тем, если бы пересылка необходимой информации производилась непосредственно, что подтверждается проведенным вычислительным экспериментом, результаты которого в настоящий момент готовятся к печати. Моделирование виртуального диагонального преобладания для матрицы ОС обеспечивает устойчивость при решении рассмотренной выше СЛАУ, что позволяет использовать в качестве контейнера в предложенном методе SISTEMA произвольное изображение, никак не изменяя его явно.

Открытым пока является вопрос организации непосредственного решения СЛАУ. Использование стандартных методов является здесь нежелательным в силу большой размерности матрицы изображения и специфики ее вида.

Список литературы

1. *В.А. Хорошко, А.А. Чекатков.* Методы и средства защиты информации. – К.: Юниор, 2003. - 501 с.

2. *Дж. Деммель.* Вычислительная линейная алгебра. – М. Мир, 2001. – 430 с.

3. *Бахвалов Н.С., Жидков Н.П., Кобельков Г.М.* Численные методы.- М.: БИНОМ. Лаборатория знаний, 2006 г.-636 с.

4. *R.D. Skeel.* «Scaling for numerical stability in Gaussian elimination». Journal of the ACM, 26: 494-526, 1979.

5. *Фихтенгольц Г.М.* Курс дифференциального и интегрального исчисления. Т.1.- М.: Наука, 1969. – 608 с.

6. *Ф.Р.Гантмахер.* Теория матриц.- М.: Наука, 1988. – 552 с.

Поступила 23.11.2006 г.

УДК 681.3.064

Куржеевский И.В., Лакаева Е.А.

АЛГОРИТМ ЗАЩИТЫ ИНФОРМАЦИИ С ПОМОЩЬЮ ВСТРАИВАЕМЫХ В ИЗОБРАЖЕНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

Надежная защита информации от несанкционированного доступа является более чем актуальной. Одно из перспективных направлений защиты информации сформировали современные методы стеганографии. Слово стеганография в переводе с греческого буквально означает тайнопись.

Стеганография представляет собой совокупность методов, основывающихся на различных принципах, которые обеспечивают сокрытие самого факта существования секретной информации в той или иной среде, а также средств реализации этих методов. К ней можно отнести огромное множество секретных средств связи, таких как невидимые чернила, микрофотоснимки, условное расположение знаков, тайные (скрытые) каналы, средства связи с плавающими частотами, голография.

В настоящее время развитие средств вычислительной техники дало толчок развитию компьютерной стеганографии. Сообщения встраивают в цифровые данные, как правило, имеющие аналоговую природу – речь, аудиозаписи, изображения, видео и даже текстовые файлы и исполняемые файлы программ.

Можно выделить две причины популярности исследований в области компьютерной стеганографии в настоящее время: ограничение на использование криптосредств в ряде стран мира и появление проблемы защиты прав собственности на информацию, представленную в цифровом виде. Первая причина повлекла за собой большое количество исследований в духе классической стеганографии (то есть скрытие факта передачи информации), вторая – еще более многочисленные исследования в области так называемых

водяных знаков. Цифровой водяной знак (ЦВЗ) – специальная метка, незаметно внедряемая в изображение или другой сигнал с целью контролировать его использование и для повышения достоверности идентификации цифровых изображений для систем автоматизированной обработки информации.

ЦВЗ могут применяться в основном для защиты от копирования и несанкционированного использования. В связи с бурным развитием технологий мультимедиа остро стал вопрос защиты авторских прав и интеллектуальной собственности, представленной в цифровом виде. Примерами могут являться фотографии, аудио- и видеозаписи и так далее. Преимущества, которые дают представление и передача сообщений в цифровом виде, могут оказаться перечеркнутыми легкостью, с которой возможно их воровство и модификация. Поэтому разрабатываются различные меры защиты информации организационного и технического характера. Одно из наиболее эффективных технических средств защиты мультимедийной информации и заключается во встраивании в защищаемый объект невидимых меток ЦВЗ. Разработки в этой области ведут крупнейшие фирмы в мире.

Название этот метод получил от всем известного способа защиты ценных бумаг, в том числе и денег, от подделки (термин «digital watermarking»). В отличии от обычных водяных знаков ЦВЗ могут быть не только видимыми, но и (как правило) невидимыми. Невидимые ЦВЗ анализируются специальным декодером, который выносит решение об их корректности. ЦВЗ могут содержать некоторый аутентичный код, информацию о собственнике либо какую-нибудь управляющую информацию. Наиболее подходящим объектом защиты при помощи ЦВЗ являются файлы видео- и аудиоданных, изображения.

Задачу встраивания и выделений сообщения из другой информации выполняет стегосистема, состоящая из следующих элементов, представленных на рисунке 1 [2].

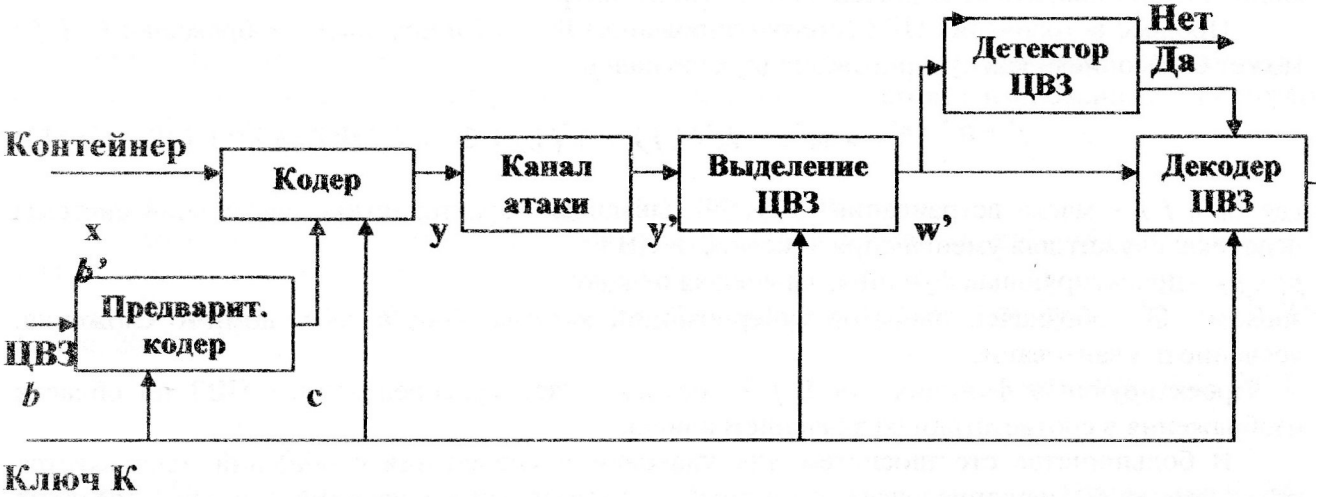

Рис. 1. Структурная схема типичной стегосистемы

- прекодер— устройство, предназначенное для преобразования скрываемого сообщения к виду, удобному для встраивания в контейнер;
- стегокодер — устройство, предназначенное для осуществления вложения скрытого сообщения в другие данные;
- устройство выделения встроенного сообщения;
- стегодетектор — устройство, предназначенное для определения наличия стегосообщения;
- декодер — устройство, восстанавливающее скрытое сообщение.

Сообщение $m \in M$ — это секретная информация, наличие которой необходимо скрыть, $M = \{m_1, m_2, ..., m_n\}$ — множество всех сообщений.

Контейнером $c \in C$ называется несекретная информация, которую можно использовать для скрытия сообщения, $C = \{c_1, c_2, ..., c_q\}$ — множество всех контейнеров,

причем q>>n. В качестве сообщения и контейнера могут выступать как обычный текст, так и файлы мультимедийного формата.

Пусть W^*, K^*, I^*, B^* есть множества возможных ЦВЗ, ключей, контейнеров и скрываемых сообщений, соответственно. Тогда генерация ЦВЗ [1] может быть представлена в виде

$$F: I^* * K^* * B^* \rightarrow W^*, \qquad W = F(I, K, B), \tag{1}$$

где W, K, I, B – представители соответствующих множеств. Функция F обычно является составной:

$$F = T \circ G, \text{ где } G: K^* * B^* \rightarrow C^* \text{ и } T: C^* * I^* \rightarrow W^*, \tag{2}$$

т.е. ЦВЗ зависит от свойств контейнера. Для реализации функции G используется разработанный генератор псевдослучайной последовательности (ПСП), основанный на применении к результатам работы первичного генератора ПСП хэш – функции SHA – 1. Как известно, хэш – функции являются необратимыми функциями, поэтому данный способ повышает криптостойкость ПСП.

Прежде чем осуществить вложение ЦВЗ в контейнер, ЦВЗ должен быть преобразован в подходящий вид. Если в качестве контейнера выступает изображение, то и последовательность ЦВЗ представляется, как двумерный массив бит. Начальную обработку скрываемой информации выполняет прекодер.

Упаковка сообщения в контейнер (с учетом формата данных, представляющих контейнер), выполняется с помощью стеганокодера. Вложение происходит, например, путем модификации наименьших значащих битов контейнера.

Процесс встраивания ЦВЗ (стегокодирование) $W(i, j)$ в исходное изображение $I_0(i, j)$ может быть описан как суперпозиция двух сигналов:

$$\varepsilon: \quad I^* * W^* * L^* \rightarrow I_w^*, \quad I_w^*(i,j) = I_0^*(i,j) \oplus L(i,j)W(i,j)p(i,j) \tag{3}$$

где $L(i, j)$ – маска встраивания ЦВЗ, учитывающая характеристики зрительной системы человека; служит для уменьшения заметности ЦВЗ;
$p(i, j)$ – проектирующая функция, зависящая от ключа;
знаком $\oplus$ обозначен оператор суперпозиции, включающий в себя, помимо сложения, усечение и квантование.

Проектирующая функция $p(i, j)$ осуществляет «распределение» ЦВЗ по области изображения в соответствии со значением ключа.

В большинстве стеганосистем для упаковки и извлечения сообщений используется ключ, который предопределяет секретный алгоритм, определяющий порядок внесения сообщения в контейнер. Скрываемая информация заносится в соответствии с ключом в те биты, модификация которых не приводит к существенным искажениям контейнера. Эти биты образуют, так называемый, стеганопуть.

В стеганодетекторе определяется наличие в контейнере скрытых данных. Различают стеганодетекторы, предназначенные только для обнаружения факта наличия встроенного сообщения, и устройства, предназначенные для выделения этого сообщения из контейнера, — стеганодекодеры.

Для определения ЦВЗ в полученном по открытому каналу связи изображении используется операция детектирования, которую обозначим через D.

$$D: I_w^* * K^* \rightarrow \{0,1\}, \quad D(I_w, W) = D(I_w, F(I_w, K)) = \begin{Bmatrix} 1, если W есть \\ 0, если W нет \end{Bmatrix} \tag{4}$$

Таким образом, разработанный алгоритм содержит следующие этапы:

1. Содержание электронного документа хешируется с помощью хэш-функции SHA-1. Результатом работы хэш-функции является дайджест размером 160 бит.

2. В угловой штамп учреждения, рассмотренный как изображение, встраивается ЦВЗ следующим образом: с помощью генератора псевдослучайных чисел с ключом формируются координаты пикселей, в которые автор скрывает по одному биту хэш-значения электронного документа. Хэш-значение встраивается следующим образом: считаем сумму бит пикселя, если она четная, а нам необходимо скрыть 0, то изменений в цветности пикселя не происходит, если скрываем 1, то меняем наименее значащий бит цветности, и если сумма нечетная, а нам необходимо скрыть 1, то ничего не меняем, если же скрыть 0, то меняем.

3. Получатель электронного документа, имея аналогичный генератор с ключом, определяет координаты пикселей со скрытой информацией и извлекает ее, формируя, таким образом, хэш-значение электронного документа.

Затем, используя хэш-функцию SHA-1, получатель вычисляет хэш-значение и производит сравнение полученных дайджестов. Если результат сравнения положительный, то это свидетельствует о подлинности электронного документа.

К ЦВЗ предъявляются следующие требования:

— ЦВЗ должен легко извлекаться законным пользователем.
— ЦВЗ должен быть устойчивым либо неустойчивым к преднамеренным и случайным воздействиям. Если ЦВЗ используется для подтверждения подлинности, то недопустимое изменение контейнера должно приводить к разрушению ЦВЗ (хрупкий ЦВЗ) [1].

Программное обеспечение разработано в среде *C++Builder*. Его разработка для встраивания ЦВЗ в изображения основана на известном принципе, что безопасность системы должна полностью определяться секретностью ключа и знание нарушителем факта наличия сообщения в каком – либо контейнере не должно помочь ему при обнаружении сообщения в других контейнерах.

Разработанный алгоритм встраивания в документы ЦВЗ позволяет осуществлять контроль целостности электронных документов в автоматизированных системах электронного документооборота.

Список литературы

1. *Хорошко В.А., Чекатков А.А.* Методы и средства защиты информации / Под ред. Ю.С.Ковтанюка – К.: Издательство Юниор, 2003. – 504 с.,

2. *Грибунин В.Г., Оков И.Н., Туринцев И.В.* Цифровая стеганография. – М.: СОЛОН-Пресс, 2002.-272 с.

Поступила 21.12.2006 г.

УДК 621.391:519.2

Игнатенко С. М.

МОДИФИКАЦИЯ МЕТОДА МАКСИМУМА ПРАВДОПОДОБИЯ РЕШЕНИЯ СИСТЕМ ЛИНЕЙНЫХ УРАВНЕНИЙ С ИСКАЖЕННОЙ ПРАВОЙ ЧАСТЬЮ НАД КОЛЬЦОМ ВЫЧЕТОВ ПО МОДУЛЮ 2^N

При декодировании линейных блоковых кодов, применении корреляционных атак на двоичные комбинирующие генераторы гаммы, недвоичные поточные шифры, а также при решении других задач криптографического анализа симметричных криптосистем возникает необходимость решения систем линейных уравнений (СЛУ) с искаженной правой частью (ИПЧ) над кольцом $R = Z/2^N$ [1 – 5].

Как правило, указанная система линейных уравнений имеет вид

$$Ax = b = Ax^{(0)} + \varepsilon, \qquad (1)$$