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.

Смысл работы первого метода заключается в постановке программных фильтров на «уязвимые» части файлов, такие как зарезервированные поля в mp3-формате, поля расширений в видеофайлах, наименее значимые биты в картинках (последнее больше всего относится к bmp-формату). Помимо этих указанных частей существует множество полей, которые должны оставаться неизменными на протяжении всего файла. Также в первом методе ставятся фильтры на известные стегосистемы и, учитывая свойства их работы, делаются предположения о внедрении или не внедрении данных. Таким образом, метод применим при условии, что мы представляем себе те средства, с помощью которых потенциальный противник производит вставку информации, и, используя систему фильтров, находим передаваемое скрытое сообщение.

Второй метод носит теоретический характер, однако он позволяет с высокой степенью вероятности определять факт наличия в файле-контейнере стеганографической вставки. Смысл его действия сводится к следующему: проводится множество экспериментов над мультимедийными файлами без вставки данных, затем проводится то же самое над этими же файлами только с внедрением информации, произведенной по определенной схеме. После этого строятся статистики некоторых служебных величин, влияющих на воспроизведение файла-контейнера, и находятся отличия в исходных файлах и файлах с внедрением. На основе этого ставятся фильтры, работающие на построении данной статистики и реагирующие на ее существенные изменения. Примером может стать резкое изменение дисперсии параметров part23_length и main_data_end при использовании известного стеганографического продукта MP3Stego в mp3-файлах. Сложность метода заключается в том, что многие мультимедийные файлы получены с помощью различных кодеков. Это предполагает дополнительные требования при построении стегофильтров, так как для некоторых стегосистем первоначальной задачей будет определение того, каким именно кодеком был закодирован файл.

В заключение хотелось бы отметить, что первый метод стегоанализа более подходит для обнаружения скрытия данных в форматной области файлов, тогда как второй больше ориентирован на обнаружение факта передачи в неформатных частях и является более сложным в создании, однако имеющим большее применение в решении практических задач.

СПИСОК ЛИТЕРАТУРЫ:

1. ISO 11172 Annex A., Annex B., Annex C.
2. *Грибунин В. Г., Оков И. Н.* Цифровая стеганография. М., 2007.

Д. С. Булавский, Е. Б. Маховенко

ЦИФРОВАЯ ПОДПИСЬ ГОСТ Р.34.10-2001 НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ В ФОРМЕ ЭДВАРДСА

Значительное время работы функций формирования и проверки цифровой подписи, реализованных в соответствии с ГОСТ 34.10-2001, занимает арифметика на эллиптической кривой. Чтобы ускорить время работы функций, возможен переход к кривой в другой форме, на которой арифметика будет работать быстрее.