

Г. И. Борзунов, А. Е. Войнов, Е. А. Сучкова

## ВЫБОР БАЗОВОГО АЛГОРИТМА ДЛЯ РАСЧЕТА МИНИМАЛЬНОГО КОЛИЧЕСТВА ПРОЦЕССОРОВ, ОБЕСПЕЧИВАЮЩЕГО ДОСТИЖЕНИЕ ЗАДАННОГО ЗНАЧЕНИЯ КОЭФФИЦИЕНТА УСКОРЕНИЯ

Известно, что проблема оптимального разделения взвешенного графа является NP-сложной и точные методы ее решения существуют для узкого класса задач. Анализ используемых подходов к оптимальному разделению взвешенных графов показал, что геометрические методы обладают рядом преимуществ при расчетах баланса вычислительной нагрузки процессоров без учета коммуникационных затрат, а спектральные методы минимизируют коммуникационные затраты при существенных ограничениях на структуру графа. В общем случае минимизация коммуникационных затрат и равномерное распределение вычислительной нагрузки по процессорам являются противоречивыми требованиями. Поиск компромиссного решения требует применения комбинаторных методов, которые основываются на конструктивном перечислении вариантов разбиения множества вершин графа. Алгоритмы, опубликованные в работах [1, 2], не обеспечивают перечисления вариантов разбиений множеств в порядке монотонного возрастания числа подмножеств, что не позволяет их использовать при определении минимального числа параллельно работающих процессоров, которые обеспечивают заданное ускорение параллельных вычислений. Указанного недостатка лишен алгоритм Eq2\_1, который был предложен в работе [3]. Теоретический анализ показал, что вычислительная схема на основе алгоритма Eq2\_1 позволяет ускорить последовательный поиск разбиения множества, удовлетворяющего заданным ограничениям, в среднем в два раза. Указанное ускорение определяется числом сравнений и характеризует свойства алгоритма. При таком анализе не учитывались временные затраты на генерацию каждого нового характеристического вектора разбиения множества. Поэтому для объективной оценки временных сложностей вычислительных схем, основанных на алгоритмах, описанных в работах [1, 2], и вычислительной схемы на основе алгоритма Eq2\_1 оказалась необходимой оценка временной сложности генерации характеристических векторов разбиений, т. е. самих указанных базовых алгоритмов.

В данной работе приводятся результаты вычислительного эксперимента по исследованию временной сложности программной реализации этих алгоритмов. Для сравнения с алгоритмом Eq2\_1 из двух стандартных алгоритмов был выбран алгоритм, описанный в книге [1], как более быстродействующий. Эксперимент проводился с использованием компьютера, оснащенного процессором Intel® Pentium® 4 с тактовой частотой 3,00 ГГц и ОЗУ объемом 0,99 ГБ. Так как генерация одного варианта характеристического вектора происходит практически мгновенно, были измерены интервалы времени, в течение которых генерировались все возможные разбиения множества заданной мощности. При этом мощность множества менялась от 10 до 18. Для исключения влияния на время вычислений процессов операционной системы замеры времени генерации разбиений повторялись 16 раз, после чего вычислялись средние значения, которые представлены ниже в таблице 1. Результаты эксперимента, приведенные в таблице 1, показали, что алгоритм Eq2\_1 превосходит по быстродействию стандартный алгоритм, выбранный для сравнения, начиная с мощности множества, равной 12. Причем это превосходство в быстродействии, как видно из таблицы 1, непрерывно возрастает с увеличением мощности множества и, следовательно, с увеличением объема вычислений.



Таблица 1. Сравнение быстродействия базовых алгоритмов генерации разбиений множеств.

Мощность множества (n)	Число вариантов разбиений	Время генерации по алгоритму, описанному в [1], с	Время генерации по алгоритму Eq2_1, с
10	115975	0,001	0,00344444
11	678570	0,007875	0,00877778
12	4213597	0,038875	0,037125
13	27644437	0,23925	0,2285
14	190899322	1,61719	1,542
15	1382958545	11,4268	10,9776
16	10480142147	84,7764	81,6416
17	82864869804	659,559	633,456
18	682076806159	5323,19	5098,03

Таким образом, вычислительный эксперимент подтвердил теоретические результаты анализа временной сложности вычислительной схемы на основе алгоритма Eq2\_1. Это позволяет сделать вывод, что и в реальных условиях использование программной реализации этой вычислительной схемы позволяет ускорить последовательный поиск разбиения множества, удовлетворяющего заданным ограничениям, в два раза.

#### СПИСОК ЛИТЕРАТУРЫ:

1. Романовский И. В. Алгоритмы решения экстремальных задач. М.: Главная редакция физико-математической литературы издательства «Наука», 1971. — 352 с.
2. Липский В. Комбинаторика для программистов. М.: Мир, 1988. — 213 с.
3. Борзунов Г. И. Совершенствование математической модели поиска экстремальных разбиений множеств // Безопасность информационных технологий. 2008. № 3. С. 58–61.

А. С. Борщ

#### МЕТОДЫ СТЕГОАНАЛИЗА

В данной работе приводятся методы анализа файлов мультимедийных форматов на предмет наличия в них вставки скрываемой информации. Описываются основные принципы разработки модели для обнаружения внедрения информации. В ходе выполнения работы были рассмотрены аудио- и видеоформаты, и форматы изображений.

Основной частью работы является анализ двух различных подходов к обнаружению стеганографической вставки. Рассмотрены вставки в форматные части файлов, а также непосредственно в сами данные, отвечающие за аудио- и видеоданные или данные неподвижного изображения.

