

В. П. З я з и н, А. Ю. К у л а й, М. В. Ф е д ю к и н (Москва, МИР-ЭА, ООО «Линфо»). **Об одном подходе к созданию цифровых водяных знаков в тексте на естественном языке.**

Использование текста на естественном языке в качестве стеганографического контейнера достаточно долгое время не вызывало особого интереса со стороны исследователей. Значительно большее внимание уделялось использованию мультимедийных файлов (аудио, видео, графических) для скрытия информации, что вполне естественно, учитывая возможности размещения в них дополнительных, избыточных данных. Вместе с тем, постановка вопроса об использовании в качестве контейнера естественного текста вполне правомерна, поэтому уже в девяностых годах прошлого века отдельные работы на эту тему все же стали появляться.

Первоначально для внедрения водяных знаков в текст использовались методы, характерные для работы с мультимедийными водяными знаками. В их основе лежали такие принципы стеганографии, как случайное присвоение символьных пробелов, смещение строки, смещение слова и вставка символа. Однако данные методы имели ограниченные возможности применения и не всегда были устойчивы против атак. Вследствие этого для внедрения в тексты на естественных языках цифровых водяных знаков стали применять методы, основанные на лингвистических принципах.

В работе [1] впервые был представлен метод лексической замены, заключающийся в использовании управляемой замены слов синонимами. Дальнейшее развитие метод получил в [2, 3]. В работах [5, 6] рассмотрены подходы к практической реализации метода. Применения этого метода для русского языка даны в [4].

В работе [7] метод был уточнен с учетом использования синонимов в зависимости от соседних слов (контекста). Оценки полезной скорости передачи (полезной нагрузки) при использовании лексической замены даны в [8].

Семантические преобразования текстов, заключающиеся в заменах слов словами одного семантического поля, рассмотрены в работах [9, 10]. На возможности применимости семантических преобразований существенно сказываются особенности языка.

Наиболее часто используемая категория цифровых водяных знаков основана на синтаксических преобразованиях предложения. Этот метод основан на факте, что предложения на одном языке могут быть выражены больше, чем одной синтаксической структурой (см. [5, 8, 11]).

Следующий подход изменения текстов связан с использованием двукратного машинного перевода (см. [12–14]).

В работе [15] предложен метод преднамеренного использования опечаток в тексте.

Высказывались соображения о возможности использования изменения пунктуации, однако практического развития этой идеи пока нет.

Необходимо отметить, что задача создания цифровых водяных знаков исследуется применительно к различным языкам. Помимо работ, касающихся английского и русского языков, упомянем работы [16–18], в которых рассматриваются турецкий и китайский языки.

Предлагается применять для кодирования скрываемой информации преобразования естественного текста на основе использования m -граммной модели на словах. Параметр m определяется, исходя из вычислительных возможностей и объема текстов, по которым строится модель. Текст на естественном языке разбивается на последовательные отрезки длиной n слов, где n не менее $2m + 1$. Для средней позиции на основе m -граммной модели определяются наиболее вероятные слова. Если имеется одно слово с доминирующей вероятностью, то замена и, соответственно, кодирование при помощи данного отрезка не производятся. Если наиболее вероятное слово не одно, то осуществляется замена.

Для применения метода необходимо, чтобы отправитель и получатель имели идентичные модели текстов. Из построения метода видно, что статистические ха-

рактические должны адекватно соответствовать характеристике текстов на естественном языке, по которым строилась m -граммная модель. Поэтому установить факт наличия скрытой информации автоматическими методами представляется затруднительным. Однако в связи с тем, что замены слов предполагается делать исключительно на основе статистических данных, человеком, в принципе, могут быть выявлены тексты, которые потенциально могут содержать скрытую информацию.

Для точного определения параметров метода необходимо дальнейшее проведение объемных экспериментов с использованием построенных моделей текстов.

СПИСОК ЛИТЕРАТУРЫ

1. *Chapman M., Davida G.* Hiding the hidden: A software system for concealing ciphertext as innocuoustext. — In: Proceedings of the 1st International Conference on Information and Communication Security CICS 97. Lecture Notes in Computer Science № 1334. Springer, 1997, p. 335–345.
2. *Chapman M., Davida G., Rennhard M.* A Practical and Effective Approach to Large-Scale Automated Linguistic Stenography. — In: Proceedings of International Conference on Information and Communication Security ICS 2001. Lecture Notes in Computer Science 2200. Springer, 2001, p. 156–165.
3. *Chapman M. T., Davida G. I.* Plausible deniability using automated linguistic steganography. — In: Infrastructure Security: International Conference. Lecture Notes in Computer Science, № 2437, October 2002. Springer, 2002, p. 276–287.
4. *Большаков И. А.* Использование синонимов, ограниченных контекстными словосочетаниями, для целей лингвистической стеганографии. Донецкий национальный технический университет, Информационные процессы и системы, 2004, № 8.
5. *Topkara M., Riccardi G., Hakkani-Tur D., Atallah M. J.* Natural language watermarking: Challenges in building a practical system. — In: Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents, January 2006.
6. *Topkara U., Topkara M., Atallah M. J.* The hiding virtues of ambiguity: quantifiably resilient watermarking of natural language text through synonym substitutions. — In: Proceeding of the 8th Workshop on Multimedia and security MM& Sec'06. New York: ACM Press, 2006, p. 164–174.
7. *Taskiran C. M., Topkara U., Topkara M., Delp E. J.* Attacks on lexical natural language steganography systems. — In: Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents, January 2006.
8. *Murphy B., Vogel C.* Statistically constrained shallow text marking: techniques, evaluation paradigm, and results. — In: Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents, January 2007.
9. *Atallah M. J., Raskin V., Hempelmann C. F., Karahan M., Sion R., Topkara U., Triezenberg K. E.* Natural language watermarking and tamperproofing. — In: The Fifth International Workshop on Information Hiding. Lecture Notes in Computer Science, № 2578. Springer, October 2002, p. 196–212.
10. *Raskin V., Hempelmann C. F., Triezenberg K. E., Nirenburg S.* Ontology in information security: a useful theoretical foundation and methodological tool. — In: Proceedings of the 2001 workshop on New security paradigms NSPW'01. ACM Press, September 2001, p. 53–59.
11. *Meral H. M., Sankur B., Ozsoy S.* Syntactic tools for natural language watermarking. In: — Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents, January 2007.
12. *Grothoff C., Grothoff K., Alkhutova L., Stutsman R., Atallah M.* Translation-based steganography. Technical Report TR 2005-39, Purdue CERIAS, 2005.

-
13. *Grothoff C., Grothoff K., Alkhutova L., Stutsman R., Atallah M.* Translation-based steganography. — In: Proceedings of Information Hiding Workshop (IH 2005). Springer, 2005, p. 213–233.
 14. *Stutsman R., Atallah M., Grothoff C., Grothoff K.* Lost in just the translation. — In: Proceedings of the 21st Annual ACM Symposium on Applied Computing (SAC 2006), April 2006.
 15. *Topkara M., Topkara U., Atallah M. J.* Information hiding through errors: A confusing approach. — In: Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents, January 2007.
 16. *Merall H. M., Sevinç E., Ünkar, Sankur B., Özsoy A. S., Güngör T.* Syntactic tools for text watermarking Linguistics Program. Boğaziçi University.
 17. *Yuling L., Xingming S., Can G., Hong W.* An efficient linguistic steganography for chinese text. Changsha, China: School of Computer and Communication Hunan University.
 18. *Yuling L., Xingming S., Yong W.* A Natural Language Watermarking Based on Chinese Syntax. Changsha, China: School of Computer and Communication Hunan University.