

УДК 004.056.55

Д.С. Сипаков, Н.Е. Губенко

Донецкий национальный технический университет, г. Донецк
кафедра компьютерных систем мониторинга

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ЛИНГВИСТИЧЕСКОЙ СТЕГАНОГРАФИИ

Аннотация

Сипаков Д.С., Губенко Н.Е. Сравнительный анализ методов лингвистической стеганографии. Были проведены исследования методов лингвистической стеганографии, с целью определения достоинств и недостатков, а так же для определения наиболее качественного метода.

***Ключевые слова:** стеганография, лингвистика, защита данных.*

Постановка проблемы.

Развитие информационных технологий и IT индустрии в целом повлекло за собой возникновения ряда проблем связанных с предоставлением и обработкой информации. Одной из самых актуальных на сегодняшний день является проблема защиты информации. Для обеспечения защиты информации при передаче ее между сотрудниками или отделами используются стеганографические алгоритмы. Сейчас популярность набирает так называемая лингвистическая стеганография — скрывает сообщение, изменяя параметры элементов, из которых состоит носитель или, создавая новый носитель таким образом, чтобы он содержал передаваемое сообщение. Другими словами, целью лингвистической стеганографии является скрытие факта передачи информации, а также ее шифрование.

Цель статьи.

Выполнить сравнительный анализ методов лингвистической стеганографии, выявить достоинства и недостатки исследуемых методов.

Решение задач и результаты исследований.

Для проведения сравнительного анализа были выбраны следующие методы лингвистической стеганографии: семаграмма, фонетика, жаргон, скрытое кодирование. Для каждого метода были установлены достоинства и недостатки.

1 Семаграмма

Семаграмма – скрытие информации с помощью знаков или символов. Например, знак рукой, головой, определенная последовательность чисел или слов, все это семаграммы. Такие знаки не бросаются в глаза, и не заметны для стороннего человека. Иногда использование визуальных семаграмм – единственный способ связи с друзьями и коллегами.



Рисунок 1 — Схема семаграммы

Текстовые семаграммы – это послания, скрытые внутри текста. Заглавные буквы, подчеркивания, особенности почерка, пробелы между буквами и словами – все они могут быть использованы для передачи какого-либо сообщения.

Достоинства:

- незаметно для сторонних лиц;
- простота реализации.

Недостатки:

- из-за простоты реализации, достаточно легко можно получить скрытую информацию.

2 Фонетика

Данный способ можно применить, если точно знать на какой язык запрограммирован фильтр, который "отлавливает" слова на том языке, который преимущественно используют жители страны. Иногда (вдобавок) и на том языке, который сильно распространен или используется на веб-сайтах (английский, французский). Конечно, нельзя с уверенностью сказать, как в

точности запрограммирован фильтр. Но чтобы приблизиться к пониманию, можно использовать фонетически схожие слова. Этот способ наиболее подходит, если вы используете алфавит, отличный от принятого в вашей стране (например, латинский вместо русского)[3].

политзаключенный politzaklyutchenny

Рисунок 2 — Пример фонетики

Достоинства:

- простота реализации.

Недостатки:

- легко получить скрытую информацию;
- фактически информация не скрывается.

3 Жаргон

Использование жаргонов в тексте может озадачить постороннего читателя. Более того жаргонные слова могут быть придуманы членами переписки. Для реализации данного метода создается база данных слов и соответствующих жаргонов, при скрытии слова заменяются. Получатель, должен обязательно знать использованные жаргонизмы что бы понять текст сообщения. Лучше выбирать такие слова, которые сохраняют текст-"носитель" в понятном, читаемом виде, даже если воспринимать жаргонизмы "как есть"[3].

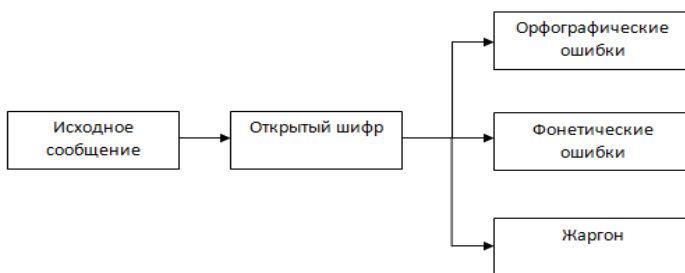


Рисунок 3 — Схема метода жаргонов

Достоинства:

- простота реализации;
- если сохранять текст в читаемом виде, не возникнет подозрений о наличии скрытой информации.

Недостатки:

- перечень слов ограничен участниками переписки;
- получатель должен знать жаргоны;
- при неудачном использовании жаргонов, злоумышленник может догадаться и понять скрытый смысл сообщения.

4 Скрытое кодирование

Частный случай лингвистической стеганографии, наиболее сложен в реализации, однако обеспечивает высокую скрытность информации. В данном методе используется специальная функция, которая шифрует и дешифрует сообщение для передачи. Используется так называемый «контейнер», в который помещается скрываемое сообщение, при получении определенным алгоритмом сообщения достается из «контейнера».



Рисунок 4 — Общая схема передачи скрытого сообщения

Достоинства:

- при наличии программы шифрования дешифрования, получателю не обязательно знать алгоритм скрытия информации;
- крепкая стойкость к дешифрованию;

- тяжело понять, что сообщение-шифр имеет скрытый подтекст.

Недостатки:

- сложность реализации;
- при генерации текста «сообщения-контейнера» тяжело получить читаемый вид передаваемого сообщения.

После проведения анализа исследуемых методов стеганографии, была составлена таблица сравнения.

Таблица 1 — Сравнительная таблица методов стеганографии

Наличие достоинства/недостатка	Метод лингвистической стеганографии			
	Семаграмма	Фонетика	Жаргон	Скрытое кодирование
Сложность реализации	-	-	-	+
Легкость определения наличия зашифрованного сообщения	-	+	-	-
Легкость дешифрования сообщения	+	+	+	-
Искусственные ограничения (например: запас слов у отправителя и получателя, или другие условности между ними)	+	+	+	-

Анализируя таблицу 1, можно сделать вывод, что наиболее качественным методом стеганографии является скрытое кодирование. Данный метод гарантирует полное скрытие самого факта передачи сообщения, не имеет ограничений, однако он же является самым сложным в реализации.

Выводы

Таким образом, при проведении исследований было выяснено, что наиболее стойким методом лингвистической стеганографии является скрытое кодирование. Данный метод имеет сложную реализацию, которая связана с генерированием слов с помощью определенной функции, однако именно данный метод маскирует сам факт передачи скрытого сообщения и получить это сообщение без определенного ключа (функции) практически невозможно. Поэтому целесообразно тратить усилия на реализацию именно этого метода.

Список литературы

1. Life-Prog [Электронный ресурс] – Режим доступа: http://www.life-prog.ru/1_6417_aktualnost-problemi-zashchiti-informatsii.html
2. Википедия [Электронный ресурс] – Режим доступа: <https://ru.wikipedia.org/wiki/Стеганография>
3. Digital Security [Электронный ресурс] – Режим доступа: https://equalit.ie/eseaman/russian/chapter2_8.html
4. Википедия [Электронный ресурс] – Режим доступа: <https://ru.wikipedia.org/wiki/Жаргон>