Г. И. Борзунов, А. С. Соловьев

СРАВНЕНИЕ АЛГОРИТМОВ КУТТЕРА И БРАЙНДОКСА

Электронная цифровая подпись (далее просто ЦП) — реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования ЦП и проверить принадлежность подписи владельцу сертификата ключа ЦП. В данной работе приводятся результаты сравнения алгоритмов Куттера [1] и Брайндокса [2] по следующим показателям: временная сложность — количество итераций, необходимых для прохода всего изображения с целью формирования и размещения ЦП; устойчивость — способность ЦП реагировать на изменение подписанного изображения; скрытность — способность ЦП не изменять визуального образа подписанного изображения; надежность — вероятностная характеристика несанкционированного удаления ЦП из защищенного изображения. При сравнении использовалась программная реализация двух вышеописанных алгоритмов.

Оценка временной сложности, определяемой как количество итераций, необходимых для обработки всего изображения, показывает, что алгоритм Брайндокса реализует решение указанной задачи быстрее, чем алгоритм Куттера (см. таблицу 1).

Таблица 1.

Размерность изображения	Алгоритм Куттера		Алгоритм Брайндокса	
	Внедрение	Извлечение	Внедрение	Извлечение
786432	786432	2348556	608448	786432
1024000	1024000	3059532	798144	1024000
1296000	1296000	3873972	984256	1290240
1764000	1764000	5275632	1285504	1760640
2073600	2073600	6202812	1495424	2073600
2304000	2304000	6893292	1665600	2304000

Исследование устойчивости как способности цифровой подписи реагировать на изменение подписанного изображения выявило, что алгоритм Брайндокса является более чувствительным по сравнению с алгоритмом Куттера к изменению размеров и к повороту изображения.

Что касается скрытности как способности цифровой подписи выдавать факт своего наличия в подписанном изображении, то определить преимущество одного из этих двух алгоритмов непросто. При использовании алгоритма Куттера места внедрения проявляются только на ярких участках изображений в виде синей сетки. К тому же, если находятся яркие участки с содержанием синей компоненты цвета в количестве выше среднего (больше 128), то они становятся весьма заметными. При использовании алгоритма Брайндокса места внедрения становятся заметными только на переходах от немонотонных по яркости областей к монотонным областям. Так как сетка является более заметной для человеческого зрения и легко выделяется в изображении, то можно считать, что алгоритм Брайндокса обладает большей скрытностью.

При определении надежности рассматриваемых алгоритмов учитывалась вероятность подбора параметров (а также масок при анализе алгоритма Брайндокса), необходимых для извлечения цифровой подписи. Между значениями шага выбора точек внедрения алгоритма Куттера или габаритом маски алгоритма Брайндокса и надежностью алгоритмов выявлена

зависимость: в области малых значений этих параметров более надежен алгоритм Куттера, а в области больших значений этих параметров — алгоритм Брайндокса.

Таким образом, сравнение показало, что алгоритм Брайндокса превосходит алгоритм Куттера по таким характеристикам, как временная сложность (как внедрения, так и извлечения), устойчивость, скрытность, а также надежность в области больших значений параметров.

СПИСОК ЛИТЕРАТУРЫ:

1. *Kutter M., Jordan F., Bossen F.* Digital signature of color images using amplitude modulation // Proc. of the SPIE Storage and Retrieval for Image and Video Databases V. 1997.
2. *Darmstaedter V., Delaigle J.-F., Quisquater J., Macq B.* Low cost spatial watermarking // Computers and Graphics. 1998. Vol. 5. P. 417–423.

М. Ю. Ваганов

РАЗРАБОТКА ИСКУССТВЕННОЙ ИММУННОЙ СИСТЕМЫ, ПРЕДНАЗНАЧЕННОЙ ДЛЯ ОБНАРУЖЕНИЯ ЗАРАЖЕНИЙ КОМПЬЮТЕРНОЙ СИСТЕМЫ

Искусственная иммунная система

Под искусственной иммунной системой принято понимать программные комплексы, принципы функционирования которых аналогичны иммунным системам живых организмов [1].

В данной работе предпринимается попытка создания программного комплекса, использующего принципы иммунной системы [2] для детектирования вредоносного кода. В качестве целевой платформой выбраны операционные системы семейства Windows, а именно: XP, 2000, Server 2003, Vista, Server 2008 и 7. В качестве критериев состояния системы выбраны статистические параметры, на которые в большинстве случаев оказывают влияние вредоносные программы. Все параметры разбиты на четыре группы:

- связанные с работой файловой системы (создание/модификация исполняемых файлов, создание файлов с нестандартными именами, создание файлов с расширениями, не соответствующими заголовку, и т. п.);
- связанные с реестром операционной системы (модификация и удаление ключей, в том числе ключей, гарантированно не связанных с наблюдаемым процессом);
- связанные с сетью;
- связанные с запуском и работой других процессов (запуск процессов с уровнем доступа, допускающим его остановку или запись в его адресное пространство, открытие потоков других процессов, использование хуков, выгрузка системных процессов).

Каждому параметру приписывается вес, характеризующий степень его опасности. Значения весовых коэффициентов определялись в процессе компьютерного эксперимента. Для инициализации системы выбирается гарантированно не зараженная система в виде вектора параметров. В процессе работы системы подсистема защиты набирает статистику параметров и периодически вычисляет отклонения состояния системы от здорового. При обнаружении значительных отклонений идентифицируется подозрительное приложение и переводится в карантин. В дальнейшем приложения, попавшие в карантин, проверяются антивирусными средствами.