УДК 519.6:519.633.9

Способы передачи QR-кода в компьютерной стеганографии

Сергей ВАКУЛЕНКО
Sergey P. VAKULENKO

Наталья ВОЛОСОВА
Natalya K. VOLOSOVA

Дмитрий ПАСТУХОВ
Dmitry F. PASTUKHOV

Вакуленко Сергей Петрович *– кандидат технических наук, профессор, директор Института управления и информационных технологий Российского университета транспорта (МИИТ), Москва, Россия.*
Волосова Наталья Константиновна *– студентка магистратуры МГТУ имени Н. Э. Баумана, Москва, Россия.*
Пастухов Дмитрий Феликсович *– кандидат физико-математических наук, доцент кафедры технологий программирования Полоцкого государственного университета, Новополоцк, Беларусь.*

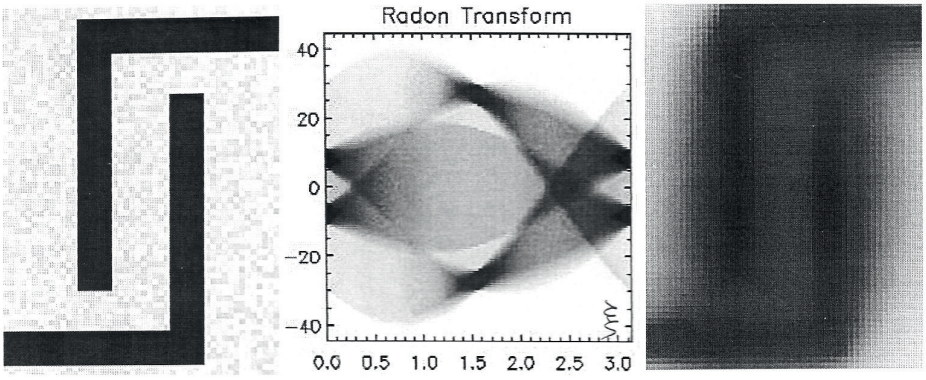
Methods of QR code Transmission in Computer Steganography
(текст статьи на англ. яз. – English text of the article – p. 21)

Предложено передавать данные, закодированные в QR-код, предварительно маскируя его. В частности, для надёжности восстановления «оригинала» решать одну и ту же задачу разными методами посредством итерации с помощью линейных систем, преобразования Радона, краевой задачи для уравнения Пуассона, а помимо этого и методами, основанными на теории вероятностей. К преимуществам такого варианта относится возможность применения современных компьютерных средств и программного обеспечения, наработанного в области различных видов томографии и в математической физике, при этом несколько модифицируя их.

Ключевые слова: криптография, стеганография, код быстрого реагирования (QR-код), информационная безопасность, преобразование Радона, уравнение Пуассона, итерационные методы.

Важность криптографии с точки зрения передачи скрытых данных очевидна. Тем не менее, будучи тайнописью, она оставляет носителю потенциальной угрозы сам факт существования зашифрованного сообщения, то есть указание на то, что именно надо подвергнуть криптоанализу. С помощью стеганографии конструируются математические методы, которые лишают носителя потенциальной угрозы указанных подсказок. Целью становится такое размещение секретного текста во внешне безобидном послании, когда не возникает никаких подозрений о спрятанной информации. Применительно к транспорту, например, необходимо скрыть, когда и где будут перевозиться опасные или особо ценные грузы, время и место их хранения и т.д. Надо сделать так, чтобы информация была передана совсем незаметно для общей массы людей, имеющих доступ к сетям.

В статье [1] на конкретном примере реализуется итерационный алгоритм обратного преобразования Радона при наличии случай-



а) *б)* *в)*

Рис. 1: а) простейший пример фрагмента QR-кода; б) преобразование Радона; в) на объект рис. 1b наложен модельный 10% шум, распределённый по равномерному закону, и затем выполнено обратное преобразование Радона. После применения программы очистки от шума получается объект, совпадающий с рис. 1а на 99%.

ного шума и систематических ошибок и сбоев в работе детекторов. Объясняется, что интегральное преобразование функции g(x, y) в идеале (без шумов) обладает свойством совместности, которое накладывает определённое ограничение на измеренные в разных направлениях угла ξ проекций f(ξ, p) (в теории томографии эта функция называется синограммой). В строгой формулировке условия совместности выражают связь между одномерными моментами проекций и двумерными моментами изображений. В реальных экспериментальных измерениях свойство совместности нарушается. Такое нарушение проявляется в большом значении нормы невязки, т.е. в существенном отличии проекционных данных от псевдопроекций, полученных преобразованием Радона от восстановленной тем или иным алгоритмом томограммы. Учёт условия совместности проекций позволяет получать более точное решение обратной задачи.

ИСПОЛЬЗОВАНИЕ ПРЕОБРАЗОВАНИЯ РАДОНА

В работе [2] предлагается использовать подобные методы в другой области приложения – стеганографии. Предполагается, что некто (НК) желает отправить адресату (А) информацию скрытно от постороннего наблюдателя, закодированную в QR-коде.

Задаём функцию двух переменных:

$$\varphi(x,y)=\begin{cases}1, & if\ (x,y)\in\Omega,\\ 0, & if\ (x,y)\notin\Omega\end{cases}, \qquad (1)$$

где через Ω обозначено множество чёрных квадратов на рис. 1а, а всю область рис. 1а можно представить как объединение некоторого множества одинаковых чёрных и белых элементарных квадратов. Маскируемым изображением является преобразованный QR-код, в нем находится передаваемая информация.

Здесь через $d_1 = 12$ пикселей обозначена толщина уголка, а через $d_2 = 1{,}7d_1$ пикселей – ширина щели между уголками. Выбраны сетка 64 x 64 и 100 ракурсов.

Затем используется известная технология «водяных знаков» [6], и подходящий, заранее оговорённый контейнер передаётся «А», который располагает программой восстановления «ВО».

Разбиваем всё поле и заданный QR-код на одинаковые элементарные белые и чёрные квадраты (прямоугольники) и вычисляем их центры тяжести (это точка пересечения диагоналей). Вычисляем функцию (1).

В работе [2] предложены некоторые методы предварительной маскировки и усложнения сообщения. В данном случае предлагается для этой цели использовать другой способ, а именно метод, применяемый в теории фракталов: «итерация линейными системами».

Организуем итерационный процесс

$x_{k+1} = e + ax_k + by_k$, $y_{k+1} = f + cx_k + dy_k$,

где k = 0, 1, ... – номер итерации, x_k, y_k – координаты центров тяжести элементарных чёрных квадратов, составляющих QR-код

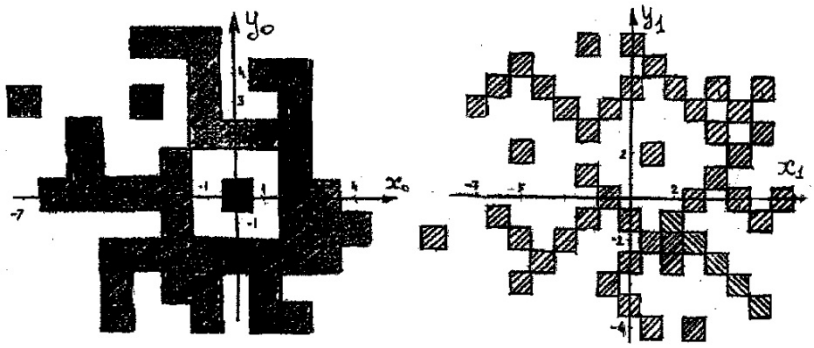


Рис. 2. Фрагмент QR-кода. Справа приведена первая итерация с помощью линейных систем; a = 1, b = –1, c = 1, d = 1, e = 1, f = 2.

в декартовой системе координат на k-итерации. Начало координат, точка (0, 0) на Ω, масштаб и направление осей относительно графика известны только НК и связаны с заданным QR-кодом. Это же относится к заданным вещественным константам {*e, a, b, f, c, d*} и выбранному числу итераций k. Таким образом, появляются дополнительные ключи. Отметим, что структура и геометрия при каждой итерации существенно меняется, но существует единственное обратное преобразование, позволяющее восстановить исходное начальное условие – QR-код по формулам:

$$x_k = -(b\,f - d\,e + d\;x_{k+1} - b\,y_{k+1})\,/\,Dn,$$
$$y_k = -(c\,e - a\,f - c\,x_{k+1} + a\,y_{k+1})\,/\,Dn, \quad (2)$$
$$Dn = b\,c - a\,d \neq 0.$$

Изложим кратко применяемый алгоритм [2, 3].

Замечание 1. *Предлагается конструировать параллельно две программы. В программе 1 описывается процедура вычисления преобразования Радона для семейства QR-кодов и вычисляются или задаются все ключи (необходимые значения констант).*

Вторая программа восстанавливает оригинал по изображению с шумами, с вероятностью возникающими при отделении от стегаконтейнера. Для надёжности восстановления «оригинала», т.е. вычисления центров тяжести элементарных квадратов, из которых состоит «О», предлагается решать одну и ту же задачу разными методами, используя итерации с помощью линейных систем, преобразование Радона и краевую задачу для уравнения Пуассона, а затем включая методы отбора центров тяжести элементарных квадратов, основанные на теории вероятностей.

В модельном варианте в данной работе рассматриваются три объекта: оригинал «О»: изображение, полученное после интегрального преобразования «И»: восстановленный оригинал «ВО». При этом «ВО» отличается от «О» ошибкой, возникающей из-за шума и решения обратной некорректной задачи.

Обозначим в двумерной постановке через g(x, y) неизвестную функцию, подлежащую определению «ВО»; через f(ξ, p) – «И», интегралы от этой функции вдоль семейства параллельных прямых, идущих под углом ξ к оси OX: «прицельный параметр» p – расстояние от луча из семейства прямых до начала координат (со знаком). Связь между функцией f(ξ, p) «И» с функцией g(x, y) «О» установлена Иоганном Радоном в 1917 году как преобразование Фурье, записанное в полярной системе координат. Преобразование Радона становится методом решения обратной задачи интегральной геометрии, суть которого в восстановлении *(реконструкции)* многомерных функций по их интегральным характеристикам «И». Частный случай преобразования, используемый в [2], имеет вид:

$$f(\xi, p) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} g(x,y)\,\delta(p + x\sin\xi - y\cos\xi)\,dx\,dy. \quad (3)$$

Однако этот метод не нашёл широкого применения до тех пор, пока не появился первый томограф в 1972 году. Освоение томографии привело к прогрессу в медицине, диагностике болезней, кристалло-

графии, изучении строения молекул, в геофизике, астрофизике и т.д. Теперь к этому списку добавляется и стеганография [1, 6].

Обозначим через

$$W = \left\{ x_{ij}, y_{ij}, i = 1,\ldots,n, \mathrm{j} = 1,\ldots,m \right\}$$

множество центров тяжести белых и чёрных элементарных квадратов в области Ω. Отдельно выделим множество V пар индексов (ð, ν) центров тяжести только чёрных элементарных квадратов (прямоугольников) в области.

Замечание 2. *В известных расчётах координаты центров тяжести элементарных квадратов задавались в программах вручную. Этим и объясняется то, что вычисления делались для конкретного фрагмента и его двух итераций (рис. 2).*

В. В. Пикалов в переписке с авторами высказал своё мнение о том, что самой сложной и весьма громоздкой нерешённой частью предлагаемого комплекса алгоритмов является программа автоматического определения центров тяжести элементарных квадратов для каждого следующего представителя из семейства QR-кодов.

Отметим, что библиотека синограмм для моделей, составленных, в частности, из прямоугольников на языке Mathlab и Python (оболочка с интерпретатором Anaconda), имеется в [15]. Сложности могут возникать при восстановлении «И» с большим шумом, распределённым по неизвестному закону (см. замечание 1).

Подчеркнём, что в тех же целях перспективно использование взвешенного преобразования Фурье (взвешенного преобразования Радона) [7]. Функция веса в этом преобразовании также является дополнительным «ключом», препятствующим несанкционированной реконструкции «ВО».

Определение. *Маскирующей функцией будем называть функцию χ(x, y), которая задаёт координаты центров тяжести новых чёрных квадратов, не существовавших ранее в заданном QR-коде и дополняющих множество в Ω.*

СПОСОБ ПЕРЕДАЧИ С ПОМОЩЬЮ КРАЕВОЙ ЗАДАЧИ ДЛЯ УРАВНЕНИЯ ПУАССОНА

Вместо преобразования Радона возможно предлагаемое в [3] решение краевой задачи Дирихле для уравнения Пуассона. Интерес к задачам в областях сложной формы имеется в различных приложениях [16].

Замечание 3. *Известна запись решения краевой задачи Дирихле для уравнения Пуассона в прямоугольнике с помощью функции Грина и метода рядов Фурье. На практике, чтобы достичь необходимой точности вычислений, надо суммировать не одну сотню членов осциллирующего ряда с медленно убывающими коэффициентами. Приходится вычислять ещё и интегралы от таких сумм.*

Другое направление исследований проблемы, с точки зрения авторов, лежит в развитии подходов, изложенных в [4].

В нашем случае покажем, как может быть реализован предполагаемый алгоритм.

Выше предлагалось разбивать всё поле и заданный QR-код на белые и чёрные элементарные квадраты и вычислять их центры тяжести. То есть по формуле (1) строим функцию двух переменных ϕ(x, y).

Шаг 1. Здесь два варианта.

В первом случае выбираем двухшаговый шаблон сетки, необходимой для разностной аппроксимации краевой задачи. Чаще всего четырёхугольник минимальной площади, охватывающий все заштрихованные элементарные квадраты, составляющие QR-код, оказывается прямоугольником.

Положим для определённости:

$$x \in [x_{\min}, x_{\max}],\ y \in [\mathrm{y}_{\min}, \mathrm{y}_{\max}],$$

$$x_{\max} > 0,\ y_{\max} > 0,\ x_{\min} < 0, \mathrm{y}_{\min} < 0.$$

Обозначим через

$$m_1 = |x_{\max}| + |x_{\min}|,\ m_2 = |y_{\min}| + |y_{\max}|.$$

Если это квадрат, то переходим во второй случай с одним постоянным шагом. Чтобы получить после разностной аппроксимации краевой задачи квадратную невырожденную матрицу, используем маскирующую функцию χ(x, y), добавляя в QR-код элементарные чёрные квадраты, добиваясь отсутствия в матрице линейно зависимых строк и столбцов, что заведомо обеспечивает невырожденность преобразования (2). Естественно, координаты центров тяжести таких элементарных квадратов записываются в программах 1 и 2 в некоторые массивы, аналогичные упомянутым в замечании 1. Вся область разбивается на элементарные прямоугольники двумерной

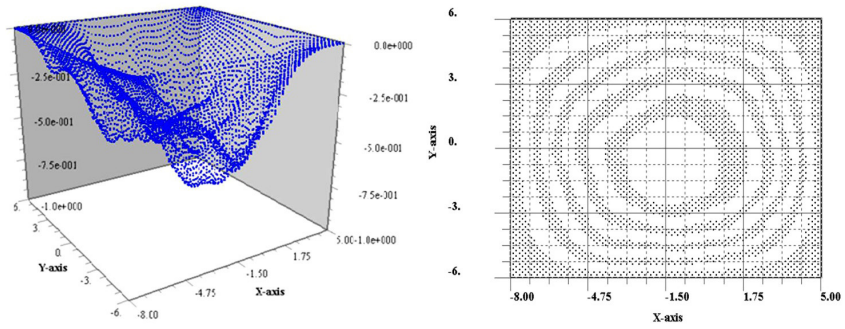


Рис. 3. Решение задачи (6) в изометрии соответствует QR-коду, изображённому на левом фрагменте рис. 2. $n_1 = 104$, $n_2 = 96$, aa = –8, bb = 5, cc = –6, dd = 6 и линии уровня. Число итераций k = 2000.

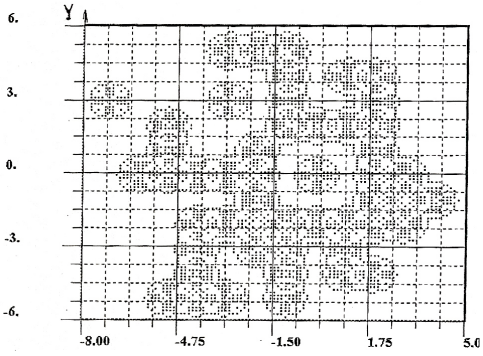


Рис. 4. Узловые точки сетки, попадающие на фрагмент QR-кода.

сеткой. Вводим двумерную равномерную сетку:

$$\omega_{n_1 n_2} = \left\{ \begin{array}{l} x_m = x_{\min} + m h_1,\ y_m = y_{\min} + n h_2, \\ m = \overline{0, n_1},\ n = \overline{0, n_2},\ h_1 = \dfrac{x_{\max} - x_{\min}}{n_1}, \\ h_2 = \dfrac{y_{\max} - y_{\min}}{n_2} \end{array} \right\}. \quad (4)$$

Отметим также, что длины сторон элементарного чёрного (белого) прямоугольника, обозначенного в программе через h_{11}, h_{22}, кратны шагам сетки h_1, h_2, а оси системы координат x, y в графиках, построенных программой, имеют идентификаторы X, Y соответственно (рис. 3).

Шаг 2. Заданная в (1) функция имеет разрыв. Введём функцию f(x, y) = ϕ(x, y) + χ(x, y), непрерывно дифференцируемую с помощью суммы двумерных гауссианов:

$$f(x,y) = \left\{ \begin{array}{l} \sum\limits_{(\delta,\nu)\in V} e^{-\left(\frac{x-x_\delta}{h_{11}0{,}5}\right)^2 - \left(\frac{y-y_\nu}{h_{22}0{,}5}\right)^2}, (\delta,\nu)\in V, (x_\delta, y_\nu)\in W. \\ 0. \end{array} \right. \quad (5)$$

Центры квадратов x_i. y_j определяются формулой (4), где коэффициенты ($h_{11} \cdot 0{,}5$; $h_{22} \cdot 0{,}5$ – половины сторон элементарного прямоугольника) регулируют локально дисперсию распределения Гаусса; (x_i, y_j) – центры чёрных квадратов на равномерной координатной сетке.

Отметим, что в конструируемой программе хранится массив индикаторной функции амплитуды:

$$F_{ij} = \left\{ \begin{array}{l} 1, (i,j) \in N_1^2 \equiv W_{i,j} \\ 0, (i,j) \in N_2^2 \end{array} \right. ,$$

который используется в технических, вспомогательных целях. Здесь N_1^2 – двумерное целочисленное множество узлов-центров чёрных квадратов, соответствующих множеству V; N_2^2 – двумерное целочисленное множество узлов-центров белых квадратов, $N_1^2 \cup N_2^2 = \left\{ (i,j) \in i = \overline{0, n_1},\ j = \overline{0, n_2} \right\}$.

Константы в показателях экспоненциальных функций, которые определяют дисперсию, могут быть заданы не единственным образом.

Запишем двумерное уравнение Пуассона в прямоугольнике

$$0 < x < |aa| + bb,\ 0 < y < |cc| + dd$$

с нулевыми краевыми условиями:

u(0, y)=0, u(a, y) = 0, u(x, 0) = 0, u(x, b) = 0,

$$\Delta u(x, y) = f(x, y), \quad (6)$$

где через

$$\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}$$

обозначен оператор Лапласа.

Для простоты аппроксимации задачи в данном примере выбираем простейший пятиточечный шаблон разностной схемы «крест» и получим на сетке (4) разностное уравнение для двух разных шагов по на-

правлениям, которое приведено во многих работах, например [4], [8, 9, 11, 12]. В [13] изложен хорошо себя зарекомендовавший на практике метод верхней релаксации. В англоязычной литературе его называют Successive QverRelaxation (SOR) метод. Для краткости запишем его в случае равномерной сетки с шагом h:

$$u^{k+1}_{m-1,n} - \frac{4}{\omega}u^{k+1}_{m,n} + u^{k+1}_{m,n-1} =$$
$$= -(u^{k}_{m+1,n} + u^{k}_{m,n+1}) +$$
$$+4(1 - 1/\omega)\mathrm{u}^{k}_{m,n} - h^2 f_{m,n}. \qquad (7)$$

Для реализации этого метода не требуется знания спектра задач, а оптимальное значение параметра ω определяется в процессе численного эксперимента. Авторы [4] предложили обобщить метод и многократно проверили его на задачах, в которых правая часть является аналитической функцией, и сравнили результаты с данными работ [8, 11, 12].

В ходе решения задачи (6) строим итерационный процесс с номером итерации k, используя аналогию с методом (7) и методом чередования направлений [4, 8, 9, 11, 12]. Для конкретности приведём итерационную формулу по одному из направлений на сетке (4):

$$\frac{h_2^2}{2(h_1^2+h_2^2)}u^{k+1}_{m-1,n} - u^{k+1}_{m,n} + \frac{h_2^2}{2(h_1^2+h_2^2)}u^{k+1}_{m+1,n} =$$
$$= \frac{-h_1^2}{2(h_1^2+h_2^2)}(u^{k}_{m,n-1} + u^{k}_{m,n+1}) +$$
$$+ f_{m,n}\frac{h_1^2 h_2^2}{2(h_1^2+h_2^2)} + O(h_1^2 h_2^2). \qquad (8)$$

Здесь через $f_{m.n}$ обозначена разностная аппроксимация сглаженной формулы (5). Очевидно, что на каждой итерации имеем трёхдиагональную матрицу, и следовательно, можно использовать формулы алгоритмизированного метода Гаусса, или формулы правой прогонки. По сути, выполнено хорошо известное условие устойчивости этого метода. Оно заключается в том, что обеспечено выполнение неравенства «диагональное преобладание элементов матрицы над суммой модулей недиагональных элементов» [9]. Погрешность решения указана в формуле (8).

Далее текстовой файл решения задачи (6) можно использовать в технологии

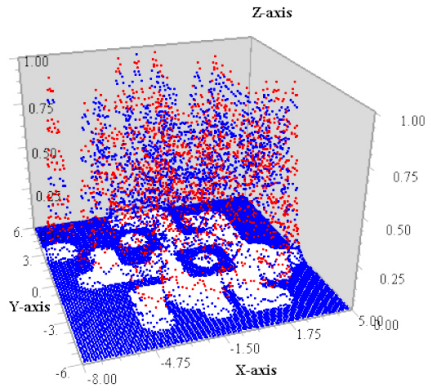


Рис. 5. Изометрия разностной аппроксимации функции (5).

встроенных «водяных знаков» [6]. Подходящий, заранее оговорённый стегоконтейнер передаётся «А» с программой восстановления «ВО».

Обратное преобразование проводится с помощью нахождения локальных максимумов и минимумов лапласиана. Вычисляются точки центров тяжести элементарных чёрных квадратов и далее «руками в программе» восстанавливаются сами квадраты.

В [4, 8, 11] разработаны методы решения задачи (6) с повышенной точностью.

В частности, там рассмотрен девятиточечный шаблон «крест» и построены итерационные формулы. Приведены доказательство достаточных условий устойчивости $\lambda_s < 1$ и доказательство сходимости итерационного процесса по принципу сжимающих отображений [10]. Составлены программы на современной версии языка Fortran [12], поддерживающая максимальные массивы для функции решения (8) и вычисляющая нормы Чебышева невязки между разностным решением и проекцией точного решения на сетку.

Второй случай с одним шагом сетки. Дополняем с помощью маскирующей функции χ(x, y) QR-код до большого квадрата, то есть добиваемся, чтобы полученная матрица функции f(x, y) = ϕ(x, y) + χ(x, y), содержащая единицы, была квадратной и невырожденной (см. формулы (1),(5)). Если в заданном QR-коде имеются повторяющиеся строки или столбцы квадратов (линейно зависимые), то с помощью маскирующей функции можно добавить некоторое минимальное количество заштри-

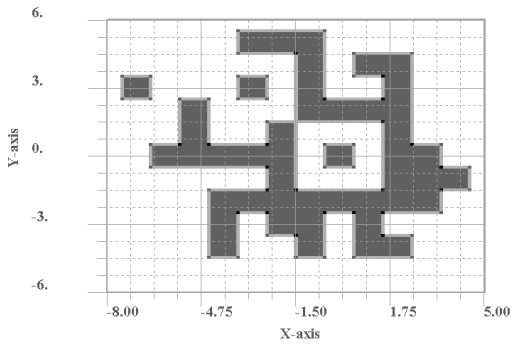


Рис. 6. m = 2000, n_1 = 104, n_2 = 96, m_1 = 13, m_2 = 12, a = –8, b = 5, c = –6, d = 6, n = max (n_1, n_2). В центре точки каждого локального максимума оператора Лапласа «руками в программе» восстанавливаются, строится элементарный чёрный квадрат со сторонами, параллельными координатным осям, т.е. правая сглаженная часть уравнения Лапласа опять заменяется разрывной функцией с разрывами первого рода на краях элементарных прямоугольников (см. начало статьи).

хованных квадратов в QR-код и нормализовать ситуацию. Конечно, координаты центров тяжести введённых новых квадратов с помощью функции $\chi(x, y)$ надо запомнить в программах 1 и 2 (см. замечание 2). Далее в приведённых ранее формулах следует положить шаги сетки равными h. Затем следуем алгоритму, изложенному в первом случае.

ВЫВОДЫ

Предложены варианты сокрытия информации в новом направлении развития стеганографии, которые дают веер возможностей для применения различных математических результатов из других областей приложений. Достоверность результатов подтверждается строгостью математических построений в упоминаемых работах, многолетним применением их на практике, включая томографию разного вида в медицине, томографию в физике плазмы, в теории и методологии распознавания образов, методов обратной задачи рассеяния, в математической физике, электро- и магнитостатике, гидродинамике и т.д. К преимуществам метода относится возможность применить наработки и программы, имеющиеся в указанных областях приложений.

ЛИТЕРАТУРА

1. Пикалов В. В., Казанцев Д. И. Итерационное восстановление возмущения синограммы в пространстве Радона для задач стеганографии // Вычислительные методы и программирование. – 2008. – № 1. – С. 1–9.

2. Волосова Н. К. Применение преобразования Радона в стеганографии // LXXI международная конференция «Герценовские чтения». – СПб., 2018. – С. 234–238.

3. Волосова Н. К. Преобразование Радона и уравнения Пуассона в компьютерной стеганографии // Международная конференция по дифференциальным уравнениям и динамическим системам. – Суздаль, 2018. – С. 61.

4. Пастухов Д. Ф., Пастухов Ю. Ф. Аппроксимация уравнения Пуассона на прямоугольнике повышенной точности // Вестник Полоцкого государственного университета. Серия: Фундаментальные науки. Математика. –2017. – № 12. – С. 62–77.

5. Тихонов А. Н., Арсенин В. Я., Тимонов А. А. Математический анализ компьютерной томографии. – М.: Наука, 1987. – 160 с.

6. Шелухин О. И., Канаев С. Д. Стеганография. – М.: Горячая линия-Телеком, 2017. – 592 с.

7. Novikov R. G. Weighted ray transform and application Conference handbook and proceedings. Quasilinear Equations, Inverse Problems and Their Applications, MIPT, Russia, 5–7.12.2017.

8. Бахвалов Н. С., Лапин А. В., Чижонков Е. В. Численные методы в задачах и упражнениях. – М.: Высшая школа, 2000. – 190 с.

9. Самарский А. А., Вабищевич П. Н. Численные методы решения обратных задач математической физики: Учеб. пособие. – М.: Изд-во ЛКИ, 2014. – 480 с.

10. Колмогоров А. Н., Фомин С. В. Элементы теории функций и функционального анализа. – 7-е изд. – М.: Физматлит, 2004. – 572 с.

11. Волков К. Н., Дерюгин Ю. Н., Емельянов В. Н. и др. Методы ускорения газодинамических расчётов на неструктурированных сетках. – М.: Физматлит, 2013. – 536 с.

12. Бахметьев О. В. Современный Фортран. – М.: Диалог-МИФИ, 2000. – 449 с.

13. Федоренко Р. П. Релаксационный метод решения разностных эллиптических уравнений // Журнал вычислительной математики и математической физики. – 1961. – № 5. – С. 922–927.

14. Мицкевич М. Н. Обнаружение областей изображений для встраиваемых цифровых водяных знаков с помощью вейвлет-преобразования // Вопросы защиты информации. – 2015. –№ 1. – С. 81–83.

15. Терещенко С. А. Методы вычислительной томографии. – М.: Физматлит, 2004. – 320 с.

16. Басараб М. А., Кравченко В. М. Полуаналитические координатные последовательности для решения краевых задач Дирихле в областях сложной формы // Доклады РАН. – 2004. – № 2. – С. 172–176.

Координаты авторов: **Вакуленко С. П.** – k–gdsu@mail.ru, **Волосова Н. К.** – navolosova@yandex.ru, **Пастухов Д. Ф.** – dmitrij.pastuhov@mail.ru.

Статья поступила в редакцию 05.07.2018, актуализирована 17.10.2018, принята к публикации 19.10.2018.