

ՀՀ ԳԱԱ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

Պետրոսյան Ալեքսանդր Հուսիկի

Ինքնաներդրման եղանակով պատկերի պաշտպանության և վերականգնման
ալգորիթմերի և ծրագրերի համալիրի մշակում

ՍԵՂՄԱԳԻՐ

Ե13.04 – «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի
մաթեմատիկական և ծրագրային ապահովում» մասնագիտությամբ տեխնիկական
գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության

Երևան – 2016

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ НАН РА

Петросян Александр Усикович

Разработка комплекса алгоритмов и программ, предназначенных для защиты
и восстановления изображений с использованием методов самовнедрения

АВТОРЕФЕРАТ

Диссертации на соискание ученой степени кандидата технических наук по специальности
05.13.04 – “Математическое и программное обеспечение вычислительных машин,
комплексов, систем и сетей”

Ереван – 2016

Ատենախոսության թեման հաստատվել է ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում

Գիտական դեկավար՝
ընդդիմախոսներ

տելս.գիտ. դոկտոր
ֆիզ.մաթ.գիտ. դոկտոր
ֆիզ.մաթ.գիտ. թեկնածու

Ղ.Գ.Ասատրյան
Մ. Ե. Հարությունյան
Հ.Ռ.Բոլիբեկյան

Առաջատար կազմակերպություն՝

Հայաստանի ազգային պոլիտեխնիկական
համասարան

Պաշտպանությունը կայանալու է 2016թ. հունիսի 12-ին, ժ. 15:00-ին ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող 037 «Ինֆորմատիկա և հաշվողական համակարգեր» մասնագիտական խորհրդի նիստում հետևյալ հասցով՝ Երևան, 0014, Պ. Սևակի 1:

Ատենախոսությանը կարելի է ծանոթանալ ինստիտուտի գրադարանում:

Սեղմագիրն առաքված է 2016թ. հունիսի 11-ին:

Մասնագիտական խորհրդի գիտական
քարտուղար, ֆիզ.մաթ.գիտ. դոկտոր



Հ. Գ. Մարտիսանյան

Тема диссертации утверждена в Институте проблем информатики и автоматизации НАН РА

Научный руководитель:

доктор тех. наук

Д. Г. Асатрян

Официальные оппоненты:

доктор физ.-мат. наук

М.Е.Арутюнян

кандидат физ.-мат. наук

Օ.Ր.Յոլիբեկյան

Ведущая организация:

Национальный политехнический университет
Армении

Защита состоится 12-го июля 2016г. в 15:00 часов на заседании специализированного совета 037 “Информатика и вычислительные системы” в Институте проблем информатики и автоматизации НАН РА по адресу: 0014, г. Ереван, ул. П. Севака 1.

С диссертацией можно ознакомиться в библиотеке ИПИА НАН РА.

Автореферат разослан 11 июня 2016г.

Ученый секретарь специализированного
совета, доктор физ. мат. наук



А. Г. Саруханян

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы

Проблема авторского права на изображения (например, авторское право на картину), а также необходимость проверки подлинности тех или иных визуальных данных являются актуальными с давних времен в различных аспектах жизнедеятельности людей. В частности, это может быть причастность некоторых лиц к каким-либо событиям, изображенным на фотографии, электронные подписи, подлинность документов, фактическая достоверность улик, изображенных на фотографии и т.д.

Ещё в середине XX века обработка изображений была по большей части аналоговой и выполнялась оптическими устройствами. Подобные оптические методы до сих пор важны, в таких областях как, например, голография. Тем не менее, с резким ростом производительности компьютеров, эти методы всё в большей мере вытеснялись методами цифровой обработки изображений. Методы цифровой обработки изображений обычно являются более точными, надёжными, гибкими и простыми в реализации, нежели аналоговые методы.

На данный момент существует множество методов представления визуальной информации в электронном формате, но, к сожалению, большинство из них не позволяет удостовериться в подлинности того или иного изображения (например, фотография может быть подвергнута искажениям, манипуляциям, что выявить часто крайне затруднительно, а то и не представляется возможным и во многом зависит от человеческого фактора).

Цифровые визуальные данные в большинстве своем представляются, кодируются и распространяются с помощью наиболее распространенных форматов их представления, таких как GIF, JPEG, PNG. Несмотря на значительные преимущества данных форматов кодирования дискретных изображений, недостаток данных форматов заключается в большой сложности нахождения искажений по сравнению с имеющимся оригиналом, что в большинстве случаев вообще не представляется возможным, тем более проблематична задача восстановления оригинала.

В настоящее время наиболее распространены методы встраивания дополнительной информации в исходное электронное изображение, такую информацию принято называть ЦВЗ (цифровой водяной знак). Имеется множество разнообразных алгоритмов встраивания ЦВЗ в изображение.

Настоящая диссертационная работа посвящена разработке комплекса алгоритмов и программ для защиты цифрового изображения с возможностью его восстановления.

В данной работе разработан один из усовершенствованных методов защиты и восстановления электронного изображения, основанный на внедрении в него определённого образа самого защищаемого изображения, закодированного новым

методом. Предложенный подход обеспечивает также повышенный уровень устойчивости процедуры защиты авторского права к различным типам преднамеренных и не преднамеренных атак. В соответствии с этим был предложен метод для хранения и внедрения ЦВЗ в изображении, в результате которого совмещаются методы сокращённого кодирования изображения и встраивания ЦВЗ.

Цель работы

Целью диссертационной работы является разработка комплекса алгоритмов и программных модулей, основанных на самовнедрении сжатого и закодированного изображения, обеспечивающих одновременно защиту авторского права и восстановления искаженного оригинала.

Для достижения поставленной цели были сформулированы и решены следующие задачи:

- Разработка методов защиты визуальной информации от несанкционированного доступа и искажения данных путем использования методов самовнедрения;
- разработка методов кодирования изображения с повышенной устойчивостью к атакам и искажениям;
- разработка алгоритмов и программных модулей восстановления исходника видеоизображения, основываясь на декомпиляции атакованного изображения.

Научная новизна

- разработаны методы обработки, хранения и передачи графических данных с использованием методов самовнедрения и кодирования электронного изображения;
- разработан усовершенствованный пространственно-частотный алгоритм защиты электронного изображения;
- разработан новый подход для кодирования и хранения изображений, основанный на обработке растровых данных изображения;
- предоставлена процедура оптимизации метода встраивания ЦВЗ в изображение, закодированного в использованном разработанном формате;
- разработаны методы для оптимизации полученных алгоритмов под многопоточные видеочипы типа GPGPU.

Практическая ценность

- Разработаны программные системы и модули для реализации перечисленных выше методов;
- программное обеспечение позволяет обрабатывать графические данные в реальном времени, тем самым реализуя возможность использования его в различных прикладных целях;

- применение алгоритма возможно для статических изображений, так и для динамических видеоданных;
- реализован механизм использования программного обеспечения в мобильных устройствах;
- разработан сетевой сервис обработки электронных изображений;
- реализована возможность использования графических чипов GPGPU с использованием технологии NVIDIA CUDA для производства вычислений описанных алгоритмов и методов.

На защиту выносятся:

- Методы защиты и восстановления изображений путем их самовнедрения в качестве ЦВЗ обеспечивающие сохранность данных и устойчивость к различным искажениям и атакам;
- алгоритмы, их программные реализации и экспериментальные результаты исследований в данном направлении;
- алгоритмы и программная реализация многопоточного кодирования учитывающие особенности использования возможностей графических видеочипов типа GPGPU;
- клиент-серверная технология конвертации при использовании мобильных систем.

Апробация работы

Материалы и положения диссертационной работы обсуждались во время семинаров ИПИА, а также на семинарах Российско-Армянского (Славянского) университета. Материалы докладывались на 9-ой международной конференции “Computer Sciences and Information Technologies” (CSIT-2013, г. Ереван, Армения), а также на Международной Научно-Практической конференции: «Проблемы и перспективы современной науки» 2016 (г. Москва).

Публикации

Основные результаты исследований отражены в 5 научных публикациях, список которых приведен в конце автореферата.

Внедрение результатов работы

Результаты работы внедрены в исследовательском отделе ООО «Армянские Программы».

Структура и объем работы

Диссертация состоит из введения, четырех глав, содержит 5 таблиц и 28 рисунков. В конце приведен список использованной литературы. Общий объем диссертации 103 страницы.

СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Введение содержит обоснование актуальности темы, сформулированы цели и основные задачи, а также научная новизна и практическая значимость работы, представлены основные положения, выносимые на защиту.

В первой главе приведен обзор научной литературы по теме диссертации, опубликованной преимущественно за последние годы, анализ состояния рассматриваемых задач. Рассмотрены актуальные методы кодирования данных в современных ИТ технологиях в том числе и визуальных данных. Представлены спецификации основных присутствующих форматов кодирования и представления данных, за основу взят один из наиболее распространенных алгоритмов кодирования – алгоритм Лемпеля — Зива — Велча¹ и его современные модификации, такие как LZMA. Рассмотрены также альтернативные наиболее известные и распространённые методы шифрования данных, таких как AES, DES (одобренные для шифрования особо секретной информации АНБ США). Рассматриваются возможности расчёта контрольных сумм типа MD5. Для каждого из методов проанализированы основные возможности и ограничения, рассчитаны показатели производительности и оптимальности использования в том или ином контексте.

Далее описаны методы расчёта алгоритмов на различных вычислительных чипах. Представлены различные схемы вычислений на многопоточных системах. В качестве наиболее подходящей такой системы рассмотрена система GPGPU от NVIDIA CUDA. Произведено тестирование, выделены критерии оптимальности и обосновано использование подобных систем в поставленных задачах.

Приведена историческая справка относительно состояния и развития систем защиты авторского права, основанных на ЦВЗ технологиях. Рассмотрены требования и критерии устойчивости ЦВЗ-алгоритмов и их основные области и приложения. Продемонстрированы преимущества пространственно-частотных алгоритмов, в результате показано, что такие методы позволяют существенно увеличить объём встраиваемой информации, при сохранении сравнительно высокого качества встраиваемой информации после извлечения.

¹ Welch, Terry (1984). "A Technique for High-Performance Data Compression". Computer 17 (6): pp. 8–19. doi:10.1109/MC.1984.1659158.

Во второй главе описаны детали комбинированных пространственно-частотных методов встраивания дополнительной информации, и построения соответствующей модели встраивания ЦВЗ в изображение. Разработан частотный алгоритм встраивания ЦВЗ в изображение, основанный на известном алгоритме линейного встраивания ЦВЗ.²

В качестве дискретного изображения рассматривается объект-матрица $A = \{a_i^j\}$, где $1 \leq i \leq M, 1 \leq j \leq N$ и каждое значение a_i^j есть натуральное число, удовлетворяющее условию $1 \leq a_i^j \leq h$, где h – некоторая постоянная (рассматриваются черно-белые, серотонные изображения, где $h=255$). Аналогичным образом предложенный алгоритм может быть рассмотрен и для цветных дискретных изображений, в которых каждое a_i^j – тройка чисел от 1 до 255, а h есть тройка (255,255,255)). Параметры M, N, h определяют структуру рассматриваемого дискретного изображения. Аналогично определяется изображение ЦВЗ для встраивания $W = \{w_{kl}\}$. Следует заметить, что в качестве матрицы ЦВЗ берется матрица, сходная с изображением, но не обязательно в точности та же самая, т.к. визуального сходства достаточно для нахождения искажений (в этом и заключается основная идеология методов самовнедрения). Для определения понятия сходства двух изображений, вводятся математически описываемые критерии расчёта среднеквадратического отклонения (MSE) и расчёта пикового отношения сигнала к шуму (PSNR) которые позволяют численно оценить насколько сходны два изображения. Допустим имеются два изображения, представляемые матрицами числовых значений $A = \{a_i^j\}$, где $1 \leq i \leq M, 1 \leq j \leq N$ и $A' = \{a_i'^j\}$, где $1 \leq i \leq M, 1 \leq j \leq N$, то значение PSNR будет выглядеть следующим образом:

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_{A,A'}}{MSE^2} \right) = 20 \cdot \log_{10} \left(\frac{MAX_{A,A'}^2}{\sqrt{MSE}} \right) \text{ дБ, где } MSE = \frac{1}{MN} \cdot \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} |a_i^j - a_i'^j|^2$$

MSE – среднеквадратическое отклонение, а $MAX_{A,A'}$ – динамический диапазон расхождения между значениями пикселей изображений A и A' .

Пусть $W = \{w_{kl}\}$ – матрица ЦВЗ для встраивания, сходная, с оригинальным изображением A , размерами $K \times L, k = 0,1, \dots, K-1, l = 0,1, \dots, L-1$. Рассматриваются K и L кратные M и N соответственно. Далее ЦВЗ делится на блоки размером $b \times b$ пикселей, где b может принимать значения 4,8 и 16, основываясь на размере изображения. В случае пространственно-частотный алгоритма встраивания ЦВЗ в изображение для каждого из выделенных блоков ЦВЗ рассчитывается матрица коэффициентов двумерного Дискретного Косинусного Преобразования (ДКП, DCT – Discrete Cosine Transform).

² D. Asatryan, N. Asatryan, A. Petrosyan, N. Lanina. Method for Detection of Image Tampering and Partial Recovery. // Proc. of 9th Int. Conf. on Computer Science and Information Technologies - CSIT'2013, pp. 177-180, Yerevan, September 2013.

Среди существующих разновидностей ДКП в мы будем использовать разновидность двумерного DST-II и соответствующее ему обратное преобразование DST-III:

Для ускорения расчетов подобного рода рассматривается также двумерное Быстрое Преобразование Фурье (БПФ, FFT). На вход преобразование получает значения с заданной вещественной частью, мнимая же часть содержит нулевые значения. В результате преобразования получаем матрицу мнимых чисел, размера $b \times b$ (по размеру величины блока разбиения ЦВЗ), в которой в действительной части в интервале $\left[(0,0), \left(b, \frac{b}{2} \right) \right]$ принимает значения равные значениям в интервале $\left[\left(0, \frac{b}{2} \right), (b, b) \right]$. Аналогично получаем значения в мнимой матрице с тем отличием, что значения в интервалах $\left[(0,0), \left(b, \frac{b}{2} \right) \right]$, $\left[\left(0, \frac{b}{2} \right), (b, b) \right]$ принимают значения равные по модулю. Для восстановления матрицы действительной составляющей, в каждом блоке записываются значения в интервале $\left[(0,0), \left(b, \frac{b}{2} \right) \right]$, а для восстановления матрицы с мнимыми коэффициентам записываются значения в интервале $\left[(0,0), \left(b, \frac{b}{2} \right) \right]$ и маска значений $(-1)^n$ отображающая первую половину значений матрицы на $\left[\left(0, \frac{b}{2} \right), (b, b) \right]$, длиной $\frac{b}{2} \cdot b$, по сути представляющую собой маску битовых значений. Например, если размер блока равен 8, то объём маски для блока будет занимать 32 бита = 4 байта. При размере изображения 1024 x 1024 размер маски при размере блока 8 без сжатия будет составлять не более 64 кб. В результате одного из преобразований ДКП или БПФ, получаем матрицу коэффициентов интенсивности спектра пикселей водяного знака.

Каждый блок представляется следующим видом $S = (S_i^j)$ $i, j = 0,1 \dots b - 1$
 $t \times t$ коэффициентов спектрального преобразования каждого блока сохраняются остальные игнорируются.

Оставшиеся коэффициенты каждого блока выписываются в сжатую матрицу коэффициентов спектрального представления ЦВЗ $S^{comp} = (S_{k'l'}^{comp})$ размером $K' \times L'$, где $(l' = 0,1 \dots L' - 1, k' = 0,1 \dots K' - 1)$

Целые числа из интервала $[0 \dots 255]$ присваиваются каждому элементу матрице S^{comp} по следующей формуле

$$s'_{k',l'} = \left[255 \cdot \frac{S_{k',l'}^{comp} - Min}{Max - Min} \right], \quad (1)$$

, где Max, Min соответственно максимальные и минимальные элементы матрицы S^{comp} . Полученную матрицу (1) обозначаем через SPW и называем интенсивностью спектрального шаблона водяного знака (Spectral Pattern Watermark).

Для встраивания ЦВЗ (SPW) в исходное изображение $A = \{a_i^j\}$ размером $M \times N$; $m = 0,1 \dots M - 1$; $n = 0,1 \dots N - 1$, изображение делится на $K' \times L'$ блоков A_ξ размером $(M/K') \times (N/L')$, где $\xi = 0,1 \dots (K' \times L') - 1$. Если K' и L' не множители M и N , то тогда матрица спектральных значений пикселей заполняется соответствующим количеством

нулей. Производится смешивание пикселей исходного изображения с преобразованным изображением водяного знака. В работе так же рассматривается вопрос соотношения качества водяного знака при декодировании, если вместо линейного взаимно однозначно соответствия пикселей используется некоторое правило Θ устанавливающее соответствие между пикселями исходного изображения и ЦВЗ. Соответствие устанавливается на нескольких этапах. Первый этап производит смешивание пикселей перед обработкой ЦВЗ. Второй этап производится после спектральной обработки ЦВЗ. Подобный подход двухэтапного смешивания показывает улучшенные показатели качества ЦВЗ после его восстановления. Такое смешивание также производится как для увеличения секретности. В работе рассматривается несколько различных правил Θ смешивания пикселей. Одним из таких правил является правило псевдослучайное правило.

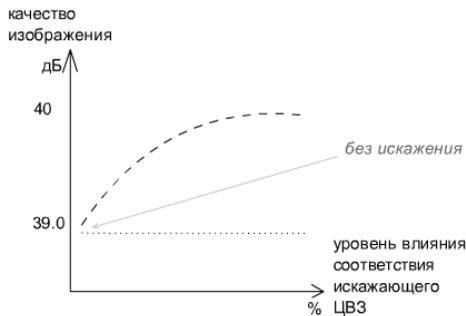


Рис.1 Показатель качества относительно мощности перемешивания пикселей

Псевдослучайное правило строится на основании некоторого ключа, описывающего данное псевдослучайное правило. Таким образом только в случае обладания ключом можно расшифровать информацию, закодированную в исходном изображении, что увеличивает безопасность встраиваемой информации. Необходимо использование достаточно больших значений в качестве ключа подобного рода для усложнения дальнейшего его несанкционированного декодирования методом примитивного перебора.

Допустим w'_ξ ξ -ый пиксель водяного знака SPW . Пусть w'_ξ встроен в блок $A_\xi = \{a_{m_\xi n_\xi}\}$. В данной главе рассматривается следующее правило встраивания ЦВЗ в изображение:

$$a_{m_\xi n_\xi}^{SPW} = (1 - \alpha)a_{m_\xi n_\xi} + \alpha w'_\xi$$

где $a_{m_\xi n_\xi}^{SPW}$ соответствующий пиксель изображения A^{SPW} в которое встраивается ЦВЗ. Значение α здесь достаточно малое действительное число лежащее в интервале $[0,1]$ и

представляющее собой мощность встраивания водяного знака в изображение. α едино для всех блоков встраиваемого изображения. При высоких значениях α оригинальное изображение сильно искажается в связи с этим используются сравнительно не большие значения α . В среднем подходящие значения лежат в отрезке $(0, \frac{1}{2})$.

При извлечении ЦВЗ имеем изображение со встроенным водяным знаком и возможно подвергнутое атаке. Обозначим матрицу описывающую такое изображение через $A^{spw\tau} = \{a_{ij}^{spw\tau}\}$, где τ – символизирует отображение-атаку на изображение.

Изображение $A^{spw\tau} = \{a_{ij}^{spw\tau}\}$ делится на блоки по количеству пикселей встроенного водяного знака. Обозначим среднюю интенсивность пикселей блоков изображения-контейнера, через $\{\mu_{\xi}\}$, где

$$\mu_{\xi} = \frac{KL}{MN} \sum_{m_{\xi}} \sum_{n_{\xi}} a_{m_{\xi}n_{\xi}}$$

Обозначим среднюю интенсивность пикселей ξ -ого блока атакованного изображения водяного знака через

$$\mu_{\xi}^{spwX} = \frac{KL}{MN} \sum_{m_{\xi}} \sum_{n_{\xi}} a_{m_{\xi}n_{\xi}}^{spwX}$$

Приближение элемента SPW с присутствующей атакующей составляющей τ вычисляется по следующей формуле

$$w_{\xi}^{\prime X} = \frac{\mu_{\xi}^{spwX} - (1 - \alpha)\mu_{\xi}}{\alpha}$$

приведенная формула получается методом наименьших квадратов.

Полученная информация трансформируется следующим образом:

$$S_{k'l'}^{comp} = w_{k'l'}^{\prime} \frac{(Max - Min)}{255} + Min$$

Матрица с полученными элементами $S_{k'l'}^{comp}$ делится на блоки размером $t \times t$, каждый блок заполняется необходимым количеством нулей до размера $b \times b$.

Каждый полученный блок размера $b \times b$ подвергается обратному спектральному преобразованию в зависимости от примененного преобразования.

Полученные данные комбинируются в матрицу и конвертируются в изображение исходного размера водяного знака.

После преобразований пиксели изображения подвергаются обратному смешивающему преобразованию в соответствии с алгоритмом смешивания примененным во время встраивания ЦВЗ.

Третья глава посвящена разработке нового формата кодирования изображений. Представленные в главе методы дают значительную возможность экономии объема информации преимущественно для таких изображений, в которых имеются однородные части.

Метод относительных отклонений (разностей). Как было указано выше, имеем матрицу изображения $\{a_i^j\}$, допустим начальный элемент матрицы a_0^0 лежит в левом верхнем углу матрицы, кодирование начинается именно с данного элемента. Для дальнейшего облегчения вычислений преобразуем матрицу $\{a_i^j\}$ к виду, в котором каждый элемент матрицы является четным числом, иными словами, каждый элемент матрицы заменяется самым близким меньшим четным числом. При таком преобразовании изменения в изображении не будут ощутимы человеческим глазом, что проверяется расчетом PSNR. Обозначим полученную матрицу через $\{b_i^j\}$. Для каждого b_i^j рассмотрим разность $c_i^j = (b_i^{j+1} - b_i^j)$. Каждый элемент b_i^j принимает значения в интервале $[-255, 255]$. Рассмотрим матрицу $\left\{\frac{c_i^j}{2}\right\}$, её значения будут лежать в интервале $[-127, 127]$, причем каждое $\frac{c_i^j}{2}$ будет целым числом, т.к. c_i^j – четное (в чем легко убедиться). Прибавим к каждому $\frac{c_i^j}{2}$ число 127, тем самым получим третью матрицу $\{e_i^j\}$, где $e_i^j = \left(\frac{c_i^j}{2} + 127\right)$ значения которой лежат в интервале $[0, 255]$. Для дальнейшего восстановления исходного изображения, кодируются все строки кроме последней, т.е. для $i \neq M$. Полученная матрица $\{e_i^j\}$ и есть закодированная матрица методом отклонений. Данным методом кодируются только отклонения (или разности), тем самым уменьшая численный разброс цветовой гаммы. Полученная информация сжимается в случае, если разброс не слишком велик. Например, перекодирование изображения, в котором чередуются строки со значениями 0 и 255, не имеет смысла, так как в закодированном виде оно не отличается от оригинала.

Однако такое изображение практически не встречается среди электронных фотографий, для наглядности далее приводится пример такого изображения (см. Рис.2.а стр.12):

Рассматривается кодирование методом отклонений по оси Y, но ничто не мешает кодировать разности и по оси X. Закодированное таким образом изображение примет следующий вид (см Рис.2.б).

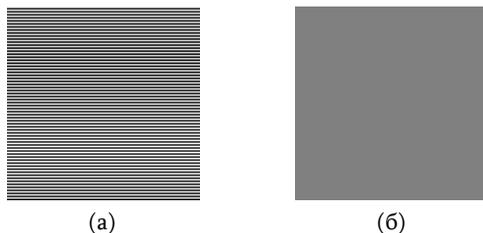


Рис.2 Числовые значения пикселей 255 и 0, где (а) оригинал (б) закодирован методом отклонений по оси Y

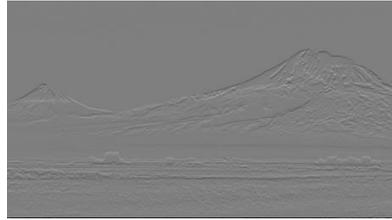
Таким образом получается небольшой прирост в экономии свободного места по сравнению с кодированием по оси Y, которое не меняет данное изображение.

Декодирование производится аналогичным методом. Для каждого элемента матрицы $\{e_i^j\}$ считается следующая сумма $a_i^j = e_{i+1}^j + (e_i^j - 127) * 2$ для каждого элемента начиная с $i = M - 1$ до $i = 0$. Таким образом, изображение возвращается к своему исходному виду.

Применим данный алгоритм к изображению – «Ararat».



(а)



(б)

Рис. 3. (а) «Ararat» оригинал (б) «Ararat» закодирован методом отклонений
изображение закодировано форматом gif размером в 83.1 KB

После применения алгоритма кодирования изображение будет выглядеть следующим образом (см. Рис. 3. (б))

Как видно из рис. 3. (б), новое изображение в основном представлено в средних тонах. Далее, если сохранить изображение в исходном формате gif, оно займет 53.5 KB тем самым обеспечивая сжатие в 35% относительно оригинала.

Применяя алгоритм декодирования возвращаем изображение к исходному виду:



Рис.4. «Ararat» после декодирования

В результате кодирования и декодирования получаем PSNR равное 51.13 дБ.

Рассмотрим следующий пример крупного изображения 2508x1254 с множеством деталей – «Ruins»³:

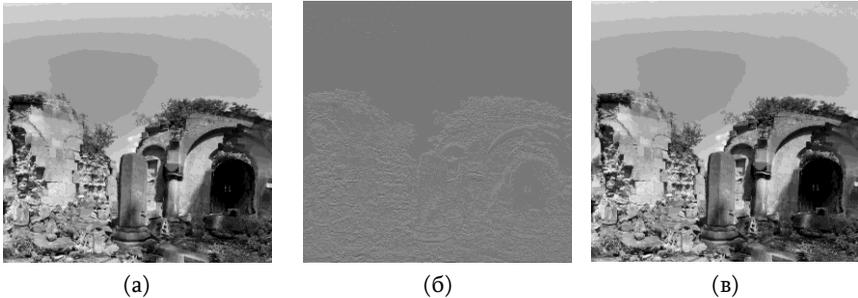


Рис. 5. «Ruins» (а) оригинал (б) закодирован методом разностей (в) после декодирования размер 496 KB

Размер полученного изображения 342 KB, тем самым мы сэкономили 31% места, занимаемого данным изображением. Заметим, что кодирование и декодирование производится без значительных потерь, ощутимых человеческим глазом.

После декодирования изображение примет следующий вид (см.Рис. 5 (в)).

При подсчете значений PSNR получаем численные значения равные 51.16дБ, из чего видно, что искажения не заметны для человеческого глаза.

Для достижения наилучшего результата сжатия метод разностей следует применять не для всего изображения в целом, а для фрагментов изображения, полученных путем последовательного разбиения изображения. Описание подобного алгоритма фрагментации представлено ниже.

Метод прямоугольных сеток. Основным объектом, входящим в способ кодирования изображения, является последовательность ординат $c_1 < c_2 < \dots < c_k$ таких, что $c_1 = 0, \dots, c_k = N_n$ для каждого i удовлетворяющего условию $1 \leq i \leq k - 1$, задается система $D_i = (d_{i1}, d_{i2}, \dots, d_{il})$, удовлетворяющая условиям $d_{i1} \leq d_{i2} < \dots < d_{il}$ $d_{i1} = 1, d_{il} = M$ (разумеется, при этом l зависит от i). В результате изображение разбивается на прямоугольники

$$G_{ij} = \{(x, y) | (c_i \leq y < c_{i+1}) \& (d_{ij} \leq x < d_{i,j+1})\}, \quad (1)$$

Где $1 \leq i < k$, и при каждом i в указанных пределах выполнено неравенство $1 \leq j < l$ (здесь l зависит от i).

Выбор параметров указанного разбиения должен осуществляться специальным алгоритмом, о котором пойдет речь ниже. Если параметры разбиения уже выбраны, то

³<https://plus.google.com/+RolandYeghiazaryan/photos/photo/5913759708537069538?pid=5913759708537069538&oid=108391226186149093445> (изображение используется с согласия автора)

выработка способа сокращенного кодирования изображения осуществляется на основании следующего подхода. (1) выделяются прямоугольники G_{ij} , в которых значения элементов матрицы, задающей изображение, либо совпадают (в одном из вариантов метода), либо отличаются друг от друга не более, чем на некоторую константу δ (в другом варианте метода).

Выбор одного из указанных вариантов метода, а так же выбор константы δ (в случае второго варианта) осуществляется специальным алгоритмом, идея которого основана на обнаружении фрагментов G_{ij} матрицы, задающей изображение, таких, где совокупность значений G_{ij} либо постоянная (в случае первого варианта метода), либо достаточно мало отличается от постоянной.

Возвращаясь к алгоритму выбора указанных выше параметров c_i и d_{ij} , отметим, прежде всего, что применение этого алгоритма основано на результатах работы другого алгоритма, при помощи которого выделяются участки заданного изображения, в которых значения элементов матрицы задающей изображение, либо совпадают (в случае первого варианта метода), либо отличаются друг от друга на некоторую достаточно малую константу δ (в случае второго варианта метода); при этом выбор константы δ зависит от подробностей избранного способа кодирования изображений.

Описание указанных участков изображения может производиться различными способами (например, эти участки могут кодироваться в виде многоугольников с рациональными вершинами). Далее описывается один из таких методов.

Применим немного видоизмененный алгоритм подсчета разностей, описанный выше (метод отклонений). Отличие будет заключаться в том, что при подсчете элементов $c_i^j = (b_i^{j+1} - b_i^j)$ будем брать модуль разности т.е.

$$c_i^j = |b_i^{j+1} - b_i^j|$$

Назовем полученные элементы переходным весом по оси Y для заданного j. Для каждого j в матрице $\{c_i^j\}$ посчитаем сумму

$$v_j = \sum_{i=1}^M c_i^j$$

Обозначим, через v^{max} максимальный элемент среди v_j , а через v^{min} минимальный. Обозначим, через $w_j = 255 * w_j * (w^{max} - w^{min})$. w_j представляет собой численное выражение в интервале $[0, 255]$, которое определяет собой мощность переходов по оси Y для заданного j. С помощью данных коэффициентов и будем производить разбиение $c_1 < c_2 < \dots < c_k$. Там где w_j достаточно велико деление нужно производить достаточно часто, там же где мало или близко к 0 деления вовсе не необходимы. Для наглядности рассмотрим пример такого разбиения для изображения «cameraman»:

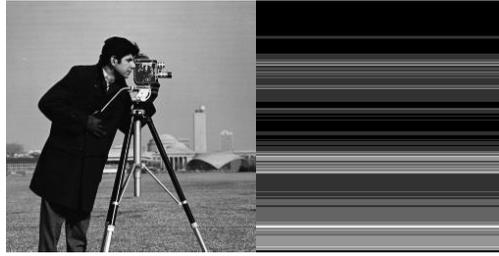


Рис.6. «CameraPan» и его переходной вес по оси Y

На рисунке справа демонстрируются значения w_j для каждого j , чем светлее оттенок тем больше переходов на данном участке и тем чаще нужно производить дробление.

После этого основной прямоугольник разбивается на два прямоугольника, расположенных соответственно выше и ниже прямой $y = c_i$. Дальнейшие действия производятся аналогичным образом для частей, на которые разбивается прямоугольник.

Построение параметров c_i продолжается до того, как их совокупность окажется в соответствии с условиями завершения построения системы значений c_i ; такие условия естественно выработать заранее с учетом взаимного расположения областей совпадения или приблизительного совпадения значений основной матрицы. Естественным образом строится система горизонтальных полос, достаточно хорошо аппроксимирующая систему областей совпадения значений основной матрицы. Указанная система горизонтальных полос основная информация для построения системы параметров c_i .

Если система параметров $c_1 < c_2 < \dots < c_k$ уже построена, то для каждого i , удовлетворяющего условию $1 \leq i < k$ строится система $d_{i1} < d_{i2} < \dots < d_{il}$ (где l зависит от i). Такая система строится таким же методом, каким строилась система параметров c_i . В результате получается разбиение основного прямоугольника на прямоугольники G_{ij} , где $1 \leq i < k$, и при каждом i таком, что $1 \leq i < k$ имеет место $1 \leq j < l_i$.

Если прямоугольники G_{ij} уже построены, то метод сокращенного кодирования основной матрицы выглядит следующим образом. Если прямоугольник G_{ij} не содержится в областях совпадения или приблизительного совпадения значений основной матрицы, то значения элементов основной матрицы, попавших в G_{ij} кодируются так же, как это делалось в основной матрице. Если значения элементов основной матрицы, попавших в G_{ij} , совпадают, то кодируется лишь общее значение указанных элементов (с соответствующими дополнительными указателями). Если же значения элементов основной матрицы, попавших в G_{ij} совпадают лишь приблизительно, то в случае первого варианта рассматриваемого метода значения элементов матрицы, попавших в такой прямоугольник G_{ij} кодируются так же, как это делается в общем случае; во втором варианте рассматриваемого метода кодируется среднее арифметическое значений матрицы, попавших в G_{ij} , и кроме того, для каждого значения

указанного вида кодируется его отклонение (в положительную или отрицательную сторону) от упомянутого среднего арифметического.

Может быть реализован метод сокращенного кодирования изображений, где роль рассматриваемых выше прямоугольников G_{ij} играют многоугольники с рациональными вершинами.

Еще раз подчеркнем, что описанный выше метод позволяет сократить объем кода не для всякого изображения. Однако опыт показывает, что для многих реальных цифровых фотографий и изображений сокращение объема кода изображения достигается представленным методом.

Реализован алгоритм фрагментации памяти для заполнения свободной памяти данными ЦВЗ вместо линейного алгоритма, описанного во второй главе.

Алгоритм встраивания ЦВЗ работает таким образом, что значения ЦВЗ распределяются равномерно в соответствии с алгоритмом фрагментации памяти.

В четвертой главе рассматриваются различные приложения описанных в первых трех главах методов.

Предварительно дается краткое описание программной системы, состоящей из модулей, реализованных на системах Visual C++, Visual Basic, NVIDIA CUDA SDK, Adobe Flash, Android SDK. Описывается комплекс системных модулей по обработке изображений и реализующий описанные в работе алгоритмы. Так же в системе присутствует множество механизмов обработки изображений, таких как размытие, добавление шума, возможность применения небольших микропрограмм попиксельной обработки, сохранение в различных форматах. В системе предусмотрена возможность визуализации изображений на каждом этапе экспериментов, что позволяет отслеживать их (и степень искажения) не только с использованием попиксельного сравнения с оригиналом, а вместе с тем такими методами расчета среднеквадратического отклонения и PSNR. Приводятся результаты экспериментов, в том числе на изображениях электронных подписей.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ДИССЕРТАЦИОННОЙ РАБОТЫ.

1. Разработаны методы и алгоритмы защиты и восстановления изображений путем их самовнедрения, обеспечивающие сохранность данных и устойчивость к различным искажениям [1].
2. Разработан метод кодирования цифровых изображений, обеспечивающий компактное представление графических изображений и дающий возможность самовнедрения изображения [3].
3. Реализована модель безопасности цифровых изображений, путем совмещения алгоритма сжатого кодирования некоторого класса изображений и

разработанного модифицированного комбинированного (пространственно-частотного) алгоритма самовнедрения изображения [2, 4].

4. Разработана программная система, реализующая модель безопасности цифровых изображений. Разработано программное обеспечение, позволяющее реализовывать описанные алгоритмы на графических процессорах, а также представлена реализация клиент-серверной технологии для мобильных устройств [1-5].

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

1. D. Asatryan, A. Petrosyan, N. Asatryan, N. Lanina. Method for Detection of Image Tampering and Partial Recovery. // Proc. of 9th Int. Conf. on Computer Science and Information Technologies - CSIT'2013, pp. 177-180, Yerevan, September 2013.
2. David Asatryan, Naira Asatryan, Natalya Lanina, Alexander Petrosyan // IEEE Conference Publications Method of detection of image tampering and partial recovery ISBN: 978-1-4799-2460-8 pp.1-6
3. А. Петросян. Метод кодирования дискретных изображений для сжатия и последующего встраивания ЦВЗ // Сборник статей ЦНС “Международные научные исследования” по материалам VII международной научно-практической конференции: «Проблемы и перспективы современной науки», N, Москва, 2016. ISSN 4684-1407 pp. 61-66
4. А. Петросян. Некоторые Методы Фрагментного Кодирования Дискретных Изображений. //Институт Проблем Информатики и Автоматизации НАН РА, Ереван, 2016. pp.1-15
5. А. Петросян. Кодирование Дискретных Изображений Методом Относительных Отклонений // «Единый всероссийский научный вестник», N6, Москва, 2016. ПИ № ФС77 – 63258

Պետրոսյան Ալեքսանդր Հուսիկի
Ինքնաներդրման եղանակով պատկերի պաշտպանության և վերականգնման
ալգորիթմների և ծրագրերի համալիրի մշակում

ԱՄՓՈՓՈՒՄ

Մույն ատենախոսությունը նվիրված է թվային պատկերների պաշտպանության ալգորիթմների և ծրագրերի համալիրի մշակմանը պատկերի հետագա վերականգնման հնարավորությամբ:

Աշխատանքում մշակված է էլեկտրոնային պատկերների պաշտպանության և վերականգնման բարելավված եղանակներից մեկը, որը հիմնված է պաշտպանվող պատկերի որոշակի նոր մեթոդով կոդավորված կերպարի ինքնաներդրման վրա: Ներկայացվող մոտեցումը ապահովում է նաև հեղինակային իրավունքի պաշտպանության ընթացակարգի կայունության ավելի բարձր մակարդակ տարբեր տեսակի կանխորոշված և չկանխորոշված պատկերի աղավաղման դեմ: Դրա հետ համահունչ առաջարկված է պատկերների մեջ Թվային Ջրանիշի (ԹՋՆ) պահպանման և ներդրման մեթոդ, որի արդյունքում համատեղվում են պատկերի սեղմված կոդավորման և ԹՋՆ-ի ներդրման մեթոդները:

Ատենախոսության նպատակն է՝ ալգորիթմների և ծրագրային մոդուլների համալիրի մշակումը, որոնք հիմնված են սեղմված և կոդավորված պատկերի ինքնաներդրման վրա, ինչը ապահովում է միաժամանակ և՛ հեղինակային իրավունքի պաշտպանումը, և՛ աղավաղված բնօրինակի վերականգնումը:

Աշխատանքի նորույթը.

- Մշակված են ինքնաներդրման միջոցով պատկերների պաշտպանման և վերականգնման մեթոդները և ալգորիթմները, որոնք ապահովում են տվյալների անվտանգությունը և տարբեր աղավաղումների դեմ կայունությունը:
- Մշակված է թվային պատկերների կոդավորման մեթոդ, որը հիմնված է պատկերի ռաստրային տվյալների մշակման վրա և ապահովում է տեսապատկերների կոմպակտ ներկայացումը և տալիս է պատկերի ինքնաներդրման հնարավորություն:
- Իրականացված է թվային պատկերների անվտանգության ապահովման մոդել՝ որոշ դասի պատկերների սեղմված կոդավորման և մշակված ձևափոխված կոմպիլացված (տարածքա-հաճախականային) ալգորիթմների համադրման միջոցով:
- Մշակված է նկարագրված ալգորիթմներն օգտագործող ծրագրային համակարգ, որն իրականացնում է թվային պատկերների անվտանգության առաջարկված մոդելը:

- Իրականացված է ծրագրային ապահովում, որը թույլ է տալիս նկարագրված ալգորիթմներն իրականացնել գրաֆիկական պրոցեսորների վրա, ինչպես նաև ներկայացված է կլիենտ-սերվերային տեխնոլոգիա շարժական սարքերի համար:

Աշխատանքի կիրառական արժեքը.

Մշակված ծրագրային ապահովումը թույլ է տալիս իրական ժամանակում մշակել գրաֆիկական տվյալները, ինչը հնարավորություն է տալիս օգտագործել այն կիրառական նպատակներով; ալգորիթմը հնարավոր է կիրառել ոչ միայն ստատիկ պատկերների, այլև դինամիկ տեսանյութերի համար; Ներկայացված ծրագրային ապահովման համար իրականացվել է շարժական սարքերում կիրառման մեխանիզմ; Մշակվել է էլեկտրոնային պատկերների մշակման ցանցային ծառայություն; Իրականացվել է հնարավորություն՝ օգտագործել GPGPU տեսաչիպերը ներկայացված ալգորիթմների հաշվարկման համար NVIDIA CUDA տեխնոլոգիայի օգնությամբ:

Աշխատանքի կառուցվածքը. Աշխատանքը բաղկացած է չորս գլուխներից, ներառությունից և հավելվածներից:

Առաջին գլխում ներկայացված են գիտական գրականության վերլուծությունը, գնահատված են պատկերների կոդավորման և պահպանման, ինչպես նաև պատկերների անվտանգությունը ապահովող առկա եղանակների առավելություններն ու թերությունները: Ներկայացված են նաև համակարգչային չիպերի վրա ալգորիթմների հաշվարկման եղանակների առանձնահատկությունները: Հիմնավորված է NVIDIA CUDA GPGPU համակարգի կիրառման առավելությունները: Վերլուծված են ԹՋՆ տեխնոլոգիաների կիրառման առանձնահատկությունները, նրանց արդյունավետության չափանիշները և առկա հիմնական թերությունները:

Երկրորդ գլխում ներկայացված են լրացուցիչ տեղեկատվության ներդրման կոմբինացված տարածքահաճախականային եղանակների էությունը և առավելությունները: Մշակված է ԹՋՆ-ի պատկերներում ներդրման հաճախականային ալգորիթմը, որը հիմնված է պատկերներում ԹՋՆ-ի գծային ներդրման վրա:

Երրորդ գլուխը նվիրված է պատկերների կոդավորման նոր ֆորմատի մշակմանը: Ներկայացրած են հարաբերական շեղումների եղանակի էությունը և ուղղանկյունների ցանցերի մեթոդը: Իրականացված է ԹՋՆ-ի տվյալներով ազատ հիշողության լրացնելու համար հիշողության ֆրագմենտավորման ալգորիթմ երկրորդ գլխում նկարագրված գծային ալգորիթմի ձևափոխումով: ԹՋՆ-ի ներդրման ալգորիթմն աշխատում է այնպես, որ ԹՋՆ-ի արժեքները հավասարաչափ են բաշխվում հիշողության ֆրագմենտավորմանը համապատասխան:

Չորրորդ գլխում ներկայացված առաջին երեք գլուխներում ներկայացրած ալգորիթմների կիրառությունները:

The Development of a Complex of Algorithms and Software for Protection and Recovery of Digital Image by Self-Embedding Technique

ABSTRACT

This dissertation is devoted to the development of a complex of algorithms and software for storing of digital image data with the ability to recover the image. In this dissertation one of the advanced methods of protection and restoration of the electronic image based on the embedding into a protected image the certain self-image, encoded by a new method is developed.

The proposed approach also provides an increased level of resistance to protect copyright procedures for different types of deliberate and unintentional attacks. In accordance with this, the method for the storage and embedding of digital watermark (DWM) in the image was proposed, resulting the method of reducing encoding of the image and the embedding of DWM are combined.

The aim of the dissertation is to develop a set of algorithms and software modules based on self-embedding of compressed and encoded image, at the same time ensuring the protection of copyright and restoring the distorted original.

Practical significance of the obtained results is as follows: the software allows you to process the image data in real time, thereby realizing the possibility of using it in a variety of applications; the application of the algorithm is possible for static images and dynamic video; the mechanism of using the software in mobile devices and the network service processing of electronic images are developed; the ability to use GPGPU graphics chips using NVIDIA CUDA technology for computing the product described algorithms and methods is implemented.

The novelty of the results of the dissertation is as follows:

The methods and algorithms of image protection and recovery by their self-embedding ensuring the data security and stability to various distortions are developed.

The method for encoding of digital images based on the processing of raster image data, providing a compact representation of the majority of graphical images enabling self-embedding of image, is developed.

The model of protection of digital images by combining the compressed encoding algorithm of some classes of images and developed a modified combination (space-frequency) algorithm of self-embedding of image is implemented.

The software system implementing the proposed model for the protection of digital images, which are used the described algorithms is developed.

The software allowing to implement the described algorithms on GPUs is developed, as well as the implementation of client-server technology for mobile systems is presented.

The dissertation consists of an introduction, four chapters, contains 5 tables and 28 figures and applications.

In the first chapter the analysis of the corresponding scientific literature as well as the estimation of the advantages and disadvantages of the available methods of the images coding, storing and protection are presented. The methods of algorithms calculation in different computing chips are described. The different computational schemes to multi-threaded systems are presented. As the most suitable GPGPU system of NVIDIA CUDA are considered. The testing, the developing of the optimality criteria and the justification of using of such systems in the task are produced. The requirements and criteria of sustainability of DWM-algorithms and the main areas of their applications are analyzed. The various performance metrics of such technologies are showed, their main limitations are identified.

In the second chapter the details and benefits of the combined spatial-frequency methods of installation of additional information in the image are analyzed, and the corresponding model of the DWM installation in the image is constructed. A frequency algorithm of DWM installation in the image based on an algorithm of linear embedding DWM is developed.

The third chapter is devoted to the development of a new format image coding. The method of relative deviations as well as the method of rectangular grids are developed. The memory fragmentation algorithm to fill the available memory with DWM data instead of linear algorithm described in the second chapter is implemented. DWM embedding algorithm operates such that DWM value uniformly distributed in accordance with the algorithm memory fragmentation.

In the fourth chapter the various applications of methods described in the first three chapters are discussed.