чения в систему прогнозирования и анализа ЧС в зависимости от текущей обстановки.

Развивая и дополняя интеллектуальные системы прогнозирования ЧС на основе применения технологий визуализации объектов трехмерной графики в таких средах как Unity, которые вносят элементы виртуальной реальности, процессы принятия решений в ЧС становятся более наглядными и эффективными. Программная реализация алгоритмов изменения окружающей обстановки, изменения всех ее факторов во времени и пространстве, включая изменения почвы, рост растительности и т. п., с последующей их визуализацией на экране средствами трехмерной графики позволит интеллектуальным системам прогнозирования ЧС добиться более значительных результатов и расширить спектр задач, решаемых данными системами.

Таким образом, в рамках современных интеллектуальных систем прогнозирования ЧС присутствует широкий спектр задач, решение которых можно было бы усовершенствовать с помощью программных средств визуализации трехмерной графики, реализующих, в частности, алгоритмы поведения почв и растительности с течением времени без ручного обновления данных с достаточно высокой долей вероятности.

УДК 681.3.06

О. А. Нистюк, маг. (БГТУ, г. Минск)

КЛАССИФИКАЦИЯ И СРАВНИТЕЛЬНЫЙ АНАЛИЗ СОВРЕМЕННЫХ МЕТОДОВ ТЕКСТОВОЙ СТЕГАНОГРАФИИ

Стеганография – наука о передаче сокрытых данных внутри других, открытых данных. В отличие от криптографии, где просто происходит конвертирование сообщение в некий нечитаемый массив данных, стеганография делает сообщение незаметным, пряча его в других данных тем или иным способом.

Все многообразие методов текстовой стеганографии подразделяется на синтаксические, которые не затрагивают семантику текстового сообщения, и лингвистические методы, которые основаны на эквивалентной трансформации текстовых файлов, сохраняющей смысловое содержание текста, его семантику.

Под лингвистической стеганографией подразумевается набор алгоритмов и приемов, использующих текст в качестве контейнера, при этом используя некие лингвистические знания. Заполненный в результате использования алгоритма лингвистической стеганографии контейнер все еще должен содержать достаточно осмысленный текст с орфографией, лексикой и синтаксисом.

Итак, разберем несколько методов текстовой стеганографии.

1. Метод изменения регистров символов. Данный метод предполагает кодирование нулевого бита сообщения строчным символом контейнера, а единичного – прописным символом. Для кодирования можно использовать только буквенные символы контейнера. Содержимое файла-контейнера считывается посимвольно, если очередной символ является буквой, происходит кодирование бита сообщения.

2. Метод добавления хвостовых пробелов. В процессе шифрования текстовый контейнер считывается построчно. Удаляются пробелы, находящиеся в конце строки, игнорируются символы _\r‘ (символ возврата каретки) и _\t‘ (табуляция).

3. Модифицированный метод добавления хвостовых пробелов. В конце каждой строки добавляется от нуля до пятнадцати пробелов, кодируя полубайт.

4. Знаки одинакового начертания. Ряд символов русского и английского языка имеют одинаковое начертание в некоторых шрифтах, но разные ASCII-коды.

5. Двойные пробелы между словами. В данном методе один или два пробела кодируют бит информации.

6. Использование синонимов. Используя большой словарь синонимов, можно заменять отдельные слова их синонимами, при этом кодируя от одного бита информации.

7. Опечатки в тексте. Суть алгоритма заключается во внедрении в готовый текстовый контейнер опечаток.

8. Эмотиконы. Эмотико́н (англ. emoticon) — пиктограмма, изображающая эмоцию; чаще всего составляется из типографских знаков.

Все перечисленные алгоритмы оцениваются по следующим параметрам:

1. Качество сокрытия – качественная характеристика меры искажения контейнера. 0 баллов – стегоканал плохо сокрыт, заполненный контейнер очень просто обнаружить. 5 баллов – стегоканал сокрыт относительно хорошо. 10 баллов – стегоканал полностью сокрыт.

2. Скрытость. Атакующая сторона может определить наличие сообщения в контейнере путем подсчета определенных статистических свойств файла и сравнения полученных результатов со значениями, которые ожидаются от таких типов файла. 0 баллов – стегоканал обнаружим за очень короткое время. 5 баллов – стегоканал обнаружим за относительно небольшое время. 10 баллов – стегоканал не обнаружим за разумное время.

3. Устойчивость. Мера способности алгоритма сохранять сообщение даже после того, как контейнер подвергался неким изменени-

ям: линейная и нелинейная фильтрация, добавление случайного шума, сжатие с потерями/восстановление или некоторых видов обработки. 0 баллов – после изменения контейнера сообщение полностью теряется. 5 баллов – после изменения контейнера сообщение можно прочесть, однако произошло искажение стегосообщения. 10 баллов – после изменения контейнера стегосообщение полностью сохранилось.

4. Соотношение «сигнал/шум». Эта величина является мерой качества сокрытия или необнаружимости. В основном, высокое значение соотношение идеально для систем коммуникации, а низкое – идеально для стеганографии, так как контейнер – это шум, а сообщение – сигнал.

На основе сравнительного анализа по нескольким критериям можно сделать вывод о каждом алгоритме. Нельзя ориентироваться только на итоговую оценку, как как лингвистические методы зависят от содержания текста. Необходимо подбирать метод по определенным критериям.

Таблица

Номер алгоритма	Соотношение сигнал/шум	Устойчивость	Скрытость	Качество сокрытия	Итоговая оценка
1	10	5	5	0	20
2	0	5	0	5	10
3	5	5	0	0	10
4	5	5	5	5	20
5	0	5	0	5	10
6	5	10	5	10	30
7	5	5	5	5	20
8	10	10	5	10	35

Сложность алгоритма также является важным свойством. Метод требующий больших вычислений может привести к высокому качеству сокрытия и устойчивости, что также может повлечь увеличение времени, требующегося атакующей стороне на попытку взлома. Время выполнения кодирования в большинстве случаев менее приоритетно, по сравнению с остальными свойствами алгоритма. В каждом методе есть свои достоинства и недостатки. В наше время разрабатывается множество программных средств для защиты информации различными способами. При выборе метода в первую очередь необходимо обращать внимание на структуру текста, на объем информации, на стиль написания текста, а также на факторы угрозы безопасности информации.

ЛИТЕРАТУРА

1. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации / П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.