Математические структуры и моделирование
2014. № 4(32). С. 225–231

УДК 004.056

ПРИМЕНЕНИЕ СЕМЕЙСТВ ОРТОГОНАЛЬНЫХ ФУНКЦИЙ ДЛЯ ПОСТРОЕНИЯ УСТОЙЧИВЫХ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

С.В. Белим
профессор, д.ф.-м.н., e-mail: sbelim@mail.ru
Е.А. Илюшечкин
аспирант, e-mail: ilushechkinea@yandex.ru

Факультет компьютерных наук, Омский государственный университет им. Ф.М. Достоевского

Аннотация. Рассмотрено применение семейств ортогональных функций для построения цифровых водяных знаков. Предложен алгоритм кодирования сообщений на основе свойств ортогональных функций, который позволяет строить цифровые водяные знаки, устойчивые к различным воздействиям на стеганографический контейнер. Исследовано влияние выбора семейства функций на стойкость цифрового водяного знака, построенного по предложенному алгоритму, к ряду искажающих воздействий.

Ключевые слова: семейства ортогональных функций, цифровые водяные знаки, многочлены Чебышёва, функции Уолша, искажающие воздействия.

Введение

Внедрение скрытой информации в растровые изображения является одним из динамично развивающихся разделов информационной безопасности, получившим название стеганографии. На сегодняшний день разработано большое количество алгоритмов встраивания информации как в пространственной области изображений, так и в частотной. Дополнительный импульс в развитии стеганографии появился в связи с развитием направления, которое принято называть цифровыми водяными знаками. Под цифровыми водяными знаками принято понимать некоторую информацию, встроенную в изображение и неотъемлемо связанную с ним, позволяющую однозначно идентифицировать источник происхождения изображения. Одно из основных требований к алгоритмам встраивания цифровых водяных знаков — устойчивость к воздействию на контейнер. То есть, встраиваемая информация должна восстанавливаться после широко распространённых преобразований растровых изображений, таких как изменение формата, применение сглаживающих фильтров и т.д.

Устойчивость большого количества стеганографических алгоритмов к воздействию случайного гауссова шума и JPEG-сжатия была исследована в работе [1]. На основе компьютерного эксперимента было показано, что наилучшей устойчивостью обладают методы Коха [2], Куттера [3] и Фридрих [4].

В данной работе разрабатывается алгоритм формирования цифровых водяных знаков, устойчивых к различным воздействиям, с использованием свойств семейства ортогональных функций, предложенного в статье [5] для кодирования информации.

1. Кодирование цифровых водяных знаков и процедура встраивания в контейнер

Для построения устойчивых водяных знаков будем использовать семейство ортогональных функций — множество функций $\{f_i(x)|\ i \in \mathbf{N}\}$ таких, что существует весовая функция $w(x)$ и интервал $[a, b]$, для которых

$$\int_a^b f_i(x)f_j(x)w(x) = \delta_{ij}, \tag{1}$$

где δ_{ij} — символ Кронекера.

Пусть информация, которую необходимо закодировать, представляет собой последовательность вещественных чисел k_i $(i = 1, ..., n)$. Используя семейство ортогональных функций $\{f_i(x)|\ i \in \mathbf{N}\}$, построим функцию:

$$F(x) = \sum_{i=1}^{n} k_i f_i(x). \tag{2}$$

Исходные числа k_i могут быть восстановлены из $F(x)$ на основе свойства ортогональности с помощью простого соотношения:

$$k_i = \int_{x_1}^{x_2} f_i(x)f(x)w(x)\mathrm{d}x. \tag{3}$$

На основе рассмотренного выше подхода можно построить следующий алгоритм кодирования k-битовой строки $(b_1, b_2, ..., b_k)$ водяного знака в виде массива из n значений:

1. Выбрать k функций: $f_1, f_2, ..., f_k$ из семейства ортогональных функций
2. Выбрать n точек $p_1, p_2, ...p_n$ на отрезке ортогональности $[x_1,\ x_2]$
3. Для каждого $i = 1, ..., n$ вычислить сумму $v_i = \sum\limits_{j=1}^{k} b_j f_j(p_i)$

Получившийся массив $(v_1, ..., v_n)$ представляет собой дискретизированный сигнал, который может быть добавлен к исходному изображению. Для лучшего распределения информации о водяном знаке по изображению сигнал можно добавлять в частотной области изображения. В нашем случае для перехода в частотную область использовалось дискретное косинусное преобразование.

Извлечь данный цифровой водяной знак можно, применив численное интегрирование по точкам $p_j,\ j = 1, ..., n$. Для бита b'_i значение интегрируемой функции в точке p_j определяется как произведение $f_i(p_j)r_jw(p_j)$, где r_j — значения тех точек водяного знака, в которые он был ранее встроен. Очевидно, значения данных точек складываются не только из встроенного сигнала, но и из исходных значений точек контейнера. Тем не менее, на практике исходные значения контейнера мало коррелируют с ортогональными функциями, и их влиянием можно пренебречь.

К полученным оценкам b'_i можно применить пороговую схему, отображающую вещественную прямую на множество {0, 1}, получив тем самым восстановленное сообщение.

Поскольку n не зависит от k, исходную информацию произвольного объёма (но не превышающего пропускной способности контейнера) можно равномерно растягивать по фиксированному количеству точек, доступному для встраивания в данном контейнере. Это позволяет эффективно и гибко использовать все доступные для встраивания точки.

2. Постановка компьютерного эксперимента

В ходе эксперимента была протестирована устойчивость цифровых водяных знаков, сформированных с помощью предложенного метода, к ряду популярных преобразований изображения — зашумлению, JPEG-сжатию, размывающей фильтрации. Мерой корректности распознавания цифрового водяного знака являлось отношение количества неверно распознанных битов сообщения к их общему числу, Bit Error Rate (BER). В роли контейнеров выступали широко используемые для тестирования различных методов обработки цветные изображения «Lenna», «Mandrill» и «Pepper» размером 512×512. Все тестируемые методы использовали для встраивания канал яркости, обозначаемый буквой Y в цветовой схеме YCbCr.

Было протестировано три вида зашумляющих воздействий: аддитивный шум с гауссовым распределением, аддитивный шум с равномерным распределением и неаддитивный импульсный шум. Под аддитивным шумом понималось изменение яркости каждой точки изображения на значение элемента псевдослучайной последовательности вещественных чисел, имеющей равномерное или нормальное распределение с заданными параметрами. Параметром равномерного шума являлась верхняя граница интервала возможных значений, симметричного относительно нуля. Этот же параметр рассматривался как мера искажающего воздействия. Для гауссового шума параметром и, одновременно, мерой воздействия являлось стандартное отклонение нормально распределённой случайной величины с нулевым средним, которую имитировала псевдослучайная последовательность. Неаддитивный импульсный шум был реализован как замена с фиксированной вероятностью p каждой точки изображения на точку с максимальной яркостью. В качестве меры искажающего воздействия в данном случае выступала величина p, выраженная в процентах.

Для реализации размывающей фильтрации использовался простой арифметический фильтр, заменяющий значение яркости каждой точки изображения на среднее арифметическое значение яркости в окне размером 3×3 точки. Для краевых неугловых точек среднее значение вычислялось по прямоугольнику размером 3×2, а для угловых — по квадрату размером 2×2. В качестве силы искажающего воздействия рассматривалось количество последовательных применений фильтра.

При JPEG-сжатии использовался стандартный алгоритм JPEG, в качестве силы воздействия рассматривался параметр алгоритма, процентно выражающий качество изображения после сжатия.

Чтобы определить зависимость точности извлечения водяного знака от силы искажающего воздействия и построить соответствующие графики, в качестве водяного знака использовалась случайная последовательность из 32 байтов, повторенная 16 раз в целях надёжности. Таким образом, каждый бит встраивался и извлекался 16 раз, а его итоговое извлечённое значение определялось как округлённое среднее всех его извлечений. Чтобы уменьшить погрешность, вызванную случайным характером данных, эксперимент проводился по несколько раз на каждом изображении и затем усреднялся.

В качестве способа численного интегрирования использовался метод трапеций.

3. Влияние выбора семейства ортогональных функций

В эксперименте были рассмотрены четыре семейства ортогональных функций. Первое — семейство синусов вида $f_n(x) = \sqrt{2}\sin(\pi n x)$. Для данного семейства использовался отрезок ортогональности [0; 2]. Чтобы пики различных функций суммы не совпадали, имеет смысл выбирать функции семейства со взаимно простыми периодами, то есть, со взаимно простыми номерами. Тогда за счёт снижения максимальных искажений коэффициентов можно будет повысить коэффициент силы встраивания без ущерба для качества изображения.

Многочлены Чебышёва первого порядка вычисляются по формуле $f_n(x) = \cos(n \arccos(x))$ и имеют единственный отрезок ортогональности [-1; 1], на котором и вычислялись значения суммы функций. Характерной особенностью многочленов Чебышёва является то, что они имеют нетривиальную весовую функцию, при умножении на которую произведение двух многочленов стремится к бесконечности на границах отрезка ортогональности. Быстрый рост у границ отрезка усложняет восстановление по точкам — при вычислении интеграла приходится немного сужать пределы интегрирования (в нашем случае — на 0.1%). Для более точной оценки возможно применение неравномерной сетки.

Многочлены Лежандра также имеют единственный отрезок ортогональности [-1; 1], но в отличие от многочленов Чебышёва имеют тривиальную весовую функцию и не создают проблем на концах отрезка.

Наконец, было протестировано семейство ортогональных функций Уолша, которые, как и многочлены Лежандра, имеют тривиальную весовую функцию и отрезок ортогональности [-1; 1].

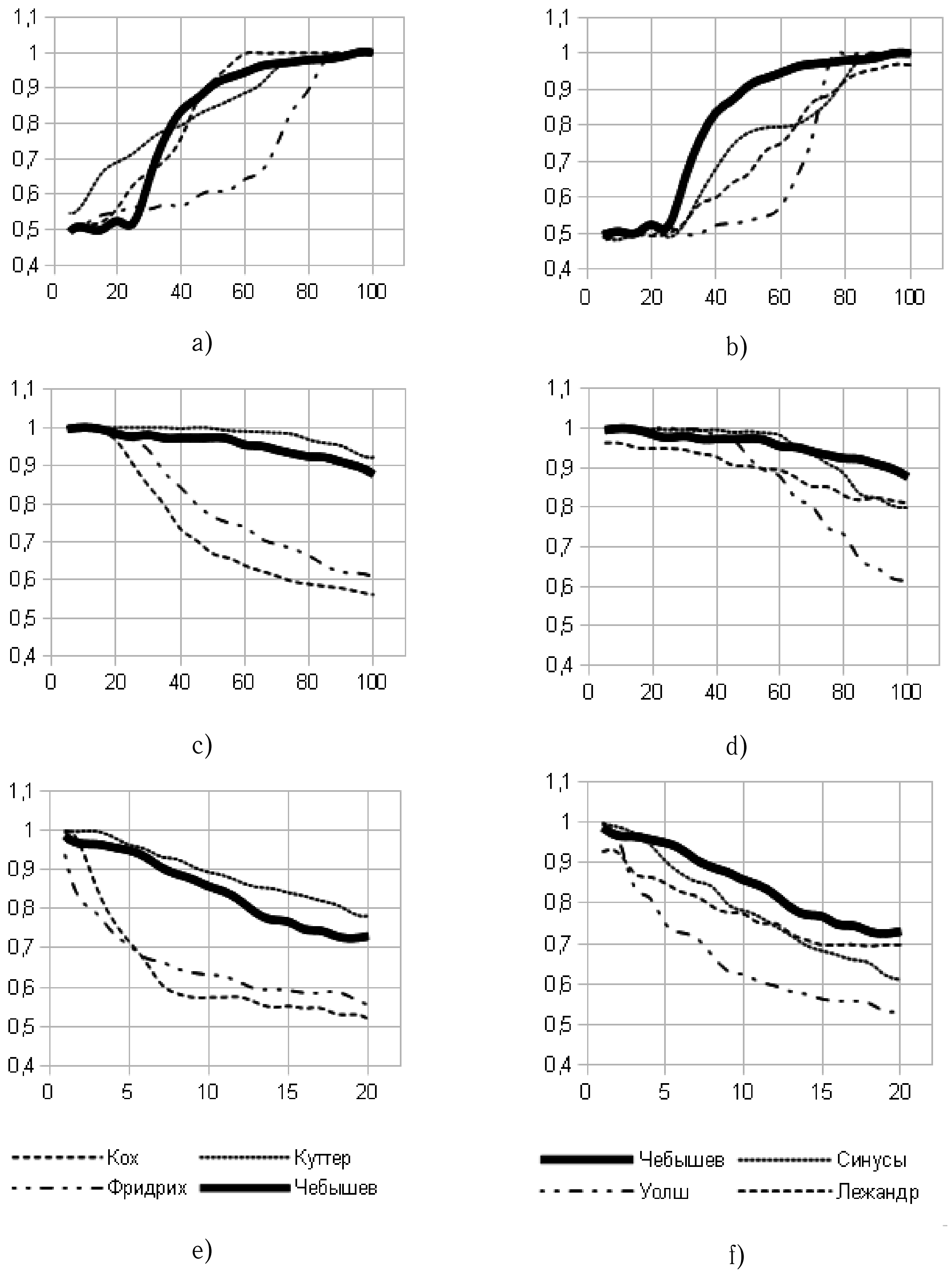

Рис. 1. Устойчивость различных методов к искажающим воздействиям: a-b) JPEG-сжатие; c-d) Равномерный шум; e-f) Импульсный шум.

4. Результаты эксперимента

По результатам проведённого компьютерного эксперимента было построено несколько графиков (рис. 1). По оси абсцисс на графиках отложена сила искажающего воздействия, по оси ординат — значение (1 - BER). Результаты для размывающей фильтрации не показаны, так как все протестированные семейства функций оказались не стойкими к данному виду искажающего воздействия. На рисунках 1 (b, d, f) показаны результаты кодирования по предложенной нами схеме для различных семейств функций. Видно, что практически на всех участках лучший результат показывает семейство многочленов Чебышёва первого рода. Второй результат показывает семейство тригонометрических функций.

Результаты, полученные для многочленов Чебышёва, были сопоставлены с результатами нескольких хорошо известных методов встраивания — методов Коха [2], Куттера [3] и Фридрих [4] (левый столбец на рис. 1 (a, c, e). Предложенный метод оказался устойчивее методов Фридрих и Коха к зашумлению равномерным и импульсным шумом, более устойчив к JPEG-фильтрации, чем метод Фридрих (рис. 1).

Развитие идеи использования ортогональных семейств функций для построения цифровых водяных знаков может заключаться в апробации других семейств и их сравнении на более широком спектре искажающих воздействий. Важным шагом также является исследование влияния метода численного интегрирования на результат восстановления водяного знака для различных семейств ортогональных функций.

Литература

1. Илюшечкин Е.А. Некоторые способы повышения устойчивости цифровых водяных знаков к искажающим воздействиям // Вестник Омского университета, 2013, Т. 70, №4, С. 217-220.
2. Koch E., Zhao J. Towards Robust and Hidden Image Copyright Labeling // IEEE Workshop on Nonlinear Signal and Image Processing. Greece. 1995. P. 123–132.
3. Kutter M., Jordan F., Bossen F. Digital Signature of color image using amplitude modulation // Proc. of the SPIE Storage and Retrieval for Image and Video Databases V. 1997. Vol. 3022. P. 518–526.
4. Fridrich. J. Combining Low-Frequency and Spread Spectrum Watermarking // Proc. of the SPIE Conference on Mathematics of Data/Image Coding, Compression and Encryption. 1998. Vol. 3456. P. 2–12.
5. Белим С.В., Белим С.Ю. Шифрование сообщений на основе собственных функций операторов // Математические структуры и моделирование, 2008, № 18, С. 95–97.

APPLYING FAMILIES OF ORTHOGONAL FUNCTIONS TO BUILDING RESISTANT DIGITAL WATERMARKS

S.V. Belim
Professor, Doctor Of Physical and Mathematical Sciences, e-mail: sbelim@mail.ru
E.A. Ilushechkin
Postgraduate Student, e-mail: ilushechkinea@yandex.ru

Omsk State University n.a. F.M. Dostoevskiy

Abstract. In this paper, the use of families of orthogonal functions for digital watermarks building is considered. We suggest an algorithm of message encoding based on properties of orthogonal functions that allows to build digital watermarks resistant to different impacts on the stegocontainer. We also investigate how the choice of orthogonal functions family influences the resistance of digital watermark built using the proposed method to various distortions.

Keywords: families of orthogonal functions, digital watermarks, Chebyshev polynomials, Walsh functions, distorting effects.