, что позволяет отслеживать их качество (степень искажения) не только с применением метрик попиксельно сравнения с их оригиналами, а также с точки зрения визуального восприятия человека.

Далее предлагается ***метод одновременной защиты и аннотирования медицинского изображения***. Для этого медицинское изображение «достраивается» фрагментом, не имеющим информативной ценности. В достроенный фрагмент встраивается аннотирующий ЦВЗ большего объема, а в само медицинское изображение - небольшой защитный ЦВЗ. Метод позволяет: 1) совместно хранить медицинское изображение и сопровождающие данные, 2) обеспечить секретность данных, представляющих медицинскую тайну, 3) защитить медицинское изображение от подлога и преднамеренного изменения содержания.

Преимущество данного метода по сравнению с подобными заключается в следующем: 1) использование одного и того же алгоритма для встраивания двух ЦВЗ, имеющих различное предназначение; 2) возможность встраивания большого количества сопровождающих данных без значительного увеличения объема сохраняемой информации.

Два метода защиты содержания цифрового изображения на основе комбинированного ЦВЗ-алгоритма.

Первый метод применим в случаях, когда содержание одного из фрагментов изображения представляет особый интерес и должно быть доступно только ограниченному числу лиц и при этом изображение без данного фрагмента может быть опубликовано и также представляет интерес. Например, на фотографии, сделанной в момент преступления, таким, не подлежащим опубликованию, фрагментом может являться лицо свидетеля.

Предлагается «вырезать» из изображения фрагмент, представляющий особенный интерес, и встроить его по комбинированному алгоритму в исходное изображение, в котором место данного фрагмента заполнено шумом или другим изображением. Таким образом, можно обеспечить секретность особо ценной информации и ее совместное хранение с основным изображением.

Второй метод позволяет восстановить содержание изображения, на котором присутствуют несколько фрагментов, которые могут быть подвергнуты подделке. В такое изображение предлагается встраивать его копию по комбинированному алгоритму. Для этой цели наиболее пригодным является именно комбинированный алгоритм, который, как было уже показано, позволяет встраивать в изображение-контейнер ЦВЗ такого же объёма, обеспечивая при этом устойчивость процедуры встраивания.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ДИССЕРТАЦИОННОЙ РАБОТЫ

1. Разработан адаптивный линейный ЦВЗ-алгоритм защиты серотонного изображения при помощи встраивания серотонного ЦВЗ [1].
2. Предложена математическая модель и разработан аналитический метод исследования ошибок линейного алгоритма, возникающих вследствие встраивания и извлечения ЦВЗ-изображения, при воздействии атак [1].
3. Предложена концепция увеличения объема встраиваемых данных, обоснован и разработан соответствующий подход для комбинирования пространственных и частотных ЦВЗ-методов [2, 6].
4. Разработан, реализован и исследован комбинированный ЦВЗ-алгоритм с одновременным сокрытием в нем данных в объеме, значительно превышающем объем защищаемого изображения [2-4, 6-7].
5. Предложены варианты решения практических задач, связанных с защитой цветного изображения, обнаружения подделки изображения и др. с помощью применения разработанного комплекса [3, 5, 7].
6. Создан комплекс программ, реализующий предложенные линейный и комбинированный алгоритмы защиты изображения [1-7].

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Асатрян Д.Г., Шахвердян Г.С., Асатрян Н.С. Устойчивый цифровой алгоритм защиты изображения. Известия НАН РА и ГИУА. Серия ТН, Т.62, №1, сс. 69–75, 2009.

2. Asatryan D., Asatryan N. Combined Spatial and Frequency Domain Watermarking. Proc. of 7-th Int. Conf. on Computer Science and Information Technologies – CSIT'2009, Yerevan, pp. 323–326, 2009

3. Асатрян Н.С. Устойчивый алгоритм двойной защиты цифрового изображения. «Вестник РАУ» (физико-математические и естественные науки). Издательство РАУ. Ереван, сс. 26-33, 2009.

4. Асатрян Д.Г., Асатрян Н.С. Комбинированный ЦВЗ-алгоритм с улучшенными параметрами качества. Труды четвертой годичной научной конференции РАУ, Ереван, сс. 101-108, 2010.

5. Асатрян Д.Г., Асатрян Н.С. Совмещенный ЦВЗ-алгоритм для защиты и аннотирования изображения. Труды пятой годичной научной конференции РАУ, Ереван, сс. 143-151, 2010.

6. Asatryan D.G., Asatryan N.S. Combined Robust and High Payload Watermarking Algorithm. Proc. of 8-th Int. Conf. on Computer Science and Information Technologies - CSIT'2011, Yerevan, pp. 319-322, 2011.

7. Asatryan D., Asatryan N. Watermarking algorithm for medical images with large annotations. Proc. Of First Armenian International Congress on Telemedicine and eHealth «ARMTELEMED: Road to the Future», Yerevan, pp. 66–73, 2011.

Ասատրյան Ն.Ս.

ՄՈՒԼՏԻՄԵԴԻԱԿԱՆ ԻՆՖՈՐՄԱՑԻԱՅԻ ՊԱՇՏՊԱՆՈՒԹՅԱՆ ՀԱՄԱԿՑՎԱԾ ԱԼԳՈՐԻԹՄՆԵՐԻ ՄՇԱԿՈՒՄ

ԱՄՓՈՓՈՒՄ

Ատենախոսության **նպատակն է**՝ չարտոնված օգտագործումից պատկերի պաշտպանության և նրանում մեծածավալ տվյալների միաժամանակյա ներմուծման տարածա-հաճախականային համակցված ալգորիթմների, ինչպես նաև դրանց անալիտիկական և էքսպերիմենտալ հետազոտությունների մեթոդների մշակումը:

Թեմայի արդիականությունը: Գիտական գրականության վերլուծությունը ցույց է տալիս, որ չարտոնված օգտագործումից և բովանդակության չարամիտ փոփոխությունից թվայնացված պատկերների պաշտպանության բնագավառում կան դեռևս չլուծված խնդիրներ: Մասնավորապես, մշակված չեն շատ թե քիչ ունիվերսալ մեթոդներ, որոնք բավարարում են պաշտպանության գործընթացներին ներկայացվող հիմնական պահանջներին, միաժամանակ ապահովելով համեմատաբար մեծ ծավալի լրացուցիչ ինֆորմացիայի միաժամանակյա ներմուծումը պաշտպանվող օբյեկտի մեջ:

Ատենախոսությունը նվիրված է տարածական և սպեկտրալ տիրույթներում աշխատող ալգորիթմների և համակցված մեթոդների մշակմանը և դրանց հատկությունների հանգամանալից ուսումնասիրմանը:

Հետազոտության արդյունքների նորույթը: Մշակվել է գծային ադապտիվ ալգորիթմ, որը հնարավորություն է տալիս տարածական տիրույթում ներմուծել մի պատկերը մյուսի մեջ: Առաջարկվել է ներմուծվող ինֆորմացիայի ծավալի մեծացման գաղափարախոսություն՝ հիմնված ջրանշման տարածական և հաճախականային մեթոդների կարևորագույն հատկությունների օգտագործման վրա: Մշակվել, իրագործվել և փորձարկվել է համապատասխան ալգորիթմների և ծրագրերի համալիր: Առաջարկվել է մաթեմատիկական մոդել և ստացվել են անալիտիկական արտահայտություններ՝ հարձակումների առկայությամբ համակցված ալգորիթմով ջրանիշի ներմուծման և արտածման սխալների

հետազոտության համար: Էքսպերիմենտների օգնությամբ հետազոտվել է ջրանիշի ներմուծման սխալի կախվածությունը ներմուծման սխեմայից:

Հետազոտության արդյունքների կիրառական նշանակությունը: Մշակվել է համակցված ալգորիթմով ջրանշման հատուկ մեթոդաբանություն, որի շնորհիվ հնարավոր է դառնում պաշտպանվող պատկերում դրա ծավալը մի քանի անգամ գերազանցող ջրանիշի ներմուծումը՝ ջրանշման գործընթացի որակի նվազագույն կորուստներով: Ստեղծվել է ծրագրային համակարգ, որը թույլ է տալիս ոչ միայն ջրանշման եղանակով իրագործել պատկերի արդյունավետ պաշտպանություն, այլև այնտեղ միաժամանակ ներմուծել մեծ ծավալի լրացուցիչ ինֆորմացիա: Առաջարկված ալգորիթմները կիրառվել են բժշկական պատկերների պաշտպանության խնդիրներում: Ստեղծված մեթոդաբանությունը, ալգորիթմները և ծրագրերը ներդրվել են համալսարանի ուսուցման գործընթացներում:

Ատենախոսության հիմնական արդյունքները

1. Մշակվել է գորշագույն պատկերի ներմուծման միջոցով գորշագույն պատկերի պաշտպանության ադապտիվ գծային ջրանշման ալգորիթմ [1]:

2. Առաջարկվել է հարձակման պայմաններում ջրանիշի ներդրման և արտածման հետևանքով առաջացող սխալների հետազոտման մաթեմատիկական մոդել և մշակվել է անալիտիկ մեթոդ [1]:

3. Առաջարկվել է ներդրվող ինֆորմացիայի ծավալի ավելացման մտահղացում, հիմնավորվել և մշակվել է համապատասխան մոտեցում ջրանշման տարածական և հաճախականային մեթոդների համակցման համար [2, 6]:

4. Մշակվել, իրագործվել և հետազոտվել է ջրանշման համակցված ալգորիթմ, որն ապահովում է պաշտպանվող պատկերի ծավալը էապես գերազանցող տվյալների միաժամանակյա ներմուծումը [2-4, 6-7]:

5. Առաջարկվել են մշակված համալիրի կիրառմամբ գունավոր պատկերների պաշտպանության, պատկերի կեղծման և այլ կիրառական խնդիրների լուծման տարբերակներ [3, 5, 7]:

6. Ստեղծվել է առաջարկված գծային և համակցված ալգորիթմներն իրագործող ծրագրային համակարգ [1-7]:

Asatryan N.S.

DEVELOPING OF COMBINED ALGORITHMS FOR PROTECTION OF MULTIMEDIA INFORMATION

Abstract

The **aims** of thesis are development of combined spatial and frequency methods for protection of multimedia information from unauthorized using and simultaneously embedding to there the information of high volume, as well as the analytical and experimental investigation of that methods.

The actuality of the investigation. The analysis of scientific literature shows that there are some unsolved problems in the area of protection of images from unauthorized using and malicious changing of the content. Particularly, there are not yet developed the universal methods for the protection procedures which satisfy the basic requirements to the quality of procedure, and for simultaneously embedding the additional information of high volume into the protected object.

The thesis is devoted to the development and applications of methods which are working in the spatial and frequency domains and combined methods, as well as to the investigation of the properties of corresponding protection procedures.

Novelty of results. Linear adaptive algorithm which allows the embedding an image into another one in the space domain is proposed. Mathematical model is proposed, and analytical expressions are obtained for investigation of a watermark embedding and extracting errors of the linear and combined algorithms at presence of the attacks. A conception for increasing the volume of embedding information is proposed, an algorithm for combining of the spatial and spectrum methods is developed. Dependence of watermark embedding error on embedding scheme is investigated.

Practical significance of the investigation results. A special methodology of watermarking by using the combined watermarking

algorithm has developed, which allows the embedding of a watermark of size exceeding the size of the protecting image several times with minimal losses of the quality of the watermarking procedure. Software system which allows the effective protection of an image by using of the watermarking procedure and simultaneously embedding additional information of large volume has created. The proposed algorithms are applied for protection of medical images and in other problems as well. The created methodology, the algorithms and software system have introduced in the education processes of the university.

Main results of investigation

1. Adaptive linear watermarking algorithm for protection of a Gray Scale image by embedding to there a Gray Scale watermark image has developed [1].

2. Mathematical model and analytical expressions for investigation of a watermark embedding and extracting errors under attacks have proposed [1].

3. A conception for increasing the volume of embedding information has proposed, an approach for combining of the spatial and spectral methods substantiated and developed [2, 6].

4. A combined watermarking algorithm which provides the simultaneously embedding of a watermark exceeding the size of protecting image several times has developed and investigated [2-4, 6,7].

5. Versions of solutions of the problems for color image watermarking, detecting of an image forgery and some other problems by using the developed complex, have proposed [3, 5, 7].

6. Software system for protecting of an image by proposed linear and combined algorithms has created [1-7].