открытой и доступной для широкой аудитории. Размещение важной информации на сайте не только повышает видимость и доступность информации о фонде, но и способствует привлечению новых доноров и волонтеров. Благодаря удобству использования и прозрачности процессов, пользователи становятся более вовлеченными в деятельность фонда, что в свою очередь способствует росту доверия и поддержки. Успешное применение цифровых технологий позволяет фондам более эффективно реализовывать свои цели, организовывать мероприятия и делиться результатами своей работы с широкой аудиторией.

Список использованных источников

1. Куянова А.В. Инструменты продвижения благотворительных фондов// Инновационные научные исследования в современном мире. Сборник науч. статей по материалам VIII Международной научно-практической конференции. - Уфа, 2022. – С.157-164.
2. Недыхалов Л.А. Маркетинговый подход в исследовании информационного сопровождения деятельности благотворительной организации «WWF»// Вестник ВУиТ. - 2022. - №2(38). URL: <https://cyberleninka.ru/article/n/marketingovyy-podhod-v-issledovanii-informatsionnogo-soprovozhdeniya-deyatelnosti-blagotvoritelnoy-organizatsii-wwf> (дата обращения: 29.10.2024).
3. Беннет, Дж. Создание веб-приложений с использованием Django и Webflow. - Нью-Йорк: Tech Press, 2020.
4. Как создать веб-приложение: основные этапы. Интернет-ресурс. <https://scand.com/ru/company/blog/main-stages-of-creating-a-web-application/>

УДК 003.26+004.9

Н. П. Шутько, П. П. Урбанович

Белорусский государственный технологический университет
Минск, Беларусь

ВЕРОЯТНОСТНАЯ ОЦЕНКА УСТОЙЧИВОСТИ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ К АТАКАМ ПРИ ИСПОЛЬЗОВАНИИ ТЕКСТОВ В ВИДЕ КОНТЕЙНЕРОВ

Аннотация. Представлены основные особенности анализа безопасности стеганографической системы. Оценка устойчивости текстового

стеганоконтейнера к атакам, направленным на определение факта размещения тайной информации в контейнере или же ее извлечения, основана вероятностном представлении и описании процессов в создаваемой стеганосистеме.

N. P. Shutko, P. P. Urbanovich
Belarusian State Technological University
Minsk, Belarus

PROBABILISTIC ASSESSMENT OF THE RESISTANCE OF STEGANOGRAPHIC SYSTEMS TO ATTACKS USING TEXTS IN THE FORM OF CARRIERS

***Abstract.** The main features of the security analysis of the steganographic system are presented. Assessing the resistance of a text steganocontainer to attacks aimed at determining whether secret information is placed in the container or its extraction is based on a probabilistic representation and description of the processes in the steganosystem being created.*

Стеганография используется для скрытой передачи/хранения одного документа (тайного сообщения, M) в другом (контейнере или носителе, C). Текстовая стеганография подразумевает, что контейнером является текстовый документ. Контейнер с размещенной информацией называют стеганоконтейром, S . Степень защищенности последнего перед попыткой несанкционированного извлечения M характеризует безопасность стеганографической системы. Безопасность стеганосистем в последнее время отождествляется с тремя характеристиками: визуальная незаметность внедренного сообщения, робастность или устойчивость стеганоконтейнера к атакам, пропускная способность скрытого канала в стеганосистеме [1, 2].

Для улучшения приведенных характеристик безопасности процессы осаждения/извлечения тайной информации основываются на использовании мультинабора ключей (по аналогии с криптосистемами) [3, 4].

С учетом многоключевого характера стеганосистемы вероятностную оценку устойчивости системы к взлому или к модификациям можно будет осуществлять не по одному, а, по крайней мере, по трем независимым параметрам, соответствующим трем типам ключей (обозначим их как K^o и K^{d1} и K^{d2} : K^o определяет основной метод осаждения/извлечения тайного сообщения; дополнительные ключи K^{d1} и K^{d2} – соответственно первого и второго рода, при этом K^{d1} соотносится с предобработкой сообщения M , а K^{d2} – с выбором пространственно-геометрических или иных параметров контейнера, которые модифицируются при осаждении M в C). Особенность

указанной вероятностной оценки заключается в следующем.

В общем случае отдельно взятому сообщению M_i , генерируемому источником сообщений стеганосистемы, соответствует вероятность $p(M_i)$. При определении численных значений данной вероятности следует принимать во внимание объем контейнера, от которого зависит максимальный объем (размер) осаждаемого сообщения. Распределение рассматриваемых вероятностей описывается совокупным распределением вероятностей случайно выбранных сообщений M_i из общего множества $\mathbf{M}$, т. е. задается множеством вероятностей:

$$P_M = \{p(M_i)\}, i = 1, 2, \dots, n. \quad (1)$$

Здесь n – некоторое целое положительное число.

Источник контейнеров порождает поток пустых контейнеров из множества $\mathbf{C} = \{C_1, C_2, \dots, C_p\}$. Аналогично источнику сообщений, «работа» источника контейнеров может описываться случайным процессом. Итогом такого процесса являются случайно (для злоумышленника) выбранный контейнер C_j . Распределение соответствующих вероятностей запишем в следующем виде:

$$P_C = \{p(C_j)\}, j = 1, 2, \dots, p, \quad (2)$$

где $p(C_j)$ – вероятность выбора контейнера C_j из множества $\mathbf{C}$.

При решении задач защиты прав интеллектуальной собственности [5] выбор контейнера носит детерминированный характер, т. е. множество контейнеров содержит только один элемент, поскольку речь идет о защите конкретного документа. В таком случае распределение вероятностей (2) можно не учитывать.

По аналогии с вышеописанными рассуждениями источник ключей K_w^o и источники дополнительных ключей (K^{d1} и K^{d2}) опишем с помощью следующих распределений вероятностей:

$$P_{K^o} = \{p(K_w^o)\}, w = 1, 2, \dots, l, \quad (3)$$

где $p(K_w)$ – вероятность выбора некоторого ключа, определяющего метод текстовой стеганографии; при этом $\{K^o, K^{d1}, K^{d2}\} = \mathbf{K}$ – некоторое конечное множество возможных ключей;

$$P_{K^{d1}} = \{p((K^{d1}))_{w1}\}, w_1 = 1, 2, \dots, l_1, \quad (4)$$

и

$$P_{K^{d1}^*} = \{p((K^{d1*}))_{w1}\}, w_1 = 1, 2, \dots, l_1, \quad (5)$$

где $p(K^{d1})$ и $p(K^{d2*})$ — вероятности выбора некоторого дополнительного ключа (или ключей) первого рода соответственно при осаждении информации и при ее извлечении;

$$P_{K^{d2}} = \{p((K^{d2}))_{w2}\}, w_2 = 1, 2, \dots, l_2, \quad (6)$$

где $p(K^{d2})$ — вероятность выбора некоторого дополнительного ключа второго рода.

Если предположить, что число существующих на данный момент

методов осаднения информации в текстовых документах является конечным (например, равно L), то при оценке стойкости стеганосистемы к взлому учет вероятностной оценки использования того или иного метода осаднения можно трактовать как поправочный (уточняющий) коэффициент. Иначе говоря, использование многоключевой модели и, соответственно, использование подмножеств распределения вероятностей выбора всех типов ключей дает в общем случае более точную оценку устойчивости S к взлому.

Если основной целью использования системы является защита интеллектуальной собственности на контент (контейнер C) – текстовый документ, а осаждаемое сообщение M – также является текстовым документом, то задача оценки устойчивости системы к взлому приобретает свойственную таким системам специфику: важен не столько факт извлечения злоумышленником сообщения M из стегоконтейнера S , сколько обеспечение целостности стегоконтейнера при умышленном или случайном воздействии на него (некоторый источник шума – обозначим его условным параметром ΔS). В соответствии с этим, для наших систем целесообразно анализировать два параметра, относящиеся к стеганостойчивости: устойчивость S к взлому (обнаружение и извлечение M) и устойчивость S к нарушению целостности стегоконтейнера. Первый из указанных параметров свойственен криптографическим системам. Понятно, что при фиксированном размере S устойчивость системы к взлому будет тем выше, чем больше будет размер (количество символов) сообщения M . Устойчивость же к нарушению целостности снижается с увеличением размера M . Это утверждение не требует доказательства. Оно очевидно: манипуляции с фрагментами стегоконтейнера уменьшают потери информативности (фрагментов) сообщения M при меньших размерах M .

Таким образом, можно сформулировать важный вывод: задача по обеспечению устойчивости системы текстовой стеганографии к взлому стегоконтейнера (обнаружение и извлечение сообщения) и обеспечению устойчивости системы к нарушению целостности стегоконтейнера относится к числу компромиссных или оптимизационных. При этом и в первом, и во втором случаях устойчивость зависит не только от ключевой информации, но и от объемов сообщения M и контейнера C .

Основой для анализа устойчивости S к взлому могут служить условные вероятности размещения в конкретно выбранном стегоконтейнере S_q ($S_q \in \mathbf{S}$) сообщений M_i ($M_i \in \mathbf{M}$):

$$P_{M_i|S_q} = \{P(M_1|S_q), P(M_2|S_q), \dots, P(M_n|S_q)\} \quad (7)$$

и условные вероятности использования различных возможных ключей при осаждении информации:

$$P_{K^o|S_q} = \{P(K^o_1|S_q), P(K^o_2|S_q), \dots, P(K^o_w|S_q)\}, \quad (8)$$

$$P_{K^{d1}|S_q} = \{P((K^{d1})_1|S_q), P((K^{d1})_2|S_q), \dots, P((K^{d1})_{l1}|S_q)\}, \quad (9)$$

$$P_{K^{d2}|S_q} = \{P((K^{d2})_1|S_q), P((K^{d2})_2|S_q), \dots, P((K^{d2})_{l2}|S_q)\}, \quad (10)$$

а также ключей первого рода для извлечения информации:

$$P_{K^{d1*}|S_q} = \{P((K^{d1*})_1|S_q), P((K^{d1*})_2|S_q), \dots, P((K^{d1*})_{l2}|S_q)\}. \quad (11)$$

Указанные множества образуют совокупность предварительных сведений для извлечения из стегоконтейнера осажденного сообщения другим лицом (интрузом или стеганоаналитиком).

Что касается второго из параметров стеганографической устойчивости – устойчивости к нарушению целостности стегоконтейнера S , – то фактически данный вид устойчивости означает определение того порога параметра ΔS , за которым происходит разрушение сообщения M в контейнере C_j т.е. в S .

Список использованных источников

1. Ahvanooey M. T. [et al.]. Modern Text Hiding, Text Steganalysis, and Applications: A Comparative Analysis. *Entropy* 21, 2019:350–381. DOI: 10.3390/e21040355
2. Fridrich J., Kodovsky J. Rich models for steganalysis of digital images // *IEEE Trans. Information Forensics and Security*. 2012. V. 7. No. 3. P. 868–882. DOI: 10.1109/TIFS.2012.2190402
3. Urbanovich P. P., Shutko N. P. Theoretical Model of a Multi-Key Steganography System. In: *Recent Developments in Mathematics and Informatics. Contemporary Mathematics and Computer Science. Vol. 2, Chapter 11.* – Lublin: KUL, 2016. P. 181–202.
4. Shutko N., Urbanovich P., Zukowski P. A method of syntactic text steganography based on modification of the document-container aprosh. *Przegląd elektrotechniczny*. 2018;6:82–85. DOI: 10.15199/48.2018.06.15.
5. Шутько, Н. П., Урбанович П. П. Защита авторских прав на текстовые документы на основе стеганографической модификации цвета символов текста // *Информационные технологии: материалы 83-й НТК профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 4–15 февраля 2019 г.* – Минск: БГТУ, 2019. – С. 41-43.