Краткие сообщения

УДК 681.3.06

Ю.Г. Савченко, д-р техн. наук

Кодирование как инструмент стеганографического сокрытия информационного обмена

Рассмотрен подход к организации скрытого канала передачи информации путем использования кодов с коррекцией ошибок, когда модификация битов контейнера является имитацией воздействия помех в канале. Проведен анализ особенностей информационного обмена. Приведены примеры использования конкретных кодов.

The method of the hidden channel for data transmission organization is observed in this work. This method is based on the use of correction codes with the content bits modification by menace of channel interferences imitation. It is provided the analyses of the information exchange organization and also examples of correction codes use are given.

Ключевые слова: *стеганография, кодирование,сокрытие помехи.*

Введение

Для защиты от несанкционированного доступа к информации в настоящее время наряду с криптографическим шифрованием все более широко используется стеганографическое сокрытие [1, 2]. В условиях воздействия помех в реальных каналах связи практически повсеместно также применяется помехозащищенное кодирование [3]. Такая ситуация достаточно типична, что создает предпосылки для объединения и совмещения процедур кодирования и стеганографической защиты для повышения эффективности информационного обмена с точки зрения пропускной способности скрытого канала и его стойкости к выявлению методами криптоанализа.

В работе [4] предложен подход, при котором модификация битов контейнера имитирует воздействие помех в канале при использовании кодов с коррекцией ошибок для защиты содержимого контейнера. В этом случае загрузка скрытого вложения (СВ) выполняется непосредственно после процедуры кодирования в те биты сообщения, которые задаются генератором псевдослучайных чисел (ГПСЧ). Формально единственное отличие предлагаемого подхода от общепринятого заключается в предварительном внесении в контейнер информационной избыточности для коррекции (обнаружения или исправления) ошибок в передаваемом сообщении.

Цель работы – рассмотрение особенностей процедуры организации скрытого информационного обмена в условиях применения помехозащищенного кодирования содержимого контейнера, а также предварительная оценка предполагаемого эффекта от совмещения стеганографического сокрытия с кодированием.

1. Общая схема организации скрытого информационного обмена

В качестве контейнера рассмотрим цифровой (битовый) поток данных, полученный, например, в результате оцифровки аудио или видеосигналов, значений технологических параметров, сканирования графических материалов и т. п. Будем также предполагать, что исходный поток всегда может быть разбит на отдельные порции (блоки, кадры, пакеты) длиной k бит. Каждый такой блок является миниконтейнером, в который может быть загружена некоторая порция СВ. При использовании метода замены наименее значащего бита (НЗБ) [1] загрузка битов СВ сводится к модификации младших битов каждого или некоторых блоков цифрового потока. Принято считать, что в этом случае для передачи СВ может быть задействовано максимум 10…12 % пропускной способности канала.

В случае предварительного кодирования потока данных каждый блок искусственно удлиняется до n символов путем добавлением $(n-k)$ проверочных разрядов в соответствии с уравнениями кодирования выбранного кода. Наличие такой возможности является необходимым условием реализации рассматриваемого подхода. Совершенно очевидно, что удлинение уже само по себе увеличивает возможности размещения СВ в контейнере. Однако применение кодов с коррекцией ошибок может быть оправдано лишь в случаях достаточно высокого уровня помех, которые могут исказить не только содержимое контейнера, но и СВ. Именно эта особенность требует детального анализа при оценке эффективности предварительного кодирования контейнера.

Очевидно также, что в рассматриваемом случае появляется дополнительная свобода в выборе позиций, в которых могут быть размещены биты СВ. Так, если при использовании метода замены НЗБ допускается модификация лишь младших битов, то после предварительного кодирования могут быть модифицированы любые позиции в пределах корректирующей способности выбранного кода. Этот дополнительный эффект, по крайней мере, потенциально увеличивает стойкость скрытого информационного обмена, поскольку криптоаналитику потребуется произвести существенно больший перебор предполагаемых вариантов размещения СВ.

Важным элементом организации стеганоканала является наличие у получателя СВ информации о конкретном расположении битов вложения в общем битовом потоке. Эта задача, как правило, решается путем синхронизации идентичных ГПСЧ (аппаратных или программных) у отправителя и получателя СВ.

Для контейнеров фиксированного размера рациональным подходом можно считать использование метода псевдослучайной перестановки [5], суть которого состоит в том, что ГПСЧ генерирует последовательность индексов $w_1, w_2, ..., w_n$ и модифицирует *i*-й бит контейнера в бите с номером w_i. В частном случае, когда один бит СВ размещается в одном контейнере длиной n бит, число возможных вариантов размещения равно также n. А для СВ длиной N бит таких вариантов будет Nn. Функция перестановки должна быть псевдослучайной, другими словами, она должна обеспечивать выбор бита контейнера и номер самого контейнера приблизительно случайным образом. В этом случае биты СВ окажутся распределенными равномерно во всем битовом пространстве общего контейнера, состоящего из отдельных блоков.

Чтобы избежать наложения при загрузке контейнера, т. е. повторной загрузки одной и той же позиции в контейнере, ГПСЧ должен генерировать неповторяющуюся последовательность чисел. Этому требованию удовлетворяют генераторы на основе регистров сдвига с обратными связями по модулю два. При правильном выборе полинома, определяющего вид обратных связей, такие схемы генерируют последовательности псевдослучайных чисел максимальной длины с периодом повторения $2^m - 1$, где m – длина регистра. Отметим, что такие схемы широко используются также для выполнения процедур кодирования и декодирования циклических кодов, что создает предпосылки для унификации оборудования при аппаратной реализации рассматриваемого подхода.

Перейдем теперь к главному вопросу: из каких соображений и по каким критериям выбирать используемый при информационном обмене код. И как свойства выбранного кода влияют на основные характеристики стеганоканала: его пропускную способность и стойкость к вскрытию при криптоанализе.

2. Выбор используемых кодов

Сразу же следует отметить, что использование кодов *только с обнаружением ошибок* в схеме, в которой кодирование предшествует загрузке контейнера, не имеет смысла. В этом случае информация об обнаруженных ошибках при декодировании лишь облегчает криптоанализ, а каких-либо дополнительных преимуществ для загрузки по сравнению с методом НЗБ нет. Поэтому сразу же перейдем к кодам с исправлением ошибок [2].

Коды Хемминга с исправлением ошибок кратности $t = 1$ *и минимальным кодовым расстоянием* $d = 3$. В этом случае количество проверочных символов

$$(n - k) \geq \log_2(n + 1).$$

Загрузка бита СВ производится в произвольный разряд миниконтейнера (а не только младшие разряды, как при методе НЗБ). При извлечении СВ используется как информация, полученная в результате стандартной процедуры декодирования (вектор ошибки), так и адрес вложенного бита, полученный от ГПСЧ приемника. В случае совпадения адресов указанный бит извлекается в регистр формирования СВ в целом. При несовпадении производится исправление ошибки в разряде, соответствующем вектору ошибки. Ситуация, когда в результате естественных помех в канале искажается бит СВ, является критической – СВ будет содержать ошибки. Однако вероятность возникновения такой ситуации при реальных значениях n по крайней мере на порядок меньше вероятности возникновения ошибки в одном бите цифрового потока в канале [4].

Пропускная способность стеганоканала в рассматриваемом случае, очевидно, в n раз меньше пропускной способности канала передачи в целом. Эту оценку следует рассматривать как верхнюю границу, поскольку не обязательно все миниконтейнеры должны загружаться битами СВ. Разумеется, применение помехозащищенного кодирования само по себе «съедает» часть пропускной способности канала, что можно оценить соотношением $\frac{n - k}{n}$. Однако при высоком уровне помех в канале избежать этих потерь не представляется возможным.

Коды Хемминга с исправлением однократных и обнаружением двукратных ошибок и минимальным кодовым расстоянием $d = 4$. Количество проверочных символов

$$(n-k) \geq \log_2 n + 1.$$

Пропускная способность стеганоканала в таком варианте несколько меньше и может быть оценена как соответствующая часть пропускной способности канала в целом. Приведенная ниже таблица иллюстрирует затраты пропускной способности на коррекцию ошибок и часть этой пропускной способности, которая может быть использована для передачи СВ.

Таблица 1

$n-k$	4	5	6	7	8	…	11	…
n	8	16	32	64	128	…	1024	…

Из практических соображений естественно перейти к использованию более мощных кодов с большей корректирующей способностью. Среди таких кодов в первую очередь заслуживают внимания *коды Боуза-Чоудхури-Хоквингема (БЧХ-коды).* Эти коды допускают простую аппаратную реализацию на регистрах сдвига с обратными связями по модулю два, кроме того, имеется большое разнообразие разработанных вариантов реализации для разных значений длины блока и кратности исправляемых ошибок. При длине блока n и кратности исправляемых ошибок t необходимое число проверочных символов определяется неравенством

$$(n-k) > \sum_{i=1}^{t} C^i{}_n,$$

где $C_n^{\,i}$ – комбинаторное число возможных ошибок кратности i в n-разрядном двоичном слове.

Например, (31,21)-БЧХ-код, порождаемый полиномом

$$P(x) = x^{10} \oplus x^9 \oplus x^8 \oplus x^6 \oplus x^5 \oplus x^3 \oplus 1,$$

исправляет 31 однократную и 465 двукратных ошибок. При умеренном уровне помех в канале такая корректирующая способность используемого кода позволяет надежно защитить контейнер в целом (включая СВ) от ошибок, вызванных естественными помехами, а также создает хорошие условия для размещения битов СВ в цифровом потоке. Однако пропускная способность стеганоканала в этом случае несколько снижается за счет увеличения уровня информационной избыточности.

При выборе кода в рассмотренной схеме информационного обмена главным критерием остается, очевидно, требуемая достоверность передачи, которая, в свою очередь, зависит от уровня помех в канале. Иными словами, используемый код должен, как минимум, обеспечить коррекцию ошибок, возникающих в результате воздействия помех, и создать условия для размещения СВ. Поэтому выбираемый код должен иметь некоторый «запас» корректирующей способности по сравнению с традиционным использованием помехозащищенных кодов.

Выводы

Решая в целом проблему защиты от несанкционированого доступа к информации, использование кодов с коррекцией ошибок является желательным как при шифровании (криптографической защите), так и при стеганографическом сокрытии. В первом случае это объясняется чувствительностью практически всех стандартов шифрования к искажению даже одиночных битов в сообщении, во втором – улучшением условий загрузки контейнера. Принимая в качестве исходной ситуацию, при которой помехозащищенное кодирование контейнера уже применяется (независимо от того, будет ли он задействован для загрузки или нет) может быть достигнуто некоторое увеличение пропускной способности стеганоканала и улучшена безопасность обмена именно за счет предварительного кодирования контейнера.

Литература

1. *Грибунин В.Г.,* Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-Пресс, 2002. – 272 с.
2. *Конахович Г.Ф.,* Пузиренко О.Ю. Комп'ютерна стеганографія. Теорія і практика. – К.: МК-прес, 2006. − 288 с.
3. *Касами Т.,* Токура Н., Ивадари Ё., Инагаки Я. Теория кодирования. – М.: Мир, 1978. − 576 с.
4. *Савченко Ю.Г.,* Сажина И.А. Организация скрытого информационного обмена в режиме реального времени // Наукові записки УНДІЗ. – 2010. – №1(13). – С. 57–62.
5. *Aura T.* Practical Invisibility In Digital Communication // Information Hiding: First Internationfl Workshop "InfoHiding96", Springer as Lecture Notes in Computing Science. – 1996. – vol. 1174. – P. 265–278.

Национальный технический университет Украины «Киевский политехнический институт»

Поступила в редакцию 22 декабря 2009 г.