



.. равах рукописи

*М. Корытова*

**КОРЫТОВА Марина Валерьевна**

**ДИОФАНТОВЫ АЛГОРИТМЫ  
ПРИ ОБРАБОТКЕ И ПЕРЕДАЧЕ ВИДЕОДАНЫХ**

05 13 01 – системный анализ, управление и обработка информации  
(в научных исследованиях) по техническим наукам

**АВТОРЕФЕРАТ**  
диссертация на соискание ученой степени  
кандидата технических наук

Омск – 2007

Работа выполнена на кафедре информационной безопасности  
факультета компьютерных наук  
ГОУ ВПО «Омский государственный университет  
им Ф М Достоевского»

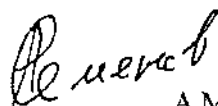
- Научный руководитель доктор технических наук,  
**Файзуллин Рашит Тагирович**
- Официальные оппоненты доктор технических наук, профессор  
**Волков Владимир Яковлевич**  
кандидат физ -мат наук доцент  
**Симанчев Руслан Юрьевич**
- Ведущая организация Институт математики и механики  
УрО РАН, Г Екатеринбург

Защита состоится 17 мая 2007 г в 14 45 на заседании диссертационного совета ДМ 212 179 03 при Омском государственном университете им Ф М Достоевского по адресу 644077, г Омск, ул Нефтезаводская, 11

С диссертацией можно ознакомиться в библиотеке Омского государственного университета им Ф М Достоевского

Автореферат разослан «12» апрель 2007 г

Ученый секретарь  
диссертационного совета  
кандидат физико-математических наук,  
доцент



А.М Семенов

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность работы.** С появлением и широким распространением вычислительной техники, а следом технологий создания и обработки графических изображений средствами вычислительной техники стали развиваться методы обработки информации, включающие в себя как вопросы эффективного представления видеoinформации в цифровом виде, так и вопросы преобразования информации

В отличие от носителей видеoinформации предыдущих поколений, таких как пленка, цифровое представление имеет целый ряд значительных преимуществ (не относящимся к вопросам создания и редактирования изображений), к которым относятся

- 1 Возможность многократного использования носителя
- 2 Уменьшение стоимости, с учетом возможности многократного использования
- 3 Упрощение технологий переноса информации на другие носители, например, бумагу
- 4 Упрощение технологии создания копий
- 5 Отсутствие ухудшения качества при копировании информации
- 6 Легкость и быстрота передачи информации по каналам связи

В том числе эти обстоятельства обусловили широкое распространение цифровых технологий представления видеоданных. Разработаны десятки возможных вариантов хранения информации, представленной в цифровом виде (например, такие форматы файлов BMP, GIF, JPEG, JPEG2000, PCX, PICT, Pixar, Raw, PNG, Scitex CT, Targa, TIFF), созданы многочисленные программные комплексы для формирования изображений, полученных на основании не визуальных данных или данных, созданных непосредственно пользователем, для визуализации естественных процессов, а так же для художественной обработки изображений

Представляется возможным, что анализ особенностей визуальной информации должен привести к построению методов преобразования и представления данных, использующих естественные ограничения, налагаемые цифровым представлением в ограниченной разрядной сетке. В дальнейшем эти методы можно применять, например, для управ-

ления уровнями качества информации и управления передачами по разделенным каналам связи. Вопрос подобного управления тесно связан с актуальной, практической проблемой защиты авторского права и проблемой более полного использования возможностей, предоставляемых глобальными сетями для регулирования доступа к информационным ресурсам.

**Целью работы** является построение методик преобразования и декомпозиции изображений, ориентированных на вариацию качества компонент цифровых изображений без потери при восстановлении. Построение этих методик основывается на рассмотрении цвета точек, из которых состоит изображение, как целых, неотрицательных, ограниченных сверху чисел, что позволяет применять методы теории диофантовых уравнений и неравенств для эффективного кодирования характеристик цифровых изображений и видеопотоков.

**Объект исследования – цифровое изображение.**

Цифровое изображение можно представить как матрицу пикселей. Пиксель – это единичный элемент изображения, который имеет фиксированную разрядность, например, для полутоновых изображений используют 8 бит, в этой работе рассматривается 24-битное представление.

Для определения значения цвета в цифровом изображении обычно используется кортеж из трех элементов. Распространено представление цвета в формате RGB, здесь в качестве базисных компонент составляющих цвета используется R – красная, G – зеленая и B – синяя. Сам же цвет представляет собой взвешенную сумму этих трех компонент, таким образом, в кортеже хранятся коэффициенты этой взвешенной суммы. Возможны и другие представления цвета, используемые как для хранения и отображения видеоданных, так и в процессе сжатия видеоданных, но в работе рассматривается именно описанное представление. Изображение состоит из «окрашенных» точек и, таким образом, описывается функцией, ставящей в соответствие каждому положению пикселя  $(u, v)$  в матрице значение цвета  $c(u, v)$ .

**Методы, применяемые в работе.** В работе применялись методы теории диофантовых уравнений и неравенств, методы декомпозиции, методы системного анализа данных и стеганографии

**Научная новизна работы:**

– разработана методика варьирования качества цифровых изображений, основанная на применении линейных диофантовых уравнений с двумя неизвестными,

– дано решение задачи ознакомления потенциального потребителя цифровых визуальных данных с информационным содержанием без представления высококачественного материала, но с возможностью его получения при наличии ключа,

– оценены искажения составляющих цвета точек в предоставляемых для ознакомления изображениях,

– показана нецелесообразность, в рамках данного подхода, использования нелинейных диофантовых уравнений и уравнений с числом неизвестных превышающих два

**Практическая значимость работы.** Предложенные в работе методы имеют практическую направленность на решение проблемы варьирования качества видеoinформации, представляемой в цифровом виде. Результаты работы используются в ЗАО «Зодиак» и в учебном процессе в Омском государственном университете им Ф.М. Достоевского

**Апробация результатов работы.** Основные результаты диссертационной работы докладывались и обсуждались на Сибирской научной школе-семинаре с международным участием «Компьютерная безопасность и криптография» (Иркутск, 2004), на Всероссийской научно-практической конференции-выставке «Единая образовательная информационная среда. Проблемы и пути развития» (Омск, 2004), на Конференции-конкурсе работ студентов, аспирантов и молодых ученых, работающих и/или обучающихся в Сибирском и Уральском регионах РФ «Технологии Microsoft в информатике и программировании» (Новосибирск, 2005), семинаре Омского филиала Института Математики им. С.Л. Соболева

**Публикации.** По теме диссертационной работы опубликовано 7 печатных работ

**Структура и объем диссертационной работы.** Работа состоит из введения, трех глав, общих выводов, списка использованных источников, включающего 87 наименований, и трех приложений. Основная часть диссертации изложена на 100 страницах машинописного текста, в число которых входят 2 таблицы 37 рисунков. Приложения занимают 28 страниц

## **КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ**

*Во введении* обосновывается актуальность темы диссертационной работы, сформулирована цель исследования, отмечена научная новизна и практическая значимость, приведены сведения об апробации результатов работы

*В первой главе* представлен обзор разработанных методов, направленных на преобразование информации представленной в цифровом виде, с целью ограничения доступа к передаваемым или хранимым данным, дана постановка задачи защиты качества видеоданных, а также рассмотрены вопросы теории диофантовых уравнений, используемых как теоретическая база основных методов, предлагаемых в работе

В п 1.1 представлен обзор разработанных и широко применяемых в настоящее время методов криптографической и стеганографической защиты данных. Криптографические методы к настоящему моменту являются хорошо исследованными и могут гарантировать, что передаваемую зашифрованную информацию может получить только законный пользователь, предварительно расшифровав. Основным недостатком этих методов является тот факт, что сторонний наблюдатель может легко понять, что передается зашифрованная информация, что само по себе может быть нежелательно. Стеганографические методы направлены на сокрытие самого факта существования скрытого канала связи, при этом передаваемая информация вкладывается в невинно выглядящие файлы, обычно с мультимедийными данными

Оба эти подхода направлены главным образом на защиту информационного содержания, так, чтобы противник не мог прочитать ни

одного бита скрываемой информации в случае криптографической защиты и доказать наличие вложения скрытой информации в случае стеганографической защиты

В п 1 2 дается постановка задачи варьирования качества видео данных, то есть предоставления пользователю информации в ознакомительном виде с возможностью последующего восстановления исходного качества при наличии некоторого секрета

В п 1 3 указаны используемые в работе принципы, любое изображение – это, прежде всего цвет, представляется интересным использовать этот факт для преобразования видео данных Рассмотрены применяемые в работе элементы теории диофантовых уравнений

*Во второй главе* представлено описание методов варьирования качества видео данных предлагаемых в работе Произведено теоретическое и практическое исследование указанных методов

В п 2 1 рассматривается метод «сложения» изображений, который из двух исходных изображений формирует одно новое

Используется следующее преобразование

$$\begin{cases} z_1 = \beta x + \alpha y, \\ z_2 = \alpha x - \beta y, \\ z = z_1 + z_2, \end{cases} \quad \alpha, \beta \in \mathbb{N} \quad (1)$$

Пусть рассматриваются два 24 битовых изображения в формате RGB Каждая точка – это комбинация трех основных цветов – красного, зеленого и синего, которые занимают каждый по 1 байту, следовательно, 3 на точку Преобразование (1) применяется по отдельности к составляющим цвета точки, считается, что значение  $x$  отвечает первому изображению, а  $y$  второму Таким образом, для каждой пары точек получается три результата для красной, зеленой и синей составляющей цвета При определенных ограничениях на  $\alpha$  и  $\beta$  полученные числа можно интерпретировать, как составляющие цвета двух новых точек, выбрав для представления первой точки первую половину записи числа  $z$ , а для второй вторую половину записи  $z$  (имеется в виду запись числа в некоторой системе счисления) Затем из этих то-

чек составляется новое изображение, оно содержит информацию об исходных данных, это изображение называется «сумма»

Поясним на примере Пусть имеются две точки изображения, кодированные кортежами  $(255,0,50)$ ,  $(100,250,20)$ , в качестве параметров преобразования выбраны значения  $\alpha = 100$ ,  $\beta = 10$  После применения преобразование для «красной» составляющей, то есть для чисел 255 и 100, получится значение  $z = 37050$  В шестнадцатеричной системе это 90BA, далее разделив  $z$  на две части, 90 и BA, и, таким образом, для красной составляющей двух новых точек получаются следующие значения 144 и 186 Аналогично вычисляются значения для синей и зеленой составляющих цвета точки В итоге получаются две новые точки  $(144,87,28)$  и  $(186,228,132)$

Для того чтобы получаемое число  $z$  можно было интерпретировать как число, определяющее составляющие цвета двух новых точек, необходимо выполнение условий  $\alpha > \beta$  и  $\alpha \leq 127$

На этапе восстановления необходимо решать систему диофантовых уравнений и неравенств относительно  $x$  и  $y$

$$\begin{cases} (\alpha + \beta)x + (\alpha - \beta)y = z, \\ 0 \leq x \leq 255, \\ 0 \leq y \leq 255, \end{cases} \quad (2)$$

где  $\alpha$ ,  $\beta$  и  $z$  – заданные числа

Для минимизации числа возможных решений системы (2) на параметры  $\alpha$  и  $\beta$  накладываются следующие ограничения  $\alpha + \beta > 127$ ,  $2\beta$  и  $\alpha + \beta$  взаимно простые числа При приведенных ограничениях даже в худшем случае надо будет выбирать всего из двух вариантов При этом одно из двух возможных решений  $x$  будет обязательно четное, другое нечетное, то же самое можно сказать относительно  $y$  Для однозначности выбора можно передавать дополнительную информацию о четности  $x$  Ниже приведен пример, иллюстрирующий представленный алгоритм Рассматриваются следующие два изображения Рис 1 и Рис 2





Рис. 1

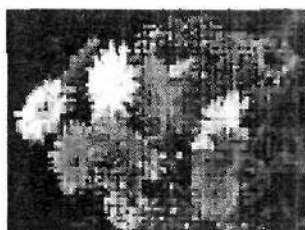


Рис. 2

Параметры преобразования выбраны следующими  $\alpha = 110$ ,  $\beta = 71$ . В результате преобразования получается изображение – «сумма», приведенное на Рис. 3.



Рис. 3

После восстановления получают исходные изображения.

Таким образом, получен алгоритм для преобразования изображений, где числа  $\alpha$  и  $\beta$  являются ключом.

Если над «суммой» изображений провести специальное преобразование – сжатие, при котором оставляются только точки соответствующие старшим разрядам числа  $z$ , то первое изображение может быть получено с нарушением цветовой передачи. Для изображения на Рис. 3 результат представлен на Рис. 4.



Рис. 4

Для оценки насколько получаемое таким образом изображение отличается от исходного первого, в зависимости от параметров  $\alpha$  и  $\beta$ , используется взятая по модулю разность между соответствующими составляющими цвета первого и полученного в результате сжатия изображения, называется этот параметр отклонением

Для всех допустимых параметров преобразования минимальное по всем возможным значениям составляющих цвета точки отклонение равно 0. Максимальное по всем возможным значениям составляющих цвета точки отклонение меняется от 3 для  $\alpha = 127$  и  $\beta = 126$  до 128 для  $\alpha = 127$  и  $\beta = 1$ . Если рассмотреть усредненное отклонение по всем возможным значениям составляющих цвета точки, то это число меняется от 1,476834 для  $\alpha = 127$  и  $\beta = 126$  до 62,519305 для  $\alpha = 65$  и  $\beta = 64$ .

Таким образом, пользователю можно предоставлять изображение «сумму», по которому можно ознакомиться с информационным содержанием исходных данных, при этом будут искажения в цветовом представлении, степень этих искажений определяется параметрами  $\alpha$  и  $\beta$ .

Предложенный метод может также быть использован для построения алгоритма шифрования статических изображений. Основная идея состоит в следующем, исходное изображение разбивается на равные части, число которых должно быть  $2^n$ , где  $n \in \mathbb{N}$ . Далее полученные части рассматриваются парами, и к каждой паре применяется предложенный метод. Получиться  $2^{n-1}$  изображений, число точек в которых в два раза больше, чем в исходных частях. Далее уже полученные изображения – результаты разбиваются на пары, и снова применяется метод и так далее пока не получится одно изображение.

Описанный метод можно применять к кортежу, сформированному из составляющих цвета точек, то есть, к числу, определяющему цвет точки или фрагмента изображения. Рассмотрим пример, возьмем точку (100,250,20) или, в 16-ричной системе счисления это (64, FA, 14), при этом получается значение для  $x$  равное 64FA14 или в десятичной сис-

теме счисления 6617620 Аналогично можно получить значения  $x$  и для фрагмента изображения, составленного из нескольких точек При переходе к фрагментам изображения, будет меняться только ограничение сверху на параметр  $\alpha$  За счет этого получается существенное увеличение числа возможных значений параметров  $\alpha$  и  $\beta$ , то есть увеличивается длина ключа, а также уменьшается количество дополнительной информации необходимой для точного восстановления исходных изображений

В работе также рассмотрен вопрос применения метода к большому числу изображений, так для случая с тремя изображениями необходимо исследовать систему

$$\begin{cases} v_1 = \alpha x + \beta y - \gamma z, \\ v_2 = -\alpha y + \beta z - \gamma x, \\ v_3 = \alpha z - \beta x + \gamma y, \\ v = v_1 + v_2 + v_3, \end{cases} \quad \alpha, \beta, \gamma \in \mathbb{N} \quad (3)$$

На этапе восстановления необходимо решать линейное уравнение с тремя неизвестными при этом невозможно обеспечить единственность решения без передачи значения для одной из составляющих цвета, например  $z$

В работе исследована возможность построения метода преобразования, в основе которого лежит уравнение, степень которого больше чем 1 Для этого рассмотрено преобразование второй степени  $ax^2 + bx + c + dy^2 + ey = f$  с целочисленными коэффициентами Показано, что если коэффициенты  $a$  и  $d$  разных знаков, то возможный диапазон значений  $f$  будет больше допустимого для сохранения результата в новом изображении Если  $a$  и  $d$  одного знака, то есть принимают только положительные значения, получается, что на этапе восстановления нельзя гарантировать однозначность решения В случае существования одного целочисленного решения для большинства значений  $f$  можно гарантировать существование еще нескольких целочисленных решений в допустимом диапазоне Если один из параметров  $a$  или  $d$  равен нулю, так же получается неоднозначность решения

Далее рассматривается общий случай преобразования второй степени

$$ax^2 + bx + c + dy^2 + ey + kxy = f$$

При помощи стандартной замены переменных, которая реализует поворот кривой второго порядка в системе координат можно легко получить ограничения на параметры и показать неоднозначность решения

В п 2.2 представлен метод «разделения» изображений, в котором из одного исходного изображения формируются два новых, по одному из них возможно определить информационное содержание исходного изображения

Метод состоит в следующем

- 1 Изображение разделяется на пары соседних по горизонтали точек
- 2 Для каждой точки определяется составляющие цвета
- 3 Из двух соответствующих составляющих цвета двух соседних выбранных точек, обозначим их  $c_1$  и  $c_2$ , составляется число  $z$ . Для этого числа  $c_1$  и  $c_2$  записываются в шестнадцатеричной системе счисления, затем составляется число  $c_1c_2$ . Для примера, пусть красные составляющие цвета двух соседних точек 100 и 200, в шестнадцатеричной системе счисления это 64 и C8, таким образом,  $z = 64C8$  или обратно в десятичной системе счисления 25800
- 4 Рассматриваются решения в целых числах следующего уравнения

$$z = ax + by, \quad (4)$$

где  $a$  и  $b$  – заданные целые положительные числа. Полученные решения  $(x, y)$  будут определять значения для двух соответствующих составляющих цвета точек в двух новых получаемых изображениях

- 5 Для получения исходного изображения достаточно вычислить число  $z = ax + by$ . Затем рассмотреть полученное число как 16-битное, где первые 8 бит – это значение соответствующей составляющей цвета первой точки, а последние 8 бит – второй точки

Необходимо выяснить ограничения на  $a$  и  $b$ . Без ограничения общности, будем считать, что  $a > b$ . Заметим, что при этом  $b$  – определяет точность восстановления  $z$  по  $x$  и  $y$ . Очевидно, что невозможно получить значение для  $ax + by$  большее  $\theta$ , но меньше  $b$ . Далее, пусть  $b$  – выбрано, необходимо, что бы выбор  $a$  обеспечивал получение всех возможных значений  $z$ , получаем  $a \geq 257 - b$

Перепишем (4) в виде

$$y = \frac{z}{b} - \frac{a}{b}x \quad (5)$$

Учитывая ограничения  $0 \leq x \leq 255$  и  $0 \leq y \leq 255$  можно предположить, что при больших значениях параметра  $a$  невозможно разрешить полученную систему в целых числах. При условии  $\frac{a}{b} \leq 255$  точное решение возможно будет отсутствовать только для тех точек, для которых выполняется  $z < 255b$

Для выбора приближенных значений  $x$  и  $y$  в случае отсутствия точного решения предлагается использовать следующий подход. Обозначим  $z_1$  – составляющая цвета получаемая в результате восстановления для первой точки и  $z_2$  – для второй точки,  $c_1$  – исходная составляющая цвета первой точки и  $c_2$  – второй точки. Выбираются  $x = x'$  и  $y = y'$ , для которых при любых  $x''$  и  $y'' \in Z$ ,  $x', y', x'', y'' \in [0, 255]$  выполняется,

$$|z'_1 - c_1| + |z'_2 - c_2| \leq |z''_1 - c_1| + |z''_2 - c_2|$$

При этом искажение в восстановленном изображении для составляющих цвета не превышает  $\left\lceil \frac{b+1}{2} \right\rceil$ , где  $[t]$  означает целую часть числа  $t$ . При малых значениях  $b$  это остается незаметным для наблюдателя.

Пример. Исходное изображение представлено на Рис. 5



Рис. 5.

Параметры выбраны  $b = 7$ ,  $a = 250$ . При этом получаются следующие два изображения Рис. 6 и Рис. 7.



Рис. 6.

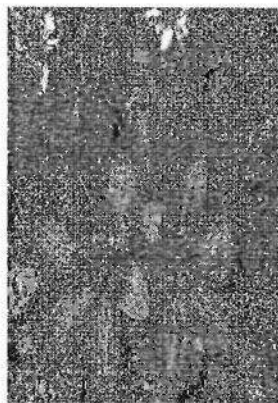


Рис. 7.

После обратной операции получается восстановленное изображение, визуально идентичное исходному, представленному на Рис. 5.

Обращают на себя внимание следующие особенности метода. Изображение, составленное из полученных значений  $x$  визуально схоже с исходным изображением сжатом в горизонтальном направлении в 2 раза, это объясняется значением параметра  $a$ . Около 5% точек в восстановленном изображении отличаются от исходных, что объясняется значением параметра  $b$ .

Для оценки, насколько изображение, составленное из полученных значений  $x$ , отличается от исходного изображения в зависимости от параметров  $a$  и  $b$ , используется взятая по модулю разность между составляющими цвета полученного первого изображения и соответствующими составляющими цвета исходного изображения называется этот параметр отклонение. Для всех допустимых параметров преобразования минимальное по всем возможным значениям составляющих цвета точки отклонение равно 0. Для иллюстрации максимального отклонения по всем возможным значениям составляющих цвета точки и среднего отклонения, используется тот факт, что на значения параметра  $b$  существуют сильные ограничения, вызванные требованием визуальной схожести исходного и получаемого после восстановления изображения. Рассмотрим частный случай  $b = 7$ . Тогда максимального отклонение меняется от 6 для  $a = 250$  до 128 для  $a = 1785$ . Если рассмотреть усредненное отклонение по всем возможным значениям составляющих цвета точки, то это число меняется от 2,105347 для  $a = 250$  до 109,718903 для  $a = 1785$ .

Рассмотренный метод можно применять и к большим фрагментам данных, но при этом надо определять новые ограничения на параметры  $a$  и  $b$ , так если применять метод для 24-битовых чисел, определяющих цвет точки, то получится следующее ограничение на параметры  $a \geq 16777217 - b$ .

При поиске значений  $x$  и  $y$  в случае, когда точное решение уравнения, удовлетворяющее соответствующим ограничениям найти невозможно, надо учитывать особенности человеческого зрения, а именно, невозможность заметить изменения в наименее значащих битах в каждой из трех составляющих цвета, таким образом, надо искать такие значения  $x$  и  $y$ , при подстановке которых в выражение

$$z' = ax + by,$$

полученное число  $z'$  будет минимизировать сумму модулей разностей между числами, полученными при разбиении  $z'$  и  $z$  на соответствующие составляющие цвета.

*В третьей главе* описаны особенности применения методов «сложения» и «разделения» изображений, включая дальнейшее расширение возможностей использования рассматриваемых алгоритмов

В п 3 1 дается, основанный на теории диофантовых уравнений подход, обеспечивающий минимизацию времени работы алгоритмов

В п 3 2 предлагается применение методов «сложения» и «разделения» изображений для варьирования качества видео-последовательностей, представленных в форматах без сжатия

Для построения алгоритма передачи можно использовать как метод «сложения» так и метод «разделения» изображений, при этом предлагается применять метод к каждому кадру видеопоследовательности

Метод «сложения» можно применять к двум последовательным кадрам, тогда пользователь может просматривать полученный видеопоток с измененной цветовой составляющей и с уменьшенной в два раза частотой кадров

Учитывая тот факт, что в методе «сложения» требуется передача дополнительной информации, а также, что в методе «разделения» этап восстановления является вычислительно более простым и может проходить в режиме реального времени, применение второго подхода выглядит более перспективным

Применяя метод «разделения» можно сохранять получаемые точки в одном итоговом изображении, при этом предоставляемая потребителю информация будет выглядеть как сильно зашумленные исходные кадры. Если пользователь информации пожелает просматривать видео с высоким исходным качеством, то ему предоставляется ключ, и он в режиме реального времени просматривает восстановленные данные

В п 3 3 представлено, как можно увеличить длину ключа в основных методах «сложения» и «разделения» изображений. Возможно применение нескольких подходов: менять ключ после обработки нескольких элементов, перераспределять по ключу получаемые результаты

В п 3 4 рассматривается, как получаемые зашумленные изображения могут быть использованы в целях организации стеганографического канала



Как в методе «сложения» изображений так и в методе «разделения» изображений, при передаче защищенных изображений по открытым каналам связи, части изображений для случайного наблюдателя будут выглядеть как шум. В первом методе – это точки, цвет которых получен из составляющих цветов второй части искомого числа  $z$ . Во втором – точки, цвет которых составлен из значений числа  $y$ . Этот факт легко использовать для организации стегаканала. Можно использовать метод разнесение точек скрываемого изображения по выглядящим как шум точкам передаваемого по открытым каналам связи изображения, например, как описано в [1].

### **ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ**

1. Построены диофантовы алгоритмы, обеспечивающие варьирование качества изображений и позволяющие пользователям получать информацию о содержании изображений, причем качество предоставляемой для ознакомления информации определяется параметрами преобразования. Используется тот факт, что в цифровом изображении цвет определяется как целое неотрицательное ограниченное сверху число и применяется теория линейных диофантовых уравнений с двумя неизвестными.
2. Исследованы возможности применения полученных методик к составляющим цвета одного пикселя, а так же к фрагментам изображений.
3. Доказана невозможность построения метода соединяющего изображения на основе диофантового уравнения степени выше первой, а также показана нецелесообразность, в рамках данного подхода, использования уравнения более чем с двумя неизвестными.
4. Показано, что получаемые изображения могут быть использованы в качестве контейнеров, обеспечивающих надежную передачу информации в стеганографических приложениях.
5. Построена система передачи видеопотока, в которой этап восстановления проходит в режиме реального времени.

### **Работы автора по теме диссертации**

- 1 Корятова, М В Крипто-стеганографический алгоритм на основе применения тригонометрических рядов с неубывающими коэффициентами / М В Корятова, Р Т Файзуллин // Известия Челябинского научного центра – 2003 – № 3 – С 1–5
- 2 Корятова, М В Применение систем диофантовых уравнений и неравенств для преобразования, передачи и защиты изображений / М В Корятова, Р Т Файзуллин // Вестник Томского государственного университета – 2004 – № 9(1) – С 65–68
- 3 Корятова, М В Защита изображений на основе решения систем диофантовых уравнений и неравенств / М В Корятова, Р Т Файзуллин // Материалы конф «Единая образовательная информационная среда проблемы и пути развития» Омск, 14–17 сентября 2004 – Омск, 2004 – С 310–312
- 4 Корятова, М В Защита графической информации с последующим контролем качества восстанавливаемых изображений / М В Корятова // Материалы конференции- конкурса «Технологии Microsoft в информатике и программировании» Новосибирск, 22–24 февраля 2005 – Новосибирск, 2005 – С 75–77
- 5 Корятова, М В Решение задачи защиты изображений на основе применения систем диофантовых уравнений и неравенств / М В Корятова, Р Т Файзуллин // Материалы конференции «Научная сессия МИФИ–2005 XII Всероссийская научная конференция «Проблемы информационной безопасности в системе высшей школы» Москва, 27 января 2005 – М, 2005 – С 113–114
- 6 Корятова, М В Использование особенностей формата представления цвета для ограничения возможностей использования информации, предоставляемой для ознакомления / М В Корятова // Информационные технологии моделирования и управления – 2006 – № 4 – С 453–457
- 7 Корятова, М В Организация ограничения доступа к видеоданным с высоким качеством, при возможности ознакомления с информационным содержанием / М В Корятова // Системы управления и информационные технологии – 2006 – № 4 1(26) – С 157–160

КОРЫТОВА Марина Валерьевна

ДИОФАНТОВЫ АЛГОРИТМЫ  
ПРИ ОБРАБОТКЕ И ПЕРЕДАЧЕ ВИДЕОДАНЫХ

05 13 01 – системный анализ, управление и обработка информации  
(в научных исследованиях) по техническим наукам

АВТОРЕФЕРАТ  
диссертация на соискание ученой степени  
кандидата технических наук

---

Подписано к печати 09 04 2007 Формат бумаги 60x84 1/16  
Печ л 1,5 Уч -изд л 1,5 Тираж 110 экз Заказ 73

---

*Издательство ОмГУ  
644077, г Омск-77, пр Мира, 55а, госуниверситет*