УДК 004.056

С.С. Бондарчук, Е.М. Давыдова, Е.Ю. Костюченко

Встраивание цифровых знаков для обеспечения защиты информации

Объектом работы являются алгоритмы и методы сокрытия информации в текстовых файлах. Предложены элементы лингвистического встраивания цифровых знаков для повышения уровня информационной безопасности передаваемой информации.

Ключевые слова: стеганография, алгоритмы, сокрытие информации, секретная передача сообщений, быстродействие, текстовые файлы.

Задача надежной защиты информации от несанкционированного доступа является одной из древнейших и не решенных до настоящего времени проблем. Процесс стеганографии можно разделить на несколько этапов.

Первым этапом в процессе стеганографии является выбор файла, который необходимо скрыть. Его ещё называют информационным файлом.

Вторым этапом в процессе стеганографии является выбор файла, используемый для сокрытия информации. Его ещё называют файлом-контейнером. В большинстве известных программ по стеганографии говорится, что для сокрытия информации объём памяти файла-контейнера должен примерно в восемь раз превышать объём памяти информационного файла [1]. Следовательно, чтобы спрятать файл размером 710 кб, понадобится графический файл объёмом 5600 кб. Но если коснуться методов сокрытия информации в тексте, то становится видно, что объём памяти файла-контейнера должен в 50–200 раз превышать объём памяти информационного файла [1].

Третьим этапом в процессе стеганографии является выбор программы, проводящей стеганографические преобразования.

После того как выбраны информационный файл, файл-контейнер и программное обеспечение для проведения стеганографии, необходимо установить защиту нового файла с использованием парольной защиты.

Пятым и последним этапом в процессе стеганографии являются отправление спрятанного файла по электронной почте и его последующая расшифровка.

При построении стегосистемы должны учитываться следующие положения:

– противник имеет полное представление о стеганографической системе и деталях ее реализации. Единственной информацией, которая остается неизвестной потенциальному противнику, является ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения;

– если противник каким-то образом узнает о факте существования скрытого сообщения, это не должно позволить ему извлечь подобные сообщения в других данных до тех пор, пока ключ хранится в тайне;

– потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений [1].

Обобщенная модель стегосистемы представлена на рис. 1.

В качестве данных может использоваться любая информация: текст, сообщение, изображение, звуковой или какой-либо другой файл. В общем случае целесообразно использовать слово «сообщение», так как сообщением может быть как текст или изображение, так и, например, аудиоданные. Далее для обозначения скрываемой информации будем использовать именно термин «сообщение».

При реализации системы стеганографического сокрытия информации был обнаружен ряд специфических особенностей данной системы. Для решения некоторых задач в процессе разработки был реализован ряд основных функций и процедур, необходимых для работы системы.

Функция преобразования битовой последовательности в символ ASCII

Входом в данную функцию служит строковая последовательность из восьми символов (например, 011011011). Далее начиная с более весомого бита, проверяется значение (0 или 1) и в соответствии с этим значением вычисляется порядковый номер символа в ASCII таблице. Перед заверше-

нием работы функции значению функции присваивается символ таблицы и результат работы функции передаётся в основную программу, где впоследствии происходит запись этого извлечённого символа в выходной файл.

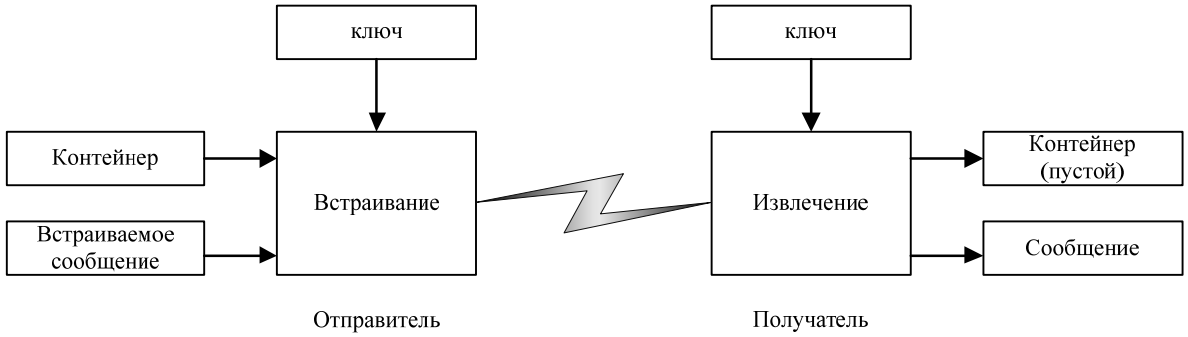

Рис. 1. Обобщенная модель стегосистемы

Входом в данную функцию служит код символа из ASCII-таблицы, который преобразовывается в битовую последовательность длиной в восемь символов и в таком виде передаётся в основную программу.

Процедура удаления лишних пробелов из файла-контейнера

Данная процедура предназначена для удаления лишних пробелов из файла-контейнера. Процедура открывает входной файл, посимвольно его анализирует, и если количество пробелов больше одного, лишние пробелы удаляются. Использование данной функции необходимо в стеганографических методах сокрытия информации в текстовых документах при использовании избыточного форматирования документов.

Процедура получения значения активного бита

Данная процедура при обращении к ней возвращает значение бита (0 или 1), который необходимо встроить. Если предыдущий символ из стегосообщения полностью встроен, производится считывание следующего символа, затем возвращение значения активного бита. Если стегосообщение встроено полностью, то значение активного бита всегда приравнивается равным нулю и считывание из файла-сообщения больше не производится.

Процедура встраивания/извлечения стегосообщения

В данной процедуре осуществляется определение вида заданного пользователем действия (встраивание или извлечение стегосообщения). Если выбрано встраивание, то три файла: файл-контейнер, файл-сообщение и файл-результат – связываются с файловыми переменными и вызывается процедура встраивания стегосообщения. Если выбрана операция извлечения стегосообщения, то файл-носитель сообщения и файл-результат извлечённого сообщения связываются с файловыми переменными, после этого вызывается процедура извлечения секретного послания. Имена файла-контейнера и файла-результата могут совпадать.

Описание работы системы

Два метода синонимического перефразирования в лингвистической стеганографии

Лингвистическая стеганография (ЛС) скрывает один текст в другом, опираясь на свойства языка и лингвистические ресурсы. Для целей ЛС предлагается два метода синонимического перефразирования текста-носителя. Метод синонимических замен заменяет отдельные слова текста их синонимами. Абсолютные синонимы используются независимо от контекста, а относительные проверяются на совместимость заменяющего слова с контекстными словосочетаниями. Словосочетания – это синтаксически связанные и семантически совместимые пары полнозначных слов. Они собираются заранее в обширную базу словосочетаний, с которой взаимодействует словарь синонимов. Метод синонимических перестановок упрощенно анализирует предложения несущего текста, выявляя в них составляющие верхнего синтаксического уровня. Из заранее составленного словаря допустимых перестановок составляющих берется та, что соответствует шифруемой информации. Обеспечиваемая стенографическая плотность для обоих методов равна примерно 1/200. Методы независимы и совместны, а при совмещении их показатели суммируются [2].

В ЛС используются словари квазисинонимов. Лексика разбивается на множество групп разного объема. Внутри групп слова сходны как грамматически, принадлежа одной части речи, так и семан-

тически, вплоть до настоящей синонимии. Если очередное слово несущего текста принадлежит группе с $m > 1$ синонимами, оно может нести скрытую информацию.

Пусть размеры всех полученных групп кратны степени двойки или сокращены до ближайшей степени двойки. Тогда для каждой группы размера $2n$ из кодируемого сообщения выделяется слог длины n и его двоичное содержимое берется в качестве внутригруппового номера синонима, подставляемого в текст вместо исходного. Операция на приемном конце очевидна. Но при крупных группах ничем не ограниченные замены делают носитель невразумительным.

В предлагаемых методах тоже используется синонимическое перефразирование, но разного типа. Феномен синонимии очень важен в лингвистике. Так, теория «Смысл <=> Текст» считается исчислением синонимических перифразов. В ней предложена сложная совокупность преобразований, сохраняющих смысл предложения и дискуса в целом. В зависимости от того, на каком уровне языка ведется перефразирование, в его процессе меняются лексика, синтаксическая структура, морфологические характеристики слов, их число и порядок. Однако программное воплощение теории пока затронуло немногое в языке.

Согласно методу замен производятся синонимические замены, сохраняющие порядок слов, синтаксическую структуру предложения и приблизительно число слов в нем. Производимые замены тестируются относительно контекста: проверяется, входит ли заменяющее слово в набор словосочетаний заменяемого слова. Только если данная замена контекстно допустима, соответствующий синоним оставляется в группе потенциальных замен. Конкретная замена определяется кодируемой информацией. Словосочетания – это синтаксически связанные и семантически совместимые пары полнозначных слов, например: правильно выразить, передать по радио, глава государства. Предполагается, что измеряемые сотнями тысяч словосочетания произвольной частотности и идиоматичности собраны заранее в некую базу, где синонимы ищутся как компоненты словосочетаний.

Согласно методу перестановок делаются синонимические перестановки составляющих предложения. Для выделения составляющих верхнего синтаксического уровня (например, обстоятельств времени и места) использует упрощенный синтаксический анализ. Далее по заранее составленному словарю допустимых перестановок выявляется, какие перестановки допустимы для данного набора составляющих, и берется по номеру соответствующая кодируемой информации.

Методы могут применяться независимо и совместно, сохраняют исходный смысл текста, а обеспечиваемые ими показатели плотности кодирования при совмещении складываются.

Абсолютные и относительные синонимы

Синонимы – это слова, могущие замещать друг друга в некотором классе контекстов с незначительным изменением смысла полного текста. Обороты с «некоторый» и «незначительный» делают данное определение нечетким, но синонимические словари продолжают строиться на его основе. Типичный синонимический словарь состоит из групп слов, считающихся синонимами друг другу. Обычно выделяют титульное слово группы (доминанту), выражающее смысл группы наиболее общим и нейтральным способом. Каждое слово синонимической группы может иметь смысловое сходство и с иной группой, даже быть в нее включенным, т.е. группы могут пересекаться.

Не стоит ограничиваться лишь однословными синонимами, подходят даже группы без единого однословного члена: {надеяться, возлагать надежды, питать надежду}, {наконец, в конечном счете, в конце концов}, {в течение нескольких дней, за несколько дней } и т.п. Очень важна абсолютная синонимия. Она не меняет смысла текста при любых контекстах (лингвистика = языкознание). К сожалению, абсолютные синонимы редки, но много эквивалентов иного рода – различных сокращений. Вот группа эквивалентов: {Соединенные Штаты Америки, Соединенные Штаты, США}. Многословные синонимы привносят их множество: {экс-президент, бывший президент}, {замминистра, заместитель министра}. В языке интернетовских новостей используется несколько тысяч склеек типа детсад = детский сад, сейсмостанция = сейсмическая станция, физлица = физические лица. Есть еще так называемые морфологические варианты типа {нуль, ноль}. Будем относить всех их к абсолютным синонимам.

Неабсолютные синонимы назовем относительными. Как средство отличения абсолютных синонимов, один из них берем доминантой, а прочие снабжаем пометой. Итак, предполагается обширный синонимический словарь, где:

– каждая группа имеет доминанту;

– эквиваленты доминанты, если они есть, помечены;

– любой член группы может состоять из несколько слов;

– любой член группы может повторяться в иной группе и/или быть омонимом члена другой группы;

– члены группы могут характеризовать не полную лексему, а ее граммему, т.е. отдельно единственное и множественное число существительного, отдельно личные формы глагола + инфинитив, причастия и деепричастия, да еще и разделенные на совершенный и несовершенный вид.

База словосочетаний и дополнения к ней

Словосочетания соединяют слова синтагматически, например: глагол и валентное ему существительное или существительное и определяющее его прилагательное. В русском языке словосочетания всегда брались в данном понимании. В рамках теории «Смысл <=> Текст» они получили адекватное описание и классификацию. Семантически они делятся на фраземы (их полный смысл не включает прямой смысл компонентов); полуфраземы (содержат прямой смысл только одного компонента) и свободные сочетания (смысл составлен только из смыслов компонентов).

В 1990–2003 гг. была разработана интерактивная система КроссЛексика, в базе которой содержится ныне более 1,2 млн русских словосочетаний разной частотности и идиоматичности – фразем, полуфразем и свободных словосочетаний. Статистика показала, что свободные словосочетания не столь уж свободны: они возможны только между словами фиксированных семантических полей, и в целом их больше, чем фразем и полуфразем вместе взятых, лишь раз в пять. Именно свободные словосочетания обеспечивают подобным базам широкое применение для создания гибкого и идиоматичного текста, совершенствования синтаксического анализа, разрешения омонимии, обнаружения и исправления семантических ошибок, синонимического перефразирования и пр. Примерно 94% словосочетаний в КроссЛексике оказались следующими: существительное / глагол / прилагательное / наречие – его модификатор (прилагательное или наречияе) (запутанный сюжет, правильно выразить, практически незаметный); глагол – его подлежащее (сушествует противоречие); глагол – его дополнение или предложное обстоятельство (дать воды, передать по радио); существительное – его дополнение (глава государства). В качестве компонентов словосочетаний берутся не лексемы целиком, а их морфологические подпарадигмы, называемые граммемами. Это обстоятельство требует пояснения.

Было известно, что существительное в единственном и множественном числе может иметь разные наборы словосочетаний. Поэтому граммемы двух чисел взяты разными единицами словаря. Глаголы играют разные синтаксические роли: сказуемого (в личных формах), определения (в форме причастия), обстоятельства (в форме деепричастия) и имеют словосочетания разных типов.

Поэтому рассматриваются раздельно все личные формы + инфинитив, причастие (походит на прилагательное) и деепричастие (походит на наречие). Дополнительное членение производится и по признаку вида глагола. Синонимический словарь оперирует теми же граммемами, что и база словосочетаний.

Множество словосочетаний вне базы можно получить эвристическим «выводом». Так, в базе имеются словосочетания о цветах вообще {купить цветов, украсить цветами,...}, и известно, что розы являются подвидом цветов. Поэтому можно «вывести» словосочетания {купить роз, украсить розами, ...}.

Метод синонимических замен

Входами в предлагаемый метод служат двоичная информация, предназначенная для шифровки, и несущий текст на русском языке, по объему примерно в 200 раз больший, чем у шифруемой информации. Формат текста произволен, но он орфографически и синтаксически правилен, дабы не спровоцировать исправлений при передаче. Последовательности цифр или личных имен допускаются, но они увеличивают требуемую длину текста. Алгоритм включает следующие шаги.

Поиск синонимичных слов. В тексте отыскиваются слова и многословные выражения, имеющие синонимы. Если одновременно найдена последовательность слов и ее подпоследовательность, предпочтение отдается объемлющей.

Формирование объединенных синонимических групп. Последовательно рассматриваются синонимичные слова текста. Если в соответствующей синонимической группе есть только абсолютные синонимы, она принимается безоговорочно. Если в группе есть хоть один относительный синоним, все такие синонимы подвергаются операции транзитивного замыкания. При замыкании для каждого синонима проверяется, не является ли он членом какой-либо иной синонимической группы. Если это так, дополнительная группа присоединяется к исходной без повторов. Далее присоединенные синонимы просматриваются на принадлежность к иным, еще не рассмотренным синонимическим

группам, и так до исчерпания пополнений. Замыкание совершается также через омонимы. Анализируется, не является ли омонимичным исходное текстовое слово или какой-нибудь член его синонимической группы. Если это так, и если еще не рассмотренный омоним имеет синонимы, привлекается группа синонимов этого омонима. Каждая вновь привлеченная группа используется для расширения и т.д. Процесс конечен, но иногда дает обширную объединенную группу. Транзитивное замыкание необходимо, поскольку делает состав объединенной группы не зависящим от того, с какого члена замыкание начинается.

Проверка словосочетаний. Если группа содержит только абсолютные синонимы, она не проверяется на контекст, а для проверки на сочетаемость с ней иных слов может браться любой ее член. Если же группа имеет относительные синонимы *si*, они подлежат проверке на совместимость с внешними полнозначными словами *wj* слева и справа от проверяемой группы. Если внешнее слово *wj* не синонимично или имеет только абсолютные синонимы, то проверяется, с какими из *si* оно образует однотипные словосочетания. Те *si*, которые не формируют словосочетания с *wj*, отбрасываются. Если внешнее слово *wj* само принадлежит объединенной группе с элементами *wjk*, то проверяются все однотипные словосочетания пар {*wjk*, *si*} при всех *i* и *k*. Отсутствие словосочетания хотя бы с одним внешним элементом ведет к отбрасыванию проверяемого элемента. При этом разных пар может не остаться и тогда группа в стеганографии не участвует. Элементы, оставшиеся в группе, нумеруются фиксированным образом от 0 до $m - 1$, где m – число оставшихся элементов.

Кодирование. Последовательность профильтрованных групп сканируется. Если их размеры кратны степени двойки или сокращены до ближайшей степени двойки, для очередной группы длиной $2n$ из кодируемого сообщения выделяется слог длины n и его двоичное содержимое берется в качестве внутригруппового номера синонима, подставляемого в текст вместо исходного. Та же операция повторяется для всех групп вдоль текста. Если имеются группы, по длине не равные степени двойки, все длины групп перемножаются и берется степень $2N$, ближайшая к полученному произведению вниз. Затем от кодируемой информации отсекается слог длины N и из него путем последовательных делений и нахождений остатков находятся номера омонимов для замены синонимичных слов в тексте. Если текстовый синоним при кодировании оказался замененным, то в общем случае пересогласуются морфосинтаксические характеристики заменителя и контекста.

Пример, протрассированный вручную.

Возьмем типичный текстовой фрагмент из потока новостей Газета.Ру:

1. Пять подземных толчков зарегистрировано за сутки на юге Республики Алтай. Сила землетрясений составляла от 2,2 до 3,1 балла по шкале Рихтера, сообщили на Акташской сейсмической станции сегодня после полудня.

Здесь синонимичные слова или цепочки слов подчеркнуты, а абсолютные синонимы выделены еще и шрифтом.

Вот группы абсолютных синонимов (они упорядочены по алфавиту и двоично пронумерованы):

0. землетрясения	1. подземные толчки
0. за 24 часа	1. за сутки
0. сейсмическая станция	1. сейсмостанция

При транзитивном замыкании синонима *зарегистрированный* выявляются синонимические группы с доминантами *зарегистрированный, закрепленный, помеченный, отпразднованный* и объединенная группа содержит: *закрепленный, замеченный, зафиксированный, зарегистрированный, отмеченный, отпразднованный, подмеченный, помеченный, прикрепленный, примеченный*.

А вот группы относительных синонимов в тексте, транзитивным замыканием не изменяемые:

0. Алтай	1. Республика Алтай
0. равняться	1. составлять
0. проинформировать	1. сообщить
0. во вторую половину дня	1. после полудня

Существительное сила имеет два омонима, каждый со своим набором синонимов:

00. магнитуда	01. мощность	10. мощь	11. сила	1
0. действенность	1. сила			2

Отфильтруем теперь относительные синонимы, не отвечающие контексту. Абсолютный синоним землетрясения образует словосочетания с замеченный, зарегистрированный, зафиксированный и отмеченный, остальные члены группы (2) отбрасываются. Все оставшиеся члены сочетаются с абсолютным синонимом за сутки и с несинонимичным словом юг. В итоге (2) принимает вид

00. замеченный 01. зарегистрированный 10. зафиксированный 11. отмеченный

Из групп сила только синонимы сила1 удовлетворяют контексту. У сейсмическая станция эквивалентного сейсмостанция, нет словосочетаний в базе, но их имеет родовое понятие станция, так что выводим: (сейсмостанция IS_A станция) & (сообщить на станцию) →» (сообщить на сейсмостанцию). Группы сообщить / проинформировать и после полудня / во вторую половину дня полностью сочетаемы и поэтому способны полностью сохранить свой состав.

В целом синонимы в (1) позволяют закодировать 12 бит информации, например, две латинские буквы с кодами в виде правых 6-битовых слогов таблицы ASCII. Так, биграмма no соответствует безупречному варианту (вносимые отличия выделены):

Пять подземных толчков зарегистрировано за сутки на юге Республики Алтай. Мощность землетрясений составляла от 2,2 до 3,1 балла по шкале Рихтера, сообщили на Акташской сейсмостанции сегодня после полудня.

Поскольку объем скрытой информации 1,5 байт, а текста – 206 байт, первый составляет 1/135 последнего. Это стеганографическая плотность. Она невелика, но в многокилобайтном тексте можно скрыть нечто вполне содержательное.

Метод синонимических перестановок

Заголовок из новостей Газета.Ру:

1. [В Иране]L [во вторник]T [произошло]V [новое землетрясение]S

Набор составляющих верхнего синтаксического уровня типичен: обстоятельство места L, обстоятельство времени T, сказуемое V и подлежащее S. Если перебрать все 4! = 24 перестановки, то еще три, TLVS, SVTL, TVSL, оказываются вполне эквивалентными (3); 10 цепочек передают тот же смысл, но с иным намерением высказывания (напр., Новое землетрясение в Иране произошло во вторник); еще 10 цепочек недопустимы – вообще или в жанре новостей (напр., Произошло во вторник в Иране новое землетрясение). Объединим четыре безупречных варианта в группу синонимических перестановок, предположительно верных для всех предложений состава {S, V, L, T}, и поместим их в специальный словарь. При стеганографии предлагается анализировать каждое предложение на подобные составляющие и при выявлении указанного состава отсекать от шифруемой информации двухбитовый слог и брать его содержимое в качестве внутригруппового номера перестановки, осуществляемой в тесте-носителе. Поскольку текст (3) содержит 48 байт, в примере достигается тогда стеганографическая плотность 1/192, но обычно на примерах получается меньше.

Теперь следует дать пояснения и обобщения. Иное намерение высказываний именуется в теоретической лингвистике иным тема-рематическим членением предложения. Пока ещё рано истолковывать дескриптивные результаты в прикладном смысле и следует действовать эмпирически. Для более полного учета перестановок в произвольных предложениях новостей необходимо учитывать также два дополнения и обстоятельство цели/причины (из-за мороза, в результате оползня и т.п.). Если потребовать, чтобы данная составляющая в предложении не повторялась и никогда не распадалась на две других, нужно еще делить составные сказуемые (намерен | предъявить), а обстоятельства места разбивать на географические (в Иране), локальные (в аквапарке) и смешанные (в московской больнице). В итоге достаточно примерно десяти классов составляющих и менее сотни их сочетаний в качестве групп словаря перестановок. К выбору допустимых перестановок можно подойти гибче. Оценим в 5 баллов цепочки, появляющиеся в тексте, в 4 балла – полностью им эквивалентные и в 3 балла – отличные по намерению. Наберем соответствующую статистику баллов по группам одинакового состава (но не порядка!), напр., в виде LTVS – 4,57; TLVS – 4,14; SVTL – 4,00; SVLT – 3,28. Если установить порог допустимости для всех групп в 3,2, то в данную группу войдет уже пять членов и в ней можно будет закодировать больше информации. Балансирование идет между увеличенной стеганографической плотностью и возможным появлением неверных перестановок, способных привести к появлениям различий между исходным и модернизированным текстом.

Методы, использующие изменения форматирования документов

– Метод выравнивания пробелами – суть данного метода состоит в раздвижке строки путем увеличения пробелов между словами, когда один пробел соответствует, например, биту 0, два пробела – биту 1. Однако прямое его применение хотя и возможно, но на практике порождает массу неудобств, в частности, оформление текста становится неряшливым, что позволяет легко заподозрить в нем наличие стегонаграммы.

– Метод хвостовых пробелов предполагает дописывание в конце коротких строк (менее 225 символов; значение 225 выбрано достаточно произвольно) от 0 до 15 пробелов, кодирующих значение полубайта.

– Метод знаков одинакового начертания предполагает подмену (бит 1) или отказ от такой подмены (бит 0) русского символа латинским того же начертания.

– Метод двоичных нулей является разновидностью метода знаков одинакового начертания и предполагает либо замену первого в группе из двух или более внутренних пробелов двоичным нулем (бит 1), либо отказ от нее (бит 0) [1].

Анализ реализации методов

Эффективность описанных методов упаковки стегосообщения в контейнере была исследована на переведенном в ASCII-вид тексте главы VI тома I книги «Мертвая вода» объемом 126 729 байт и насчитывающим 2143 строки со строками, выровненными на 65-символьную границу при абзацном отступе в четыре символа [1]. Полученная плотность упаковки (в порядке возрастания) представлена в следующей таблице.

Плотность упаковки

Метод	Знаков стегосообщения	Плотность, %
Чередование маркеров конца	267	0,21
Выравнивание пробелами	411	0,32
Двоичные нули	740	0,58
Хвостовые пробелы	1071	0,85
Знаки одинакового начертания	4065	3,21

Обращает на себя внимание необычно высокая эффективность упаковки стегосообщения с использованием метода подмены символов одинакового начертания.

Полученные данные являются лишь оценочными и зависят не только от свойств контейнера, но и от свойств помещаемого в него стегосообщения, хотя и в меньшей степени.

Число автоматических методов текстовой стеганографии, естественно, не ограничивается рассмотренными примерами. Пополнить запас примеров можно, в частности, разумной комбинацией уже приведенных.

Заключение

К данной работе была разработана и реализована система встраивания цифровых водяных знаков в электронные текстовые документы. Система позволяет скрывать сообщения в текстовых документах, а также производить шифрование/дешифрование скрываемых стегосообщений и другой текстовой информации. Работа системы основана на использовании различных способов переформатирования текстовых документов и использования избытка лингвистических ресурсов русского языка. В дальнейшем планируется развитие системы в направлении обработки естественного языка [3].

Литература

1. Компьютерная стеганография – защита информации или инструмент преступления? [Электронный ресурс]. – Режим доступа: http://www.crime-research.org/library/Steganos.htm, свободный (дата обращения: 20.12.2011).

2. Лингвистическая стеганография [Электронный ресурс]. – Режим доступа: http://www.citforum.ru, свободный (дата обращения: 20.12.2011).

3. Мещеряков Р.В. Структура систем синтеза и распознавания речи // Известия ТПУ. – 2009. – Т. 315, № 5. – С. 121–126.

Бондарчук Сергей Сергеевич
Д-р техн. наук, профессор Томского государственного педагогического университета
Тел.: (382-2) 41-34-26
Эл. почта: isbi@mail.ru

Давыдова Елена Михайловна
Канд. техн. наук, доцент, зам. зав. каф.
комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Тел.: (382-2) 41-34-26
Эл. почта: dem@keva.tusur.ru

Костюченко Евгений Юрьевич
Канд. техн. наук, доцент каф. КИБЭВС ТУСУРа
Тел.: (382-2) 41-34-26
Эл. почта: key@keva.tusur.ru

Bondarchuk S.S., Davidova E.M., Kustyuchenko E.U.
Integration of digital characters for information security

The objects of the research are algorithms and methods for hiding information in text files. We propose to use the elements of linguistic integration of digital characters to increase the security level of transmitted information.
Keywords: steganography algorithms, information hiding, performance, text files.